RECONCILING PRIVACY WITH PROGRESS: FOURTH AMENDMENT PROTECTION OF E-MAIL STORED WITH AND SENT THROUGH A THIRD-PARTY INTERNET SERVICE PROVIDER

ABSTRACT

E-mail is increasingly becoming a common tool in modern society to communicate personal thoughts, feelings, and ideas. Despite the highly private nature of personal e-mail, Congress currently permits government agents to gain access to stored e-mail based upon a standard that falls short of the explicit protections provided by the Fourth Amendment. As personal e-mail progresses as a common method of communication, it must be given adequate privacy protections.

In 2010, the Sixth Circuit Court of Appeals in United States v. Warshak *found that a reasonable expectation of privacy exists in personal e-mail being sent through or held with a third-party commercial Internet Service Provider. The court in* Warshak *used a traditional Fourth Amendment analysis of telephone communications and postal mail to find a privacy interest in stored e-mail. The* Warshak *decision was a big step forward for the constitutional protection of e-mail, and it provided a strong judicial framework for other courts to follow. In order to ensure individuals are adequately protected against unwarranted governmental intrusions into private e-mail accounts, Congress must follow the judicial standards of* Warshak *and draft well-delineated statutes to adequately protect one of the most common communication methods in modern society.*

TABLE OF CONTENTS

I. INTRODUCTION

Before you send your next e-mail, take a moment to pause before clicking send to consider whether you enjoy a reasonable expectation of privacy in its contents. Are the contents of that e-mail protected under the Fourth Amendment from unwarranted government interception and seizure? The U.S. Supreme Court has yet to make that determination, and Congress currently permits governmental agents to obtain stored e-mail upon meeting a standard that falls short of the Fourth Amendment's

explicit protections.[1] In 2010, the Sixth Circuit Court of Appeals held in *United States v. Warshak* that a reasonable expectation of privacy exists in e-mail sent through or held with a third party Internet Service Provider (ISP).[2]

E-mail has become a common tool in modern society for instantaneous communication of thoughts, feelings, and ideas throughout the world with the simple click of a button.[3] E-mail not only has the ability to communicate personal information through text, but also through pictures, video, audio, links to websites, and other forms of media.[4] Over 90% of Internet users have sent or received e-mail,[5] and more than one-half of the United States' population uses e-mail daily—amounting to trillions of e-mail messages sent every year.[6] In recent years, e-mail has become so pervasive that it is commonly acknowledged as an essential element in everyday life,[7] and it is typically within an individual's immediate reach given the widespread use of smartphones, tablets, and other e-mail-capable devices.[8]

1. *See* discussion *infra* Part V.

2. United States v. Warshak, 631 F.3d 266, 284–86 (6th Cir. 2010).

3. *Id.* at 284 ("People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button.").

4. *See, e.g.*, *You're Invited to the Best Yahoo! Mail Ever*, YAHOO!, http://overview.mail.yahoo.com (last visited Oct. 17, 2012) (showing Yahoo! Mail offers video, audio, and document storage through their e-mail service).

5. Kristen Purcell, *Search and Email Still Top the List of Most Popular Online Activities*, PEW INTERNET & AM. LIFE PROJECT (Aug. 9, 2011), http://pewinternet.org/Reports/2011/Search-and-email.aspx.

6. Matthew A. Piekarski, *E-Mail Content's Brush with the Reasonable Expectation of Privacy: The* Warshak *Decision*, 47 U. LOUISVILLE L. REV. 771, 795 (2009).

7. *See Warshak*, 631 F.3d at 286 ("Over the last decade, email has become so pervasive that some persons may consider [it] to be [an] essential means or necessary instrument[] for self-expression, even self-identification." (alterations in original) (quoting City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010)) (internal quotation marks omitted)).

8. *See* Lee Rainie, *Tablet and E-Book Reader Ownership Nearly Double Over the Holiday Gift-Giving Period*, PEW INTERNET & AM. LIFE PROJECT (Jan. 23, 2012), http://pewinternet.org/Reports/2012/E-readers-and-tablets.aspx (noting that in 2012, 19% of adults owned a tablet computer); Aaron Smith, *Nearly Half of American Adults Are Smartphone Owners*, PEW INTERNET & AM. LIFE PROJECT (Mar. 1, 2012), http://pewinternet.org/Reports/2012/Smartphone-Update-2012.aspx (reporting that nearly one-half of adult cell phone users are smartphone owners, allowing mobile

Today, many personal e-mail accounts are held by web-based e-mail services such as Gmail, Yahoo! Mail, and Hotmail,[9] and e-mails are transmitted through third-party commercial ISPs.[10] Each personal e-mail sent, received, or stored on the user's web-based e-mail account must travel through or remain stored on a third-party commercial ISP server.[11] Using personal e-mail as a communication device causes individuals to have personal information stored electronically with "innumerable strangers."[12] A third-party ISP may retain limited access to e-mails stored or sent though the server in order to ensure compliance with account policies.[13] However, an ISP does not have routine access to search the personal content or to provide access for others to search the personal content of the private messages.[14] Granting governmental access to a commercial third-party ISP server to look for incriminating messages can endanger the privacy of millions.[15]

access to their e-mail).

9. *See* Janna Anderson & Lee Rainie, *The Future of Cloud Computing*, PEW INTERNET & AM. LIFE PROJECT (June 11, 2010), http://pewinternet.org/Reports/2010/The-future-of-cloud-computing/Overview.aspx (finding one of the most popular cloud services is webmail service, such as Hotmail and Yahoo! Mail); *see also, e.g.*, *Gmail: A Google Approach to Email*, GMAIL, http://www.gmail.com (last visited Oct. 17, 2012); *Sign-Up for Hotmail*, MICROSOFT HOTMAIL, http://www.hotmail.com (last visited Oct. 17, 2012); *Yahoo!*, YAHOO! MAIL, http://www.mail.yahoo.com (last visited Oct. 17, 2012).

10. *See Warshak*, 631 F.3d at 286 ("An ISP is the intermediary that makes email communication possible. Email must pass through an ISP's servers to reach their intended recipient.").

11. *Id.*; *see also* Marc J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not a Level Playing Field*, 97 J. CRIM. L. & CRIMINOLOGY 569, 573, 578–83 (2007) (detailing the role of ISPs in the transmission and storage of electronic communications).

