Stop Waiting on the World To Change: Compelled Disclosure of Email Content Under the Stored Communications Act

"[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."[1]

I. INTRODUCTION

The Fourth Amendment of the United States Constitution guarantees personal privacy by limiting the government's ability to conduct searches and seizures in the absence of probable cause.[2] When the government believes that an individual has been involved in criminal activity, a search warrant must be obtained from a judge before a search is conducted.[3] In order to obtain a search warrant, the government must produce evidence that the search will likely reveal the existence of the alleged criminal activity, details concerning the place to be searched, and the things to be seized.[4] In the context of electronic communications, such as email, upholding Fourth Amendment protection has become increasingly complex as the law has been slow to adapt to changes in technology.[5]

The Supreme Court has held that there must be a reasonable expectation of privacy for information to be protected by the Fourth Amendment.[6] To date, the Supreme Court has not determined whether there is a reasonable expectation of privacy with respect to emails stored by a third-party provider.[7]

---

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

2. *See* U.S. CONST. amend. IV (protecting citizens from "unreasonable searches and seizures"); Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 613-14 (1989) (stating role of Fourth Amendment in safeguarding "privacy, dignity, and security").

3. *See* Nicole Friess, *When Rummaging Goes Digital: Fourth Amendment Particularity and Stored E-Mail Surveillance*, 90 NEB. L. REV. 971, 972 (2012) (describing probable cause requirement).

4. *See id*. (stating requirement includes "both the place to be searched and the things to be seized"). This specificity is known as the particularity requirement. *Id.* The probable cause requirement is closely related to the particularity requirement because "to establish probable cause for the issuance of a warrant, the government must demonstrate the described items are connected with the criminal activity under investigation and the items are to be found in the place to be searched." *Id.* at 985.

5. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide To Amending It*, 72 GEO. WASH. L. REV. 1208, 1208 (2004) (explaining how changes in technology require changing analytical framework).

6. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (articulating reasonable expectation of privacy standard).

7. *See In re* Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts, Nos. 13-MJ-8163-JPO, 13-MJ-8164-DJW, 13-MJ-8165-DJW, 13-MJ-8166-JPO, 13-MJ-8167-DJW, 2013 WL 4647554, at *3 (D. Kan. Aug. 27, 2013) (stating current state of Fourth Amendment jurisprudence

While many federal courts have held that there is an expectation of privacy regarding stored emails, others have used a more traditional Fourth Amendment analysis to argue that this expectation does not exist.[8] In 2010, the Supreme Court acknowledged the challenges of applying the law to changing technology, writing "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[9] The time has come, however, to determine with clarity how the Fourth Amendment applies to search warrants for the contents of an individual's email account.[10]

In addition to case law interpreting the Fourth Amendment, Congress—through the Stored Communications Act (SCA)—has created a statutory framework designed to protect email stored by Internet service providers (ISPs), such as Yahoo! and Google.[11] SCA describes the steps the government must follow to obtain electronically stored information from an ISP.[12] From its inception, this statutory framework has been outdated with respect to email.[13] In particular, ambiguities in the statute have led the government to seek the entire contents of an individual's email account in the absence of probable cause.[14]

regarding emails); *see also* Andrew William Bagley, *Don't Be Evil: The Fourth Amendment in the Age of Google, National Security, and Digital Papers and Effects*, 21 ALB. L.J. SCI. & TECH. 153, 170-71 (2011) (explaining difficulty of applying Fourth Amendment jurisprudence to emails). *See generally* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1006 (2010) (summarizing sparse Fourth Amendment jurisprudence relating to email).

8. *Compare In re Applications for Search Warrants*, 2013 WL 4647554, at *4 (finding reasonable expectation of privacy for personal emails), *and Warshak III*, 631 F.3d 266, 288 (6th Cir. 2010) (stating society should recognize privacy expectation for email accounts), *with* City of Ontario v. Quon, 560 U.S. 746, 764-65 (2010) (declining to find reasonable expectation of privacy in electronic communications when employee used employer's equipment).

9. *City of Ontario*, 560 U.S. at 759.

10. *See Warshak III*, 631 F.3d at 284 (highlighting importance of clarifying Fourth Amendment protections for emails). "This question is one of grave import and enduring consequence, given the prominent role that email has assumed in modern communication." *Id.*

11. *See* Stored Communications Act, § 201, 18 U.S.C. §§ 2701-2711 (2012) (creating statutory framework for privacy rights regarding electronic communications).

12. *See generally* Kerr, *supra* note 5 (providing overview of statutory framework).

13. *See, e.g.*, Simon M. Baker, Seminar Article, *Unfriending the Stored Communications Act: How Technological Advancement and Legislative Inaction Have Rendered Its Protections Obsolete*, 22 DEPAUL J. ART TECH. & INTELL. PROP. L. 75, 110 (2011) (opining statutory framework outdated with respect to modern technology); Courtney M. Bowman, Note, *A Way Forward After Warshak: Fourth Amendment Protections for E-Mail*, 27 BERKELEY TECH. L.J. 809, 825 (2012) (describing outdated nature of statute regarding evolving technology); Sara E. Brown, Note, *An Illusory Expectation of Privacy: The ECPA Is Insufficient To Provide Meaningful Protection for Advanced Communication Tools*, 114 W. VA. L. REV. 277, 289 (2011) (describing need for more clarity in statutory framework); Eric R. Hinz, Notes, *A Distinctionless Distinction: Why the RCS/ECS Distinction in the Stored Communications Act Does Not Work*, 88 NOTRE DAME L. REV. 489, 502-14 (2012) (summarizing conflicting interpretations of statute in case law).

14. *See In re* Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts, Nos. 13-MJ-8163-JPO, 13-MJ-8164-DJW, 13-MJ-8165-DJW, 13-MJ-8166-JPO, 13-MJ-8167-DJW, 2013 WL 4647554, at *7-10 (D. Kan. Aug. 27, 2013) (articulating concerns with scope of statute).

This Note will explore the intermingling of Fourth Amendment jurisprudence with the statutory framework of the SCA.[15] Part II will examine the evolution of Fourth Amendment jurisprudence in connection with changes in technology.[16] It will also describe the existing statutory framework governing stored electronic communications and the procedures the government must follow in order to access the content of an individual's email account.[17] Part III will then analyze the problems with the existing statutory framework, examining cases where the inconsistencies have been particularly clear.[18] In conclusion, this Note will argue that the ability of the government to obtain disclosures of email content from ISPs without probable cause is unconstitutional.[19] Ultimately, it will suggest that both the Supreme Court and Congress have a role to play in bolstering Fourth Amendment protections for email.[20]

II. HISTORY

A. Early Development of Fourth Amendment Analysis

The Fourth Amendment prohibits "unreasonable searches and seizures" and also requires probable cause and specificity in order for a search warrant to be issued.[21] The Bill of Rights includes this provision as a direct response to the

15. *See infra* Parts II, III (describing SCA in context of Fourth Amendment rights).
16. *See infra* Parts II.A, II.B (tracking case law development over time).
17. *See infra* Parts II.C, II.D (explaining and applying statutory framework).
18. *See infra* Part III (analyzing deficiencies in SCA's email protections).
19. *See infra* Part III (arguing process unconstitutional).
20. *See infra* Part III (suggesting need for action).
21. *See* U.S. CONST. amend. IV (providing protection against unreasonable search and seizure). The Fourth Amendment states:

> 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.

Id. The first clause of the Fourth Amendment contains a general protection against searches deemed to be "unreasonable." *See id*. This is generally read as recognizing an "already existing . . . right to freedom from arbitrary governmental invasion of privacy and did not seek to create or confer such a right." *See* JACOB W. LANDYNSKI, SEARCH & SEIZURE AND THE SUPREME COURT: A STUDY IN CONSTITUTIONAL INTERPRETATION 43 (1966). The second clause provides that a search warrant can be obtained when there is probable cause. *See* U.S. CONST. amend. IV. This is generally understood as explaining the type of search that is not "unreasonable," and thus, constitutionally permissible. *See* LANDYNSKI, *supra*, at 43. The warrant must also meet the particularity requirement to "ensure[] that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." Maryland v. Garrison, 480 U.S. 79, 84 (1987). Ultimately, the purpose of the Fourth Amendment is to limit the government's ability to intrude on the lives and privacy of individuals. *See* Nicholas Matlach, Comment, *Who Let the* Katz *Out? How the ECPA and SCA Fail To Apply to Modern Digital Communications and How Returning to the Principles in* Katz v. United States *Will Fix It*, 18 COMMLAW CONSPECTUS 421, 422 (2010) (stating primary purpose of Fourth Amendment).

arbitrary and invasive searches that commonly occurred in the American colonies prior to the Revolutionary War.[22] These overbearing searches were a significant source of resentment and conflict between the colonists and the British.[23] As a result, many states included specific protections against unreasonable searches and seizures in their constitutions.[24] When the Bill of Rights was ultimately ratified in 1791, it was interpreted as codifying an already existing protection against unreasonable searches and seizures.[25]

The language of the Fourth Amendment focuses on searches and seizures carried out by physical intrusions—the same types of intrusions that British soldiers had imposed on the colonists.[26] The Fourth Amendment, however, does not expressly address how its protections apply beyond the context of a physical search.[27] For this reason, Fourth Amendment jurisprudence has focused on identifying when a warrant is necessary, which types of information should be protected, and how to best guarantee the protection is enforced.[28] To resolve these issues, courts have applied a broadened framework to reflect