12. *See* United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1005 (9th Cir. 2009), *rev'd en banc*, 621 F.3d 1162 (9th Cir. 2010).

13. *See, e.g.*, *Warshak*, 631 F.3d at 286 (acknowledging that the ISP may gain the right to access e-mails for certain purposes through the subscriber agreement).

14. *See id.* at 286–87 ("[T]he mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy."); Warshak v. United States, 490 F.3d 455, 475 (6th Cir. 2007) (noting that ISPs do not access e-mail content in "the normal course of business" and discussing the government's need to secure e-mail content through a warrant or subpoena); *see also* Tina Ebenger, *The USA PATRIOT ACT: Implications for Private E-Mail*, 4 J. INFO. TECH. & POL. 47, 55–56 (2007) (discussing the internal privacy policies of public ISPs and noting when a party's privacy is forfeited).

15. *Comprehensive Drug Testing*, 579 F.3d at 1005 ("Seizure of, for example, Google's email servers to look for a few incriminating messages could jeopardize the

Does a constitutional privacy interest attach to e-mail while it is being transmitted or stored on a third-party server? George Washington University Professor Orin Kerr has observed, "[T]he answer to the question of how much privacy protection the Fourth Amendment guarantees to Internet communications appears to be 'not much'—and certainly not enough."[16]

The decision in *United States v. Warshak*[17] was a significant leap forward for advocates of Fourth Amendment privacy protection in the digital age. The *Warshak* decision took common law Fourth Amendment principles and applied them to the modern issue of e-mail privacy protection.[18] Part II of this Note reviews the landscape of Fourth Amendment privacy. It discusses the evolution of Fourth Amendment protection and the development of both the reasonable expectation of privacy test and the third-party doctrine. Part III of this Note analyzes the Fourth Amendment protection applied to traditional forms of communication, including postal mail and telephone communication. Part IV discusses the impact of technology on the Fourth Amendment and the Supreme Court's hesitation in applying the reasonable expectation of privacy test to advancing technology. Part V of this Note looks at the federal statutes governing electronic communication, including the Stored Communications Act. Part VI provides a brief overview of how courts have generally applied the Fourth Amendment to e-mail. Part VII discusses the Sixth Circuit Court of Appeals decision in *United States v. Warshak*, finding a reasonable expectation of privacy in e-mail stored with or transferred through a third-party ISP. Finally, Part VIII evaluates the future of Fourth Amendment protection of stored e-mail. This Note advocates that courts should set clear precedent when presented with the issue of the constitutionality of the search and seizure of stored e-mail. The courts, however, cannot provide timely action, and adequate protection for users of stored e-mail ultimately lies in the hands of Congress.

privacy of millions.").

16. Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 814 (2003).

17. *Warshak*, 631 F.3d at 266.

18. *See id.* at 283–88 (finding a reasonable expectation of privacy in e-mail stored with a third-party ISP by applying common law Fourth Amendment principles).

II. FOURTH AMENDMENT PRIVACY PROTECTION

A. *History of Fourth Amendment Protection*

The Fourth Amendment protects an individual's "persons, houses, papers, and effects, against unreasonable searches and seizures" and provides that "no Warrants shall issue, but upon probable cause."[19] The fundamental purpose of the Fourth Amendment is to "safeguard the privacy and security of individuals against arbitrary invasions by government officials."[20] Fourth Amendment protections apply when the government conducts a search or seizure of an individual's property.[21] In order for the search or seizure to be within the constitutional bounds of the Fourth Amendment, it must be carried out with a valid warrant issued by a detached magistrate, or fall under one of the many warrantless-search exceptions.[22] Courts have traditionally struggled to determine when a search or seizure occurs, so as to trigger Fourth Amendment protections.[23] As society adapts and evolves around the ever-changing realities of life, it is often a difficult task for the courts to keep pace with progress.[24] It is vital to understand the judicial framework of the Fourth Amendment to fully understand the privacy protections afforded to e-mail communication.

B. *Traditional Fourth Amendment Approach*

Explicit in the Fourth Amendment are the words "[t]he right of the people to be secure in their persons, houses, papers, and effects, against

19. U.S. CONST. amend. IV.

20. Camara v. Mun. Court of S.F., 387 U.S. 523, 528 (1967).

21. *See* U.S. CONST. amend. IV; Olmstead v. United States, 277 U.S. 438, 466 (1928) (noting that the Fourth Amendment is not implicated "unless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure").

22. *See* Kentucky v. King, 131 S. Ct. 1849, 1864 (2011) ("Exceptions to the warrant requirement . . . must be 'few in number and carefully delineated,' if the main rule is to remain hardy." (quoting United States v. United States Dist. Court for E. Dist. of Mich., 407 U.S. 297, 318 (1972)).

23. *See* Kyllo v. United States, 533 U.S. 27, 31 (2001) ("[T]he antecedent question whether or not a Fourth Amendment 'search' has occurred is not so simple under our precedent.").

24. *See* United States v. Jones, No. 10–1259, slip op. at 10 (U.S. Jan. 23, 2012) (Alito, J., concurring) ("Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes.").

unreasonable searches and seizures."[25] Traditionally courts have applied the Fourth Amendment to protect physical objects such as "person, papers, houses and effects."[26] The Fourth Amendment protection of physical objects has historically been based upon common law property-based principles.[27]

Although the property-based approach was the guiding Fourth Amendment test for many years, the modern reasonable expectation of privacy test was first expressed by Justice Brandeis in a dissenting opinion in *Olmstead v. United States*.[28] In *Olmstead*, the majority held that a wiretap physically attached to telephone wires on public property was not a search because there was no invasion of a person's home or office.[29] Justice Brandeis famously disputed the property-based approach and read the Fourth Amendment as prohibiting "every unjustifiable intrusion by the Government upon the privacy of the individual," regardless of a physical intrusion.[30] Justice Brandeis' prophetic Fourth Amendment theory was echoed years later in the landmark decision of *Katz v. United States*, which established the modern test for Fourth Amendment search and seizure.[31]

C. Katz v. United States *and the Reasonable Expectation of Privacy Test*

The *Katz* decision set forth the modern test for determining Fourth Amendment privacy interests.[32] In *Katz*, the defendant entered a public phone booth, closed the door, and placed illegal bets through the telephone

25. U.S. CONST. amend. IV.

26. *See Jones*, No. 10-1259, slip op. at 4 ("The text of the Fourth Amendment reflects its close connection to property, since otherwise it would have referred simply to 'the right of the people to be secure against unreasonable searches and seizures'; the phrase 'in their persons, houses, papers, and effects' would have been superfluous.").