22. *See* Weeks v. United States, 232 U.S. 383, 390 (1914) (noting Framers sought to protect against unreasonable searches and seizures experienced in colonies), *overruled in part by* Mapp v. Ohio, 367 U.S. 643 (1961); *In re* Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts, Nos. 13-MJ-8163-JPO, 13-MJ-8164-DJW, 13-MJ-8165-DJW, 13-MJ-8166-JPO, 13-MJ-8167-DJW, 2013 WL 4647554, at *3 (D. Kan. Aug. 27, 2013) (recalling goal of Fourth Amendment to prevent arbitrary searches); Commonwealth v. Dana, 43 Mass. (2 Met.) 329, 334-36 (1841) (framing Fourth Amendment analysis in context of arbitrary searches Framers resented); *see also* LANDYNSKI, *supra* note 21, at 20 (showing Fourth Amendment responded to past abuses); Fabio Arcila, Jr., *In the Trenches: Searches and the Misunderstood Common-Law History of Suspicion and Probable Cause*, 10 U. PA. J. CONST. L. 1, 10 (2007) (stating colonial disputes with British authority over searches motivated Fourth Amendment protections). In the years leading up to the Revolutionary War, it became common practice for British officers to invade the private property of the American colonists in order to conduct searches and look for evidence of crime. *See* Olmstead v. United States, 277 U.S. 438, 463 (1928) (recounting historical backdrop of Fourth Amendment), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

23. *See* LANDYNSKI, *supra* note 21, at 37-38 (citing searches by British soldiers as source of tension). Following the outbreak of the Revolutionary War, the colonists included the following complaint in a formal petition to the British Crown: "The officers of the customs are empowered to break open and enter houses, without the authority of any civil magistrate, founded on legal information." *Id*. at 38. The colonists were particularly frustrated by the British officers' broad power to conduct searches for smuggled goods through the issuance of writs of assistance. *See id.* at 32-33; *see also* Alexander Scolnik, Note, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 352 (2009) (stating Framers sought to address concerns regarding writs of assistance and general warrants).

24. *See* LANDYNSKI, *supra* note 21, at 20 (noting states incorporated search and seizure protections in constitutions). Virginia was the first state to formalize its opposition to excessive searches in Article X of its Declaration of Rights. *See id.* at 38. By 1784, Pennsylvania, Maryland, Massachusetts, North Carolina, and New Hampshire had adopted similar protections in their own constitutions. *See id.*

25. *See id.* at 43 (demonstrating right already existed). As the Supreme Court has acknowledged, "[t]he maxim that every man's house is his castle" has long been entrenched in the ideology of the United States. *See Weeks*, 232 U.S. at 390 (internal quotation marks omitted).

26. *See* LANDYNSKI, *supra* note 21, at 15 (explaining physical nature of searches Framers resented).

27. *See* Scolnik, *supra* note 23, at 351 (opining Framers could not have anticipated future of electronic communications).

28. *See generally* Kerr, *supra* note 5 (summarizing Fourth Amendment jurisprudence).

changes in society, technology, and conceptions of the right to privacy.[29]

Significant progress in interpreting the Fourth Amendment did not occur until the late 1800s and early 1900s.[30] *Boyd v. United States*,[31] an 1886 Supreme Court case, is the Court's first articulation of a framework for Fourth Amendment analysis.[32] In *Boyd*, the trial court ordered the defendant to produce an invoice from his home, which was used as evidence against him in a trial for charges of fraud and forfeiture.[33] Although this compulsory production did not constitute a physical search and seizure, the Supreme Court held that forcing Boyd to produce these documents violated his Fourth Amendment rights because it unreasonably intruded on the privacy of his personal papers.[34] The *Boyd* decision opened the doors to interpretations of unreasonable searches beyond physical intrusions on an individual's property.[35] For instance, in 1877, the Supreme Court applied a similarly broad interpretation of the Fourth Amendment to suggest the existence of a privacy right protecting documents outside the physical boundaries of an individual's home.[36]

In the years following *Boyd*, the Supreme Court also addressed the issue of whether evidence obtained unconstitutionally could be admissible against a criminal defendant.[37] The Supreme Court's 1914 decision of *Weeks v. United*

29. *See* David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles To Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2206 (2009) (acknowledging slow evolution of Fourth Amendment jurisprudence due to changing technology).

30. *See* LANDYNSKI, *supra* note 21, at 49 (stating Fourth Amendment remained unexplored for many years).

31. 116 U.S. 616 (1886).

32. *See* Arcila, *supra* note 22, at 5 n.12 (noting lack of Fourth Amendment jurisprudence before *Boyd*).

33. *See Boyd*, 116 U.S. at 618 (describing trial court's order to produce invoice of glass purchases).

34. *See id.* at 638 (holding ordered production of evidence against defendant unconstitutional). Writing for the majority, Justice Bradley stated:

> The search for and seizure of stolen or forfeited goods, or goods liable to duties and concealed to avoid the payment thereof, are totally different things from a search for and seizure of a man's private books and papers for the purpose of obtaining information therein contained, or of using them as evidence against him.

Id. at 623. While the former is permissible, the latter type of search is unreasonable because it compels an individual to give evidence against himself in violation of the Fifth Amendment. *See id.* at 633-34.

35. *See id.* at 630 (discussing importance of privacy rights). "It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property . . . ." *Id.*

36. *See Ex Parte* Jackson, 96 U.S. 727, 733 (1877) (holding search of sealed mail without warrant unconstitutional); *see also* Steven R. Morrison, *What the Cops Can't Do, Internet Service Providers Can: Preserving Privacy in Email Contents*, 16 VA. J.L. & TECH. 253, 281 (2011) (expanding on privacy protection for mail). The Court reasoned in *Ex Parte Jackson* that the Fourth Amendment protects an individual's papers "wherever they may be," including in the mail. *See* 96 U.S. at 733.

37. *See* LANDYNSKI, *supra* note 21, at 62-64 (tracing historical background to understand exclusionary rule).

States[38] represents a fundamental shift in Fourth Amendment jurisprudence, as the Court codified the "exclusionary rule."[39] In *Weeks*, the defendant's house was searched and his papers seized without either his permission or a search warrant.[40] The papers were then entered into evidence and used against the defendant at trial.[41] The Supreme Court found this practice to be a violation of the defendant's Fourth Amendment rights and held that the trial court should have returned the papers to Weeks because they had been unconstitutionally obtained.[42] This outcome bolstered the power of the Fourth Amendment because the government could no longer use unconstitutionally obtained evidence against a criminal defendant at trial.[43]

Despite the Supreme Court's elaborations on the meaning of the Fourth Amendment, applying Fourth Amendment protections has been particularly difficult with the advent of modern technology.[44] In the 1928 case *Olmstead v.*

38. 232 U.S. 383 (1914), *overruled in part by* Mapp v. Ohio, 367 U.S. 643 (1961).

39. *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 527 (2007) (noting exclusionary rule as primary Fourth Amendment remedy); Ryan A. Ray, *The Warrantless Interception of E-Mail: Fourth Amendment Search or Free Rein for the Police?*, 36 RUTGERS COMPUTER & TECH. L.J. 178, 184-85 (2010) (describing origins of exclusionary rule).

40. *See Weeks*, 232 U.S. at 386-87 (describing search of defendant's room without authorization).

41. *See id.* at 389, 393 (explaining law enforcement's retention and placement into evidence of defendant's letters).

42. *See id.* at 398 (stating defendant's papers should have been returned). The Supreme Court reasoned:

> If letters and private documents can thus be seized and held and used in evidence against a citizen accused of an offense, the protection of the 4th Amendment, declaring his right to be secure against such searches and seizures, is of no value, and, so far as those thus placed are concerned, might as well be stricken from the Constitution.

Id. at 393.

43. *See id*. at 398 (concluding illegally obtained evidence inadmissible). Prior to the *Weeks* decision it had been common practice to allow the use of illegally obtained evidence at trial. *See id.* at 394-97 (listing cases where courts admitted similar evidence). Courts had generally reasoned that the papers were now under the "control of the court" such that "it would not inquire into the manner in which they were obtained, but, if competent, would keep them and permit their use in evidence." *See id.* at 394. This practice was explained by the Supreme Judicial Court of Massachusetts:

> If the search warrant were illegal, or if the officer serving the warrant exceeded his authority, the party on whose complaint the warrant issued, or the officer, would be responsible for the wrong done; but this is no good reason for excluding the papers seized as evidence, if they were pertinent to the issue . . . . When papers are offered in evidence, the court can take no notice how they were obtained, whether lawfully or unlawfully; nor would they form a collateral issue to determine that question.

Commonwealth v. Dana, 43 Mass. (2 Met.) 329, 337 (1841). Ultimately, without the recognition of the exclusionary rule by the Supreme Court in *Weeks*, "the protection of the Fourth Amendment would be much impaired." *See* Olmstead v. United States, 277 U.S. 438, 463 (1928) (explaining significance of *Weeks* decision), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

44. *See* Matlach, *supra* note 21, at 425 (identifying difficulties in applying Fourth Amendment to changing technology).

United States,[45] the Supreme Court was presented with its first case of wiretapping.[46] The defendant was charged as the leading conspirator and general manager of a business that imported and sold liquor in violation of the National Prohibition Act.[47] The evidence that led to the discovery of this illegal operation was primarily obtained through the use of wiretaps.[48] Law enforcement did not trespass on the defendant's property while setting the wiretaps.[49] The Court held that there was no violation of the defendant's Fourth Amendment rights because there had not been a physical trespass onto the defendant's property, and thus, the evidence was admissible at trial.[50] The framework that emerged from *Olmstead* required courts to consider whether or not a trespass had occurred on an individual's property when law enforcement searched for and seized evidence.[51]

B. Shifting Fourth Amendment Analysis: Reasonable Expectation of Privacy Standard

While Fourth Amendment analysis based on physical trespass predominated Fourth Amendment jurisprudence for a number of years, such reliance was not without criticism.[52] In fact, one of the most notable critiques of this framework came from Justice Brandeis's dissenting opinion in *Olmstead*.[53] Justice Brandeis argued that the Fourth Amendment must protect against "every unjustifiable intrusion by the government upon the privacy of the individual," even in the absence of physical trespass.[54] This dissenting opinion reflects a fear that changes in technology over time would give law enforcement new ways to obtain information assumed to be private without physical trespass into

45. 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

46. *See* LANDYNSKI, *supra* note 21, at 200 (stating *Olmstead* was Supreme Court's first wiretapping decision).