27. *See id.* ("Fourth Amendment jurisprudence was tied to common-law trespass, at least until the later half of the 20th century." (citing *Kyllo*, 533 U.S. at 31)).

28. Olmstead v. United States, 277 U.S. 438, 471 (1928) (Brandeis, J., dissenting).

29. *Id.* at 466 (majority opinion).

30. *Id.* at 478 (Brandeis, J., dissenting).

31. Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (determining that a Fourth Amendment search should be based upon the "reasonable expectation of privacy" test); *see also* California v. Ciraolo, 476 U.S. 207, 218 (1986) (noting the continued importance of *Katz* in Fourth Amendment jurisprudence).

32. *See Katz*, 389 U.S. at 360–61 (Harlan, J., concurring); *Ciraolo*, 476 U.S. at 218 (noting the "reasonable expectation of privacy" test has been followed by the Court since the *Katz* decision).

to the bookkeeper on the other end.[33] Unknown to the defendant, the government had wiretapped the phone line and recorded his conversation.[34] The content of the recorded conversation was subsequently used against him in criminal proceedings.[35] Katz challenged the constitutionality of the government's actions, claiming they violated his Fourth Amendment right of privacy.[36] The Court, straying away from property-based principles, held that Fourth Amendment protection extends to "people, not places," and noted that Katz had a reasonable expectation of privacy in the content of his telephone conversation.[37]

In a concurring opinion by Justice Harlan, the modern test for Fourth Amendment privacy protections emerged and became the governing standard to determine whether a Fourth Amendment search or seizure occurred—the "reasonable expectation of privacy" test.[38] The first component of the test is whether the individual has exhibited an "actual (subjective) expectation of privacy."[39] The second prong of the test is whether that individual's actual expectation of privacy is one that society is objectively "prepared to recognize as reasonable."[40] After *Katz*, the reasonable expectation of privacy test became the governing test to determine whether a Fourth Amendment search or seizure occurred.[41]

D. *Information Voluntarily Conveyed to Third Parties*

Fourth Amendment protection does not extend to information that has been voluntarily conveyed to third parties.[42] For example, in *Smith v. Maryland*, the Court held that an individual does not have a privacy interest in the numbers he or she voluntarily dials into a telephone.[43] In

33. *Katz*, 389 U.S. at 348.
34. *Id.*
35. *Id.*
36. *Id.*
37. *Id.* at 351.
38. *Id.* at 360–61 (Harlan, J., concurring).
39. *Id.* at 361.
40. *Id.* (internal quotation marks omitted).
41. *See, e.g.*, Rakas v. Illinois, 439 U.S. 128, 143 (1978); United States v. Chadwick, 433 U.S. 1, 7 (1977); United States v. Miller, 425 U.S. 435, 442 (1976); United States v. Dionisio, 410 U.S. 1, 14 (1973); United States v. White, 401 U.S. 745, 752 (1971) (plurality opinion); Mancusi v. DeForte, 392 U.S. 364, 368 (1968); Terry v. Ohio, 392 U.S. 1, 9 (1968).
42. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979); *Miller*, 425 U.S. at 443.
43. *Smith*, 442 U.S. at 745–46.

Smith, the government tapped into a phone conversation and used a pen register to capture the numbers the defendant entered into his telephone.[44] Using the information obtained from the pen register, the government acquired sufficient information to establish probable cause, allowing it to obtain a warrant to search the defendant's property.[45] In response to the Fourth Amendment challenge, the Court held that an individual does not have a reasonable expectation of privacy in information voluntarily given to a third party.[46]

However, even though the government may obtain information voluntarily conveyed to third parties, the holding of *Smith* was limited to non-content information.[47] Thus, the government's seizure of numbers entered into the telephone was permissible, but the government was not entitled to the content of the conversation.[48] The Court found the telephone numbers to be non-content information because they were the type of information commonly used by the telephone service provider, and therefore, the expectation of privacy in those numbers was diminished.[49]

Similarly, in *United States v. Miller*, the Court held that a search did not occur when the government obtained a customer's bank account information from the bank without a warrant.[50] The Court found there was no expectation of privacy in information voluntarily conveyed to the bank, such as bank account information.[51] The Court reasoned that the depositor takes a risk by voluntarily disclosing information to the bank because the bank could convey that information to the government.[52] Non-content information voluntarily conveyed to a third party has no reasonable expectation of privacy because the individual assumes the risk that a third

44. *Id.* at 737.

45. *Id.*

46. *Id.* at 743–44.

47. *See id.* at 743 ("Although petitioner's conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the number he dialed.").

48. *See id.* at 741 ("[Pen registers] do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers." (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977)) (internal quotation marks omitted)).

49. *Id.* at 743.

50. United States v. Miller, 425 U.S. 435, 442–44 (1976).

51. *Id.*

52. *Id.* at 443.

party could communicate the information to the government.[53]

The third-party doctrine under the Fourth Amendment has also been applied to rental property.[54] A tenant or guest permits the owner of the premise to enter the property to ensure the property is being properly maintained.[55] A reasonable expectation of privacy nonetheless exists in the property against the entry of others, such as government agents, and the owner of the premises is only given access for a limited purpose.[56]

III. FOURTH AMENDMENT AND TRADITIONAL FORMS OF COMMUNICATION

A. *Postal Mail*

The Supreme Court first addressed the protection of mail delivered through the postal system in *Ex parte Jackson*.[57] Using property-based theories, the Court established that individuals have a Fourth Amendment interest in the content of the parcels sent through the postal service.[58] Government officials must procure a warrant or show that the circumstances fit into one of the many warrantless-search exceptions in order to search packages that travel through the postal service.[59] The Court in *Ex parte Jackson* noted, "No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail," and any regulation must meet the requirements of the Fourth Amendment.[60]

Although a general constitutional right to privacy exists in the content

53. *See id.*; *see also* Guest v. Leis, 225 F.3d. 325, 335–36 (6th Cir. 2001) (finding a voluntary disclosure of information to a third-party ISP causes an individual to lose an expectation of privacy to the non-content information).