47. *See Olmstead*, 277 U.S. at 455-56 (describing charges against Olmstead).

48. *See id.* at 456-57 (stating small wires inserted in telephone line to create wiretap).

49. *See id.* at 457 (explaining agents set up wiretap using basement of nearby business building and street telephone lines).

50. *See id.* at 466 (classifying wiretap as constitutional because no physical entry onto defendant's property). The Court explained that searches are constitutional "unless there has been an official search and seizure of [the defendant's] 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." *Id*. Here, the wiretaps had been set from outside the defendant's house. *See id.* at 457. Thus, the Court reasoned that the defendant's Fourth Amendment rights had not been violated. *See id.* at 466.

51. *See* LANDYNSKI, *supra* note 21, at 201-02 (describing impact of *Olmstead* decision).

52. *See* Scolnik, *supra* note 23, at 363 (describing public concern as wiretapping increased in wake of *Olmstead*).

53. *See* Olmstead v. United States, 277 U.S. 438, 471-85 (1928) (Brandeis, J., dissenting) (disagreeing with majority), *overruled by* Kats v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

54. *See id.* at 478 (arguing for expansive Fourth Amendment protections).

the home.[55] For this reason, Justice Brandeis suggested that the Court's analysis should focus on the need to protect privacy rights against every unjustifiable intrusion, regardless of the method employed.[56]

Justice Brandeis's dissent was predictive of the future evolution of Fourth Amendment case law, as this reasoning was adopted by the Supreme Court's decision in *Katz v. United States*[57] nearly forty years later.[58] In *Katz*, law enforcement sought to introduce evidence regarding telephone conversations overheard by government agents who had attached an electronic listening device to the outside of a telephone booth in order to overhear the defendant's conversations.[59] The Court held that this practice violated the defendant's Fourth Amendment rights and any evidence obtained by such practice could not be used at trial.[60] The *Katz* decision directly overruled *Olmstead* and the Court articulated a new framework for evaluating Fourth Amendment rights based on the notion that the "Fourth Amendment protects people, not places."[61] The test established by *Katz* created a two-step inquiry to be used in Fourth Amendment cases: The first step asks whether the individual manifested a subjective expectation of privacy in the challenged search; and the second step considers whether society is willing to recognize the expectation as reasonable.[62] Thus, *Katz* significantly expanded privacy protections under the

55. *See id.* at 474 (predicting new methods of government espionage); *see also* Robert A. Pikowsky, *The Need for Revisions to the Law of Wiretapping and Interception of Email*, 10 MICH. TELECOMM. & TECH. L. REV. 1, 93 (2003) (stating accuracy of Brandeis's dissenting opinion); Matthew A. Piekarski, Note, *E-Mail Content's Brush with the Reasonable Expectation of Privacy: The* Warshak *Decision*, 47 U. LOUISVILLE L. REV. 771, 773 (2009) (reflecting on foresight of Brandeis's dissenting opinion).

56. *See Olmstead*, 277 U.S. at 477-80 (reflecting on significance of right to privacy). Justice Brandeis reasoned that the Framers "sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations." *Id.* at 478. For this reason:

> They conferred, as against the government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men. To protect, that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.

Id.

57. 389 U.S. 347 (1967).

58. *See* Piekarski, *supra* note 55, at 774 (describing *Katz*'s adoption of reasoning from Brandeis's dissent in *Olmstead*).

59. *See Katz*, 389 U.S. at 348 (describing facts of case).

60. *See id.* at 353 (overturning *Olmstead* by stating eavesdropping constitutes search and seizure). Law enforcement needed to obtain a search warrant in order to conduct surveillance in this manner. *See* Piekarski, *supra* note 55, 774-75 (stating need for search warrant).

61. *See Katz*, 389 U.S. at 351 (applying Fourth Amendment outside property-rights framework); Scolnik, *supra* note 23, at 363 (comparing *Olmstead* holding with *Katz* holding).

62. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring) (summarizing test for Fourth Amendment protection). In determining whether a reasonable expectation of privacy exists, the Supreme Court has previously considered factors, including "the Framers' intent, the ground upon which the search was conducted, societal understandings and the individual's use of the thing seized." Erin E. Wright, Note, *The Right to Privacy in Electronic Communications: Current Fourth Amendment and Statutory Protection in the Wake of*

Fourth Amendment and is the standard courts continue to apply today.[63]

While the *Katz* decision added an element of flexibility to interpretations of privacy rights, the Court also noted that sharing private information with a third party destroys the privacy expectation.[64] This limitation has been developed in case law since *Katz* and is referred to as the "third-party doctrine."[65] The third-party doctrine has most notably led the Supreme Court to justify using pen registers to monitor telephone call histories, deploying secret informants to obtain information while undercover, and accessing an individual's bank records.[66] In each of these cases, the Supreme Court reasoned that any expectation of privacy is relinquished when private information is turned over to a third party, such that no search warrant was required to carry out a search and seizure.[67] More recently, the third-party doctrine has been applied in the context of email, leading commentators to suggest that there cannot be a reasonable expectation of privacy for email because it is inevitably shared with an ISP.[68] Applying a strict interpretation of the third-party doctrine would mean that there could never be Fourth Amendment protections for email

Warshak v. United States, 3 I/S: J. L. & POL'Y FOR INFO. SOC'Y 531, 536 (2008) (footnotes omitted) (listing factors weighed in evaluating privacy interest).

63. *See, e.g.*, David S. Barnhill, Notes, *Cloud Computing and Stored Communications: Another Look at* Quon v. Arch Wireless, 25 BERKELEY TECH. L.J. 621, 624 (2010) (explaining *Katz* opened door to broader privacy rights); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1577 (2004) (describing expansive impact of *Katz*); Scolnik, *supra* note 23, at 353-54 (characterizing *Katz* test as flexible).

64. *See* Katz v. United States, 389 U.S. 347, 351 (1967) (stating exception); *see also* Couillard, *supra* note 29, at 2213-14 (noting third-party exception mentioned in *Katz*); Scolnik, *supra* note 23, at 354 (stating *Katz* affirmed lack of privacy expectation where items are exposed voluntarily to public view). The *Katz* decision notes: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Katz*, 389 U.S. at 351.

65. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563-64 (2009) (describing third-party doctrine); *see also* Jay P. Kesan et al., *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH. & LEE L. REV. 341, 411 (2013) (explaining relevance of third-party doctrine to online privacy analysis); Barnhill, *supra* note 63, at 627-28 (explaining applications of third-party doctrine). The third-party doctrine is the simple notion that "[b]y disclosing to a third party, the subject gives up all of his Fourth Amendment rights in the information revealed." Kerr, *supra*, at 563. While the Fourth Amendment protects the "security a man relies upon when he places himself or his property within a constitutionally protected area, be it his home or his office, his hotel room or his automobile . . . [a]nd when he puts something in his filing cabinet, in his desk drawer, or in his pocket," it does not protect information that has been knowingly shared with a third party. Hoffa v. United States, 385 U.S. 293, 301 (1966) (describing meaning of third-party exception).

66. *See* Smith v. Maryland, 442 U.S. 735, 745 (1979) (stating caller assumed risk of telephone company disclosing call history); *Hoffa*, 385 U.S. at 302 (holding defendant's privacy not violated solely because he misplaced confidence in informant); *see also* United States v. Miller, 425 U.S. 435, 442 (1976) (explaining deposit slips and bank records not private because of voluntarily disclosure to bank).

67. *See* Scolnik, *supra* note 23, at 355-59 (explaining Supreme Court holdings in *Smith*, *Hoffa*, and *Miller*).

68. William Jeremy Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1226-27 (2010) (noting difficulty of applying third-party doctrine in context of internet privacy).

content.[69]

C. *Statutory Paradigm Following* Katz

Shortly after the Supreme Court held in *Katz* that wiretapping implicated Fourth Amendment rights, Congress passed the Federal Wiretap Act in 1968.[70] The Federal Wiretap Act addressed the difficulties of applying Fourth Amendment protections to changes in technology by explicitly making unauthorized wiretapping and electronic eavesdropping a federal crime.[71] More specifically, the statute included language protecting "any wire, oral, or electronic communication."[72] Over time, however, this language became outdated as courts struggled to apply the law to new technologies that went beyond wire or oral communications.[73]

Establishing a statute that stands up to evolving technology is difficult.[74] Congress attempted to do so in 1986 by enacting the Electronic Communications Privacy Act (ECPA), which updated and extended the privacy protections of the Federal Wiretap Act.[75] Title II of the ECPA encompasses the SCA, which provides protections for electronic communications once such communications have been sent.[76] The SCA sets forth the relevant framework

69. *See generally* Scolnik, *supra* note 23 (discussing third-party doctrine's implications on email privacy).

70. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, Title III, 82 Stat. 197, 211-25 (codified as amended at 18 U.S.C. §§ 2510-2520); *see also* Pikowsky, *supra* note 55, at 31-33 (stating history of Federal Wiretap Act). In drafting the Federal Wiretap Act, Congress was careful to maintain a balance with existing Supreme Court decisions, such as *Katz*. *See* Pikowsky, *supra* note 55, at 32. The legality of wiretapping thus became governed by the Federal Wiretap Act. *Id.*

71. *See* Charles H. Kennedy, *An ECPA for the 21st Century: The Present Reform Efforts and Beyond*, 20 COMMLAW CONSPECTUS 129, 131-32 (2011) (summarizing impact of Act); Pikowsky, *supra* note 55, at 31-32 (describing motivation for congressional action). "By the time of *Katz* and *Berger*, it was generally agreed that the prohibition against interception and divulgence of telephone conversations as mandated by [existing law] needed to be reassessed." Pikowsky, *supra* note 55, at 31.