54. *See, e.g.*, Stoner v. California, 376 U.S. 483, 489 (1964); Chapman v. United States, 365 U.S. 610, 618 (1961).

55. *See Stoner*, 376 U.S. at 489 ("[W]hen a person engages a hotel room he undoubtedly gives 'implied or express permission' to such persons as maids, janitors or repairmen' to enter his room in the performance of their duties." (quoting United States v. Jeffers, 342 U.S. 48, 51 (1951)) (internal quotation marks omitted)).

56. *See id.* at 490; *Chapman*, 365 U.S. at 618 (holding that police officers' unwarranted search of a rented premise with permission from the landlord and not from the tenant was a search in violation of the Fourth Amendment).

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

58. *Id.* at 733.

59. *See id.*

60. *Id.*

of parcels that travel through the postal service, the right is not without limitations. In *United States v. Van Leeuwen*, the Supreme Court held that people do not maintain a privacy interest in words, substances, and physical characteristics on the exterior of the package—the non-content information.[61] While a letter sent through the mail is given protection as to the private content of the message, any communication on the visible exterior of the package may be searched without a warrant.[62]

B. *Telephone Communications*

The Supreme Court has long held a caller has a reasonable expectation of privacy in the content of a phone call.[63] In *Berger v. New York*, the Supreme Court held that an unwarranted recording of telephone conversations was a search implicating Fourth Amendment protection.[64] Specifically, the Court found a New York statute unconstitutional as it permitted court-ordered wiretaps of telephone conversations upon a showing less than probable cause.[65] After *Berger*, the Supreme Court in *Katz* again held that the Fourth Amendment protects telephone conversations because a caller is entitled to a reasonable expectation of privacy in telephone conversations.[66] The Court stated the caller is "surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[67]

In protecting the content of telephone conversations, great emphasis is placed on the recipient of the conveyed information.[68] This analysis generally implicates the doctrine of third-party voluntary disclosure.[69] Since the content of information conveyed through the phone is intended to reach only the intended recipient of the call, the caller does not lose an expectation of privacy when the conversation is routed through a phone

61. United States v. Van Leeuwen, 397 U.S. 249, 252–53 (1970).

62. *See id.* at 252.

63. *See, e.g.*, Katz v. United States, 389 U.S. 347, 352 (1967); Berger v. New York, 388 U.S. 41, 51 (1967).

64. *See Berger*, 388 U.S. at 63–64.

65. *Id.*

66. *See Katz*, 389 U.S. at 352.

67. *Id.*

68. *See id.*

69. This doctrine provides that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (citations omitted).

service company.[70] However, once the information conveyed over the telephone conversation reaches the recipient, the caller can be said to have lost all reasonable expectation of privacy in that conversation.[71]

The type of information shared with third-party service providers is also important. In telephone conversations, there is heightened protection for the content of the communication.[72] The third-party provider may freely obtain actual information intended to be conveyed to the provider such as phone numbers and customer information, but not the private content of the communication itself.[73]

IV. FOURTH AMENDMENT AND TECHNOLOGY

Difficulties emerge when applying the Fourth Amendment to technological advancements. As Justice Brandeis declared in 1928, the Fourth Amendment must have the "capacity of adaptation to a changing world."[74] More than eighty years later, the Sixth Circuit echoed Justice Brandeis' comment by stating "the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."[75] Technological advancements create difficulties in analyzing the Fourth Amendment because the property-based and reasonable expectation of privacy approaches are often rendered unworkable.[76]

A. *Challenges in the Application of the Property-Based Approach to New Technology*

New technology can make the property-based approach to the Fourth Amendment unworkable because the property at issue may not be

70. *See id.* at 743.

71. *See Smith*, 442 U.S. at 743–44; United States v. White, 401 U.S. 745, 751 (1971).

72. *See Smith*, 442 U.S. at 741–42 (finding the information revealed by a pen register does not reveal the content of communications and thus does not violate the Fourth Amendment when seized by police officers).

73. *See id.*

74. Olmstead v. United States, 277 U.S 438, 472 (1928) (Brandeis, J., dissenting).

75. United States v. Warshak, 631 F.3d 266, 285 (6th Cir. 2010).

76. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 33–34 (2001) (finding that "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology" in attempting to apply traditional tests to thermal imaging of a home).

tangible. It is often difficult to determine who the rightful owner is of data and information stored in an intangible form. Consequently, a property-based approach to the Fourth Amendment may be unworkable when an intangible object is searched or seized. Simply put, the shoe may no longer fit.

B. *Challenges in the Application of the Reasonable Expectation of Privacy Approach to New Technology*

The reasonable expectation of privacy test also produces its own complications when applied to advanced technology. As society adapts to technological advancements, a reasonable expectation of privacy takes on a new meaning.[77] It is difficult for courts to determine the second prong of the reasonable expectation of privacy test—whether an individual's subjective expectation of privacy is one that society is prepared to recognize as reasonable—when the expectation of privacy changes with the pace of changes in technology.[78]

For example, the Supreme Court in *Kyllo v. United States* addressed a technological advancement under the reasonable expectation of privacy test.[79] In *Kyllo*, the government used a thermal imaging device to scan the exterior of the defendant's home, revealing "details of the home that would previously have been unknowable without physical intrusion."[80] The government subsequently used the information it gathered from the thermal imaging device to determine the defendant was illegally growing marijuana inside his home.[81] The Court held that the government's warrantless use of sense-enhancing technology not in "general public use" violated the Fourth Amendment.[82]

Kyllo is a good illustration of how the circular nature of the reasonable expectation of privacy can often render it unworkable when applied to emerging technology.[83] New technology often becomes readily

77. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 808 (2004) ("In this era of high-tech surveillance and the Internet, no one knows whether an expectation of privacy in a new technology is reasonable." (footnote omitted) (internal quotation marks omitted)).

78. *See id.* at 808–09.

79. *See* Kyllo v. United States, 533 U.S. 27, 29 (2001).

80. *Id.* at 40.

81. *Id.* at 30.

82. *Id.* at 34.

83. *See* Kerr, *supra* note 77, at 808.

available to the general public shortly after it was exclusively available to governmental officials.[84] For example, the general public can now easily obtain a thermal imaging device similar that used by government agents in *Kyllo*.[85] As society adopts advancements in technology, what constitutes a reasonable expectation of privacy can ebb and flow, making the reasonable expectation of privacy test unworkable.