72. 18 U.S.C. § 2511 (2012) (stating federal law).

73. *See* Kennedy, *supra* note 71, at 132-33 (describing new technologies developing after Federal Wiretap Act enacted); Pikowsky, *supra* note 55, at 35-37 (explaining difficulties of applying old definition). For example, the Ninth Circuit determined the Federal Wiretap Act required one side of a conversation to take place over a wire telephone—as opposed to a conversation between two cellphones—in order to be considered a wire communication under the statute. *See* United States v. Hall, 488 F.2d 193, 198-99 (9th Cir. 1973) (determining conversation between two cellphones not protected unless parties had reasonable expectation of privacy).

74. *See* Kennedy, *supra* note 71, at 134 (describing difficulties of creating statute to protect Fourth Amendment rights); Robison, *supra* note 68, at 1227 (detailing complications of maintaining Fourth Amendment rights for internet users while following Supreme Court jurisprudence).

75. *See* Kennedy, *supra* note 71, at 132-33 (outlining Congress's response to technological changes); Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 375 (2014) (explaining history of statute); Pikowsky, *supra* note 55, at 39 (explaining ECPA amended and expanded Federal Wiretap Act).

76. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, §§ 201-202, 100 Stat. 1848, 1860-68 (codified as amended at 18 U.S.C. §§ 2701-2711) (setting forth protections for stored electronic communications); *see also* Kerr, *supra* note 75, at 375 (noting ECPA has regulated Internet privacy "for over a

to apply when analyzing privacy protections for an individual's email account.[77]

The SCA enacted three primary sections, each incorporating definitions from Title I of the ECPA.[78] First, § 2701 defines the crime of accessing stored communications without authorization.[79] Under this section, it is a federal crime to "intentionally access[] without authorization a facility through which an electronic communication service is provided" or to "intentionally exceed[] an authorization to access that facility" and, in this process, to "obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage."[80] The term "electronic storage" is defined as encompassing "any temporary, intermediate storage of a wire or electronic communication *incidental* to the electronic transmission thereof" or "any storage of such communication by an electronic communication service for purposes of *backup protection*."[81] Courts differ in their interpretations of what constitutes electronic storage because this definition is ambiguous.[82] In particular, courts are divided regarding whether an email that has already been opened by its recipient can still be considered in "electronic storage" based on the reasoning that it is being stored for purposes of "backup protection."[83]

Second, § 2702 regulates voluntary disclosure by an ISP of the contents of stored communications.[84] Under this section, an ISP is not generally permitted to disclose the contents of an electronic communication with any person or entity.[85] The statute includes a narrow exception to this basic principle, allowing a provider to "divulge the contents of a communication" in the event

quarter century"). While Title II regulates stored communications, Title I protects electronic communications from being intercepted during transmission. *See* Electronic Communications Privacy Act of 1968, Pub. L. No. 99-508, §§ 101-111, 100 Stat. 1848, 1848-60 (codified as amended at 18 U.S.C. §§ 2510-2522) (outlining federal prohibition against intercepting electronic communications). The "interception" of electronic communications has been interpreted as the instantaneous acquisition of materials as they are being transmitted. *See* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003) (defining "intercept" for purposes of ECPA).

77. *See infra* notes 78-106 and accompanying text (outlining statutory framework and judicial interpretation of privacy protections for individual's emails).

78. *See* 18 U.S.C. §§ 2701-03 (2012); Kennedy, *supra* note 71, at 136 (summarizing structure of SCA).

79. *See* 18 U.S.C. § 2701 (setting forth federal crime regarding accessing electronic communications).

80. *See id.* § 2701(a) (codifying unauthorized access to electronic communications as illegal).

81. *See id.* § 2510(17) (emphasis added) (defining "electronic storage" for ECPA).

82. *See* Kerr, *supra* note 5, at 1216-17 (describing differing definitions of electronic storage).

83. *Compare* Theofel v. Farey-Jones, 359 F.3d 1066, 1076 (9th Cir. 2003) (classifying emails stored within internet provider as backup protection), *and* Cheng v. Romo, No. 11-10007-DJC, 2013 WL 6814691, at *3 (D. Mass. Dec. 20, 2013) (holding as backup copies emails stored in individual's Yahoo! account), *with* United States v. Weaver, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009) (finding previously opened email stored on web-based server not in backup storage), *and* Jennings v. Jennings, 736 S.E.2d 242, 245 (S.C. 2012) (holding previously opened email stored with Yahoo! does not constitute backup copy).

84. *See* 18 U.S.C. § 2702 (2012) (stating procedure for voluntary disclosure of content of customer records).