C. *The Supreme Court's Hesitation to Apply the Reasonable Expectation of Privacy Test to New Technology*

Cases before the U.S. Supreme Court concerning the Fourth Amendment's application to advancing technologies are usually treated with great caution and can often be left unexplored.[86] In 2010, the Supreme Court expressed its concern over Fourth Amendment challenges to new technology in *City of Ontario v. Quon*.[87] In deciding whether a search of a government employee's text message violated the Fourth Amendment, the Court in *Quon* cautioned that it "must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment."[88] The Court was circumspect in addressing the issue due to the difficulty of predicting how privacy expectations will be shaped by the changes and adaptation of society to advancements in technology.[89]

Recently, in January 2012, the Supreme Court in *United States v.*

84. Douglas Adkins, *The Supreme Court Announces A Fourth Amendment "General Public Use" Standard for Emerging Technologies but Fails to Define It:* Kyllo v. United States, 27 U. DAYTON L. REV. 245, 255 (2002).

85. Orin Kerr, *Can the Police Now Use Thermal Imaging Devices Without a Warrant? A Reexamination of* Kyllo *in Light of the Widespread Use of Infrared Temperature Sensors*, THE VOLOKH CONSPIRACY (Jan. 4, 2010, 12:33 PM), http://www.volokh.com/2010/01/04/can-the-police-now-use-thermal-imaging-devices-without-a-warrant-a-reexamination-of-kyllo-in-light-of-the-widespread-use-of-infrared-temperature-sensors/.

86. *See* City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." (citations omitted)); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1025 (2010) ("[T]he Fourth Amendment rules governing online surveillance have remained largely unexplored.").

87. *See Quon*, 130 S. Ct. at 2629.

88. *Id.*

89. *Id.* at 2629–30 ("[T]he Court would have difficulty predicting how employees' privacy expectations will be shaped by those changes or the degree to which society will be prepared to recognize those expectations as reasonable." (citing O'Conner v. Ortega, 480 U.S. 709, 715 (1987))).

Jones avoided applying the reasonable expectation of privacy test to a Fourth Amendment challenge to advanced technology and instead reverted to a traditional property-based analysis.[90] The Supreme Court was confronted with the issue of whether a long-term detailed tracking of a suspected criminal using a GPS device attached to a vehicle constituted a search in violation of the Fourth Amendment.[91] The Court did not apply the reasonable expectation of privacy test to determine whether GPS tracking is a search.[92] Instead, it sidestepped the issue by relying on the property-based theory of trespass to determine the attachment of the device on a vehicle was a physical search in violation of the Fourth Amendment.[93] The majority failed to address whether the use of a technological advancement—long-term, detailed GPS tracking—violated the defendant's reasonable expectation of privacy.[94]

In *Jones*, the Court regarded the *Katz* test as taking a backseat to the property-based test.[95] This case illustrates the Supreme Court's inclination to revert to the common-law property-based test when confronted with a Fourth Amendment search or seizure issue, and to use the *Katz* reasonable expectation of privacy test if the property-based evaluation does not apply.[96] The application of a property-based evaluation to a technological issue by the Court raises questions about its willingness to update its standard in ruling on future issues involving new technology and the Fourth Amendment.

V. FEDERAL STATUTORY PROTECTION FOR ELECTRONIC COMMUNICATION

Congress has tried to keep pace with the technological evolution of recent years by regulating the search and seizure of e-mails and other electronic communication through federal statutes.[97] Currently, federal

90. United States v. Jones, No. 10-1259, slip op. at 3–4 (U.S. Jan. 23, 2012).

91. *Id.* at 1.

92. *Id.* at 3–4.

93. *Id.*

94. *See id.* at 5 ("But we need not address the Government's contentions [regarding a reasonable expectation of privacy], because Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation.").

95. *See id.* at 5–7 (emphasizing that the "*Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test").

96. *See id.*

97. *See* Kerr, *supra* note 77, at 855–56 (discussing how Congress has "acted on its own initiative to protect privacy against the threat of new technology" by passing

statutes are the primary source of law governing searches and seizures of electronic communication, as statutory regulations often create higher warrant requirements for electronic surveillance than that required by the Fourth Amendment, and often provide an explicit suppression remedy for search and seizure violations.[98]

Congress enacted the Electronic Communications Privacy Act (ECPA) in 1986[99] in an attempt to keep pace with the prevalence of electronic communication.[100] "[T]he ECPA was precipitated by concerns about advancements in technology and the desire to protect personal and business information which individuals [could] no longer 'lock away' with ease."[101] The ECPA divided electronic surveillance into three sections: the Wiretap Act,[102] the Stored Communications Act,[103] and the provisions regulating pen registers and tracing devices.[104]

The Stored Communications Act (SCA) is the section of the ECPA most applicable to e-mail stored or sent through a third-party ISP.[105] The SCA regulates governmental access to customer e-mail stored by third-party service providers.[106] Under § 2703(a), government agents may obtain information stored with the third-party server that has been stored on the ISP server for less than 180 days pursuant to a warrant.[107] To obtain e-mail messages on ISP servers that have been stored more than 180 days, the government can search stored e-mail pursuant to a court order, which requires a showing of a standard less than probable cause.[108] Under

the Privacy Act of 1974, the Cable Communications Privacy Act of 1984, the Electronic Communications Privacy Act of 1986, and the Video Privacy Protection Act of 1988).

98. *See* Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522, 2701–2712, 3121–3127 (2006).

99. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–2522, 2701–2712, 3121–3127 (2006)).

100. *See* United States v. Warshak, 631 F.3d 266, 334–35 (6th Cir. 2010) (Keith, J., concurring).

101. *Id.*

102. Wiretap Act, 18 U.S.C. §§ 2510–2522 (2006).

103. Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2006).

104. 18 U.S.C. §§ 3121–3127 (2006).

105. 18 U.S.C. §§ 2701–2712.

106. *See id.* § 2703.

107. *Id.* § 2703(a).

108. *Id.* § 2703(a)–(b) (allowing electronic information to be obtained pursuant to court order); *id.* § 2703(d) (providing for a court order to issue on a "reasonable grounds," rather than probable cause, standard).

§ 2703(d), the government may obtain a court order upon showing "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[109]

Although the SCA provides considerable protections for senders of electronic communication, its safeguards fall short of the standards required by the Fourth Amendment.[110] A search or seizure of personal communications based upon a standard lower than that required by the Fourth Amendment is a direct constitutional violation.

VI. GENERAL LANDSCAPE OF FOURTH AMENDMENT PROTECTION OF E-MAIL

While the Supreme Court has yet to determine the level of protection afforded to e-mail stored with or transferred through a third-party ISP, many lower courts have provided varying opinions as to whether a reasonable expectation of privacy extends to e-mail communication.[111] In *United States v. Lifshitz*, the Second Circuit Court of Appeals held that an individual has a reasonable expectation of privacy in his home computer, but not in transmissions made over the Internet or in the context of e-mails that have reached the recipient.[112] The Eleventh Circuit, in *Rehberg v. Paulk*, held that a reasonable expectation of privacy does not exist in e-mails that are sent to and received by a recipient.[113] However, the courts in *Lifshitz* and *Rehberg* did not determine the level of protection afforded to e-mail that travels through or is stored with a third-party ISP.

The U.S. Court of Appeals for the Armed Forces has recognized a

109. *Id.* § 2703(d).

110. *Compare* U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon *probable cause* . . . ." (emphasis added)), *with* 18 U.S.C. § 2703(d) (allowing records to be obtained upon "specific and articulable facts showing . . . records or other information sought, are *relevant and material* to an ongoing criminal investigation" (emphasis added)).

111. *See, e.g.*, Rehberg v. Paulk, 598 F.3d 1268, 1281 (11th Cir. 2010); United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004); United States v. Long, 64 M.J. 57, 65 (C.A.A.F. 2006).

112. *Lifshitz*, 369 F.3d at 190.

113. *Rehberg*, 598 F.3d at 1281 ("A person also loses a reasonable expectation of privacy in emails, at least after the email is sent to and received by a third party." (citing Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001))).

reasonable expectation of privacy in e-mail accounts.[114] In *United States v. Maxwell*, the court found a reasonable expectation of privacy exists in e-mail messages being transmitted through a third-party ISP.[115] However, the court noted the limited nature of this privacy interest since, much like the sender of postal mail or a telephone call, the sender loses all reasonable expectation of privacy once the recipient of the message receives the transmission.[116] Nevertheless, the court in *Maxwell* recognized that by sending e-mail via third-party ISPs, the sender still retains a reasonable expectation of privacy.[117]

VII. THE SIXTH CIRCUIT FINDS A PROTECTED PRIVACY INTEREST IN E-MAIL COMMUNICATIONS STORED WITH A THIRD-PARTY ISP

A. Warshak v. United States

In *Warshak v. United States*, the U.S. Court of Appeals for the Sixth Circuit was the first Article III court to address whether an e-mail account holder has a reasonable expectation of privacy in e-mail stored on a third-party server.[118] Facing this issue for the first time, the court ruled against the government and held that when government agents compel a third-party ISP to disclose an account holder's stored e-mails without a warrant, the government intrusion invades the user's reasonable expectation of privacy.[119]

1. *Facts of the Case*

Steven Warshak was accused of mail fraud, wire fraud, money laundering, and several other related federal offenses stemming from a massive scheme to defraud customers.[120] Warshak and his conspirators ran a series of companies that falsely marketed products by making false and fraudulent statements.[121] Most of the evidence concerning Warshak's

114. *See Long*, 64 M.J. at 65; United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996).

115. *See Maxwell*, 45 M.J. at 418 (holding that a military member had a subjective expectation of privacy in obscene e-mails communicated to another military member that were sent through a third-party ISP, America Online (AOL)).

116. *Id.*

117. *Id.* at 417.

118. Warshak v. United States, 490 F.3d 455, 469–76 (6th Cir. 2007).

119. *Id.* at 473.

120. *Id.* at 460.

121. *See* United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010) (stating

fraudulent activities was contained in Warshak's personal e-mail accounts, which were held by third-party ISPs, including NuVox Communications and Yahoo!.[122]

Responding to information regarding a suspicion of fraudulent activities, the government began to investigate Warshak and his company.[123] Relying on 18 U.S.C. § 2703—part of the SCA—the government obtained an order directing NuVox and Yahoo! to turn over the content of private e-mails stored in Warshak's personal e-mail accounts.[124] The order required a showing of "specific and articulable facts showing that there are reasonable grounds to believe the records or other information sought are relevant and material to an ongoing criminal investigation,"[125] which arises from § 2703(d).[126] The order prohibited the ISPs from disclosing information pertaining to the order or investigation to the account holder.[127] Warshak was unaware of the government's seizure of his personal e-mails until more than a year after the order was issued.[128] In total, over 27,000 of Warshak's personal e-mails were obtained by the government from NuVox and Yahoo! without Warshak's knowledge or consent.[129]

After learning of the government's actions, Warshak filed a claim for injunctive relief and declaratory judgment against the United States, alleging the compelled disclosure of his e-mails without a warrant violated the Fourth Amendment and the SCA.[130] The District Court for the Southern District of Ohio granted an injunction in favor of Warshak based on its finding that the government obtained relevant subscriber information without providing the subscriber adequate notice or a chance to be heard.[131] The government appealed the district court's grant of a

that Warshak's charges stemmed from the fraudulent distribution of an "herbal supplement purported to enhance male sexual performance" that was aggressively advertised on television).

122. *Warshak*, 490 F.3d at 460 (quoting the order obtained by the government concerning disclosure of e-mail information).

123. *See id.*

124. *Id.*

125. *Id.* (internal quotation marks omitted).

126. 18 U.S.C. § 2703(d) (2006).

127. *Warshak*, 490 F.3d at 460.

128. *Id.* at 460–61.

129. *See* United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010).

130. *Warshak*, 490 F.3d at 461.

131. *Id.*

preliminary injunction.[132]

2. *The Sixth Circuit Finds a Reasonable Expectation of Privacy in E-mail Stored on a Third-Party ISP Server*

On appeal, the Sixth Circuit Court of Appeals affirmed the grant of preliminary judgment and held Warshak had a reasonable expectation of privacy in his personal e-mails stored with NuVox and Yahoo!.[133] The court found a reasonable expectation of privacy in stored e-mail by comparing stored e-mail to telephone conversations.[134] The court considered the scope of persons who were privy to the communication and the type of information that was conveyed to each party.[135] As the ISPs had the ability to access the stored e-mail, the court applied the third-party doctrine to determine whether Warshak voluntarily gave up some level of privacy by storing e-mail with a third party.[136] However, the court reasoned that Warshak only released his privacy interest in the actual information he voluntarily conveyed, which excluded the *content* of the conversations.[137]

The court also held that the government improperly obtained Warshak's stored e-mail under § 2703 of the SCA.[138] The court noted that the government failed to provide adequate notice to the account holder and failed to prove the account holder waived his right to privacy with the ISP by granting them complete access to the content of the stored e-mail.[139]

3. *Decision Vacated*

Shortly after issuing the opinion in *Warshak*, the Sixth Circuit, en banc, vacated the decision on the grounds of ripeness, making the pinnacle holding moot.[140]

B. United States v. Warshak

In 2010, the same parties presented the same issue to the Sixth Circuit

132. *Id.* at 462.
133. *Id.* at 473.
134. *Id.* at 469–76.
135. *See id.* at 470–71.
136. *See id.* at 470.
137. *Id.* at 470–71.
138. *Id.* at 475–76.
139. *Id.*
140. *See* Warshak v. United States, 532 F.3d 521, 534 (6th Cir. 2008) (en banc).

yet again.[141] Warshak brought a criminal appeal following his conviction on multiple counts of fraud, arguing the government's warrantless seizure of his private e-mails violated the Fourth Amendment.[142] The court again held that the government violated Warshak's Fourth Amendment rights by compelling NuVox and Yahoo! to turn over the contents of his private e-mails.[143]

On hearing the issue for a second time, the Sixth Circuit took a slightly different approach to the issue. The court's analysis centered on the reasonable expectation of privacy test as described in *Katz v. United States*.[144] The court determined the first prong of the *Katz* test was met because Warshak clearly manifested a subjective expectation of privacy in his stored e-mail, as the e-mails contained "sensitive and sometimes damning substance" relating to his business practices and personal life.[145]

The main focus of the court's analysis was dedicated to the second prong of the *Katz* test—whether society is prepared to recognize that expectation of privacy as reasonable.[146] The court noted the "grave import[ance] and enduring consequence" of such determination, as the Fourth Amendment must keep pace with society or its protections could diminish.[147]

The court found the societal expectations of privacy in e-mail were fundamentally similar to the privacy interests held in traditional forms of communication.[148] The court noted that "[e]mail is the technological scion of tangible mail, and it plays an indispensable part in the Information Age."[149] Much like postal mail and telephone calls, "[e]mails must pass

141. *See* United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010) (deciding whether Warshak's approximately 27,000 e-mails were properly seized under the Fourth Amendment).

142. *Id.* at 281–82.

143. *Id.* at 282.

144. *Id.* at 284 (discussing Fourth Amendment analysis in terms of a two-prong reasonable expectation of privacy test); *see also* Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (creating a test for Fourth Amendment violations based on an individual's reasonable expectation of privacy).

145. *Warshak*, 631 F.3d at 284.

146. *Id.* at 284–88.

147. *Id.* at 284.

148. *See id.* at 285–86 ("Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection." (citations omitted)).

149. *Id.* at 286.

through an ISP's servers to reach their intended recipient."[150] Using the precedents of *Katz v. United States*[151] and *Smith v. Maryland*,[152] the court found the mere ability of the third party to access the content of e-mail is not enough to diminish the expectation of privacy.[153]

The court also used the Fourth Amendment doctrine of rented spaces to further support a reasonable expectation of privacy in stored e-mail.[154] In rental spaces, an "expectation [of privacy] persists, regardless of the incursions of handymen to fix leaky faucets."[155] Therefore, some routine access to stored e-mail to audit, inspect, or monitor is not enough to break the expectation of privacy.[156]

The Sixth Circuit held that an e-mail account holder has a reasonable expectation of privacy in the contents of stored e-mail, and the court declared 18 U.S.C. § 2703(d) unconstitutional because it permits the issuance of a search warrant upon a standard short of probable cause.[157]

VIII. FUTURE FOURTH AMENDMENT IMPLICATIONS OF E-MAIL HELD WITH A THIRD-PARTY ISP

A. *A Reasonable Expectation of Privacy Exists in E-mail Stored With or Sent Through a Third-Party ISP*

The decision in *United States v. Warshak*[158] was a giant leap forward for Fourth Amendment protection in the context of private e-mail communication. The finding of a reasonable expectation of privacy in personal e-mail messages stored with or sent through a third-party commercial ISP was a long awaited decision on a pressing issue.[159] *Warshak* stands as a significant step toward adequate Fourth Amendment protection in the digital age, and it should be acknowledged by other courts and

150. *Id.*
151. Katz v. United States, 389 U.S. 347 (1967).
152. Smith v. Maryland, 442 U.S. 735 (1979).
153. *See Warshak*, 631 F.3d at 285–87.
154. *Id.* at 287.
155. *Id.*
156. *Id.*
157. *See id.* at 288. In light of finding a reasonable expectation of privacy in Warshak's e-mail, the court did not subject the seizure of e-mails to the exclusionary rule, as the law enforcement officials relied in good faith upon 18 U.S.C. § 2703(d) in obtaining the order directing the ISP to turn over the e-mails. *Id.* at 290.
158. *Id.* at 266.
159. *See id.* at 282–88.

Congress in order to keep pace with societal progress.

B. *Resolution*

1. *A Need for a Strong Judicial Framework*

The *Warshak* "decision, assuming it survives a potential appeal to the U.S. Supreme Court, marks a major turning point in the evolution of Fourth Amendment law in the Digital Age."[160] Not only does *Warshak* have an impact in e-mail communication, but the decision has the potential to influence other future decisions involving Fourth Amendment application to new technology.[161]

It is important for courts to confront search and seizure issues concerning e-mail communication as a means to carry Fourth Amendment protections forward.[162] With such grave importance in providing adequate Fourth Amendment protection, it is vital for the courts to provide a timely and consistent judicial framework to govern the privacy protection of personal e-mail.

The *Warshak* analysis provides a good framework for courts to analyze and determine how governmental agents can permissibly search the contents of electronic communication outside of traditional means.[163] Future courts faced with the issue of Fourth Amendment e-mail protection should not sidestep the issue, as the majority did in *U.S. v. Jones*.[164] Instead, courts should use the framework developed by *Warshak* to provide consistent e-mail privacy protection across the circuits.[165]

160. Larry Downes, *Search Warrants and Online Data: Getting Real*, CNET (Dec. 15, 2010, 1:52 PM), http://news.cnet.com/8301-31921_3-20025793-281.html.

161. *See* Orin Kerr, *Sixth Circuit Rules that E-Mail Protected by the Fourth Amendment Warrant Requirement*, THE VOLOKH CONSPIRACY (Dec. 14, 2010, 11:30 AM), http://volokh.com/2010/12/14/sixth-circuit-rules-that-e-mail-protected-by-the-fourth-amendment-warrant-requirement/.

162. *See* Jim E. Lavine, *Is Mail Still Mail? And Will the Fourth Amendment Survive the 21st Century?*, 35 FEB CHAMPION 5 (2011) ("[C]ourts around the country must confront vitally important 21st century search and seizure issues. Nothing less is at stake than the vitality of the Fourth Amendment and our right to privacy.").

163. *Cf.* Mike McNerney, Warshak*: A Test Case for the Intersection of Law Enforcement and Cyber Security*, 2010 U. ILL. J.L. TECH. & POL'Y 345, 346 (2010) (arguing the original 2007 *Warshak* decision, before vacation on the ripeness issue, presented the first reasonable judicial framework for analyzing the search and seizure of electronic communications).

164. United States v. Jones, No. 10–1259, slip op. at 4–5 (U.S. Jan. 23, 2012).

165. United States v. Warshak, 631 F.3d 266, 282–88 (6th Cir. 2010).

The judiciary, however, must not be the only branch of government to take appropriate action. According to Professor Orin Kerr, the popular view to applying the Fourth Amendment to new technology is that "the courts and the Constitution should offer the primary response. While Congress and state legislatures may have a limited role regulating government investigations involving new technologies, the real work must be done by judicial interpretations of the Fourth Amendment."[166] Yet, Professor Kerr, and this Note, call into question the "popular view" of the Fourth Amendment's adaptation to advancing technologies.[167] Although judicial interpretation is necessary, the primary actions to ameliorate Fourth Amendment intrusions involving technology must be taken by Congress or state legislatures.[168]

2. *Congress Must Respond and Stay Within the Judicial Framework*

As the courts struggle to keep pace with technological advancements, Congress and state legislatures must take timely action using the framework provided by the courts. "Congress and the courts have struggled since the dawn of computers to understand just what kind of protections are appropriate for users of third-party computer services."[169] The problem the courts face is the circular nature of the reasonable expectation of privacy test.[170] A person has a reasonable expectation of privacy once the courts decide a privacy interest exists under the Fourth Amendment.[171] Yet, by the time the courts get around to addressing each issue, the expectation of privacy may diminish.[172]

In order to keep privacy protections on pace with society's acceptance of advancing technology, Congress should be the branch to take the primary action.[173] It takes years for the Supreme Court to issue a decision

166. *See* Kerr, *supra* note 77, at 802.

167. *See id.* at 804–805.

168. *See id.* at 805.

169. *See* Downes, *supra* note 160.

170. *See* Kerr, *supra* note 77, at 808 ("Part of the problem is that the [reasonable expectation of privacy] test is largely circular: a person has a reasonable expectation of privacy when the courts decide to protect it through the Fourth Amendment.").

171. *Id.* at 808–09.

172. *Id.*

173. *See id.* at 807–08 (arguing that legislatures are better equipped than the courts to confront timely technology issues under the Fourth Amendment).

after an initial action takes place.[174] Technological advancements occur daily, and what constitutes a reasonable expectation of privacy in data today, may perish tomorrow. Courts simply cannot keep pace with rapid advancements in technology. Instead, courts must work to provide constitutional principles and doctrines in order for the legislatures to have a solid framework to create and build-up statutes governing privacy concerns with technology advancements.[175] When technology advances, Congress and state legislatures must respond by drafting well-delineated statutes that stay within the bounds of the judicial guidelines governing the Fourth Amendment.

Much like Congress's intent in enacting the SCA—to address concerns about advancements in technology[176]—Congress and state legislatures must continually respond to judicial interpretations of Fourth Amendment principles to develop constitutional statutes that address technological advancements.[177] Without swift congressional action, the long-standing reasonable expectation of privacy test could begin to erode because courts can no longer keep up with expectations of privacy that society recognizes as reasonable.

IX. CONCLUSION

As e-mail increasingly becomes a common method of communication, it must be given adequate Fourth Amendment protection. The Sixth Circuit Court of Appeals in *United States v. Warshak* correctly held a reasonable expectation of privacy extends to an account holder who sends or stores e-mail with a third-party commercial ISP. The Sixth Circuit provided the proper analysis by looking at Fourth Amendment principles of traditional forms of communication to find a privacy interest in stored e-mail messages. Other circuits and the Supreme Court should follow *Warshak* in order to provide a consistent judicial framework for Congress to timely enact statutes governing the protection of stored e-mail. As society and technology progress, courts and legislative bodies must accept

174. *Id.* at 868–69 ("If the Supreme Court does agree to resolve the case eventually, it is likely to happen several years after the circuit courts have first addressed the issue.").

175. *See* McNerney, *supra* note 163, at 356.

176. *See* United States v. Warshak, 631 F.3d 266, 334–35 (6th Cir. 2010) (Keith, J., concurring) (stating that adoption of the ECPA, which contains the SCA, "was precipitated by concerns about advancements in technology and the desire to protect personal and business information").

177. *See* Kerr, *supra* note 77, at 807–08; McNerney, *supra* note 163, at 356.

that an account holder has a reasonable expectation of privacy in e-mail sent, received, and stored on a third-party server in order to properly protect one of the most commonly used methods of communication. If not, the reasonable expectation of privacy standard could wither and perish. The progress of advancing technologies, such as stored e-mail, must be met with the long-standing privacy standards of the Fourth Amendment in order to ensure individuals are adequately protected against unwarranted governmental intrusions.

*Spencer S. Cady**

* B.A., Drake University, 2009; J.D. Candidate, Drake University Law School, 2013.