85. *Id.* § 2702(a) (stating electronic communications should not be divulged).

of an emergency or to prevent the commission of a crime.[86]

Lastly, § 2703 regulates the procedure by which the government can compel the disclosure of electronic communications that an ISP stores.[87] Compelled disclosure means that the government can force an ISP to turn over the content of a user's email account.[88] Section 2703 classifies an ISP as either an electronic communication service (ECS) or a remote computing service (RCS).[89] The distinction between ECS and RCS depends on the manner in which the ISP transmits a particular communication.[90] An ECS includes any service that provides users the ability to send and receive electronic communications.[91] In contrast, an RCS provides users with storage for electronic communications or processing services.[92]

The requirements for compelled disclosure differ under § 2703 depending on how long the information has been stored and whether the ISP acted as an ECS or RCS.[93] The greatest level of protection is afforded to information stored by an ECS for less than 180 days.[94] To compel disclosure under these circumstances, the government must obtain a search warrant.[95] In comparison, there are a few different methods the government can use to compel disclosure of electronic communications stored by an ECS for more than 180 days or stored by an RCS for any length of time.[96] The government can first gain access to this information by obtaining a search warrant.[97] Next, the

86. *Id.* § 2702 (b)-(d) (providing exceptions to general rule against content disclosures).

87. *See id.* § 2703 (describing process for mandatory disclosure of content of customer records).

88. *See* Kerr, *supra* note 5, at 1224-25 (summarizing statutory provision for compelled disclosure).

89. *See* 18 U.S.C. § 2703 (a)-(b) (drawing distinction between ECS and RCS); Kerr, *supra* note 5, at 1213-28 (providing clear explanation of ECS and RCS).

90. *See* Kerr, *supra* note 75, at 383-85 (describing rationale for ECS and RCS classifications); Achal Oza, Note, *Amend the ECPA: Fourth Amendment Protection Erodes as E-Mails Get Dusty*, 88 B.U. L. REV. 1043, 1045 (2008) (acknowledging distinction rooted in 1980s computer technology); Robison, *supra* note 68, at 1226-27 (placing ECS and RCS distinction in context of existing technology). "The ECPA reflects the technology of the 1980s: most e-mail users routinely downloaded their messages to a home computer and would never have considered permanently storing messages with their service provider." Oza, *supra*, at 1045. Determining whether an ISP is an ECS or RCS is not based on their "abstract" role to the subscriber. *See* Kerr, *supra* note 5, at 1215. Rather, the classification is based on how the provider acts regarding the specific electronic communication at issue. *See id.* At the time ECPA was enacted, this distinction separated individual email users (ECS) and business email users (RCS). *See* Kerr, *supra* note 75, at 383.

91. *See* Kerr, *supra* note 5, at 1214 (elaborating on meaning of ECS).

92. *See id.*

93. *See* 18 U.S.C. § 2703 (a)-(b) (2012) (distinguishing compelled disclosure procedures between ECS and RCS); Kennedy, *supra* note 71, at 150-51 (stating role of ECS and RCS distinction). The determination of whether an Internet provider is an ECS or RCS provides the central framework for determining how difficult it will be for the government to compel disclosure. *See* Kennedy, *supra* note 71, at 150-51.

94. *See* Kerr, *supra* note 75, at 385 (explaining unopened emails stored with ECS for less than 180 days have full warrant protection).

95. *See* Kerr, *supra* note 75, at 384 (explaining protection provided for unopened emails stored with ECS for less than 180 days). *Compare* 18 U.S.C. § 2703(a) (requiring probable cause search warrant to compel disclosure), *with* § 2703(b) (requiring search warrant, administrative subpoena, *or* court order).

96. *See* Kerr, *supra* note 5, at 1218-20 (explaining government's options to obtain documents).

97. *See* 18 U.S.C. § 2703(b)(1)(A) (allowing access to content of electronic communication with search

government can compel disclosure of email content by obtaining an administrative subpoena without probable cause and providing notice to the customer.[98] Finally, the government can obtain a court order for the disclosure "if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation."[99] The government must also provide notice to the customer when compelling disclosure using a court order.[100]

The SCA also provides the government with the ability to delay giving notice to the customer.[101] This means that the government can avoid providing immediate notice to a subscriber that is otherwise required when the government compels disclosure using a subpoena or a court order.[102] In practice, this means that emails can be seized by the government with a subpoena or court order without either providing immediate notice to the user or a search warrant.[103] When this procedure is used, the government will not

warrant).

98. *See* § 2703(b)(1)(B)(i) (allowing "use[] [of] an administrative subpoena" to obtain communication); Kerr, *supra* note 5, at 1218-19 (describing need for subpoena to compel disclosure). While a search warrant can only be issued by a judge upon a finding of probable cause, a subpoena can be obtained with less scrutiny. *See* Kerr, *supra* note 5, at 1211-12. This means that the content of emails can be obtained from the ISP by court order, and the ISP will be compelled to disclose the information. *See id.* There is no probable cause required in order to obtain this subpoena. *See id.*

99. *See* 18 U.S.C. § 2703(d) (2012) (describing requirement to obtain court order); § 2703(b)(1)(B)(ii) (stating court may order disclosure); Kerr, *supra* note 75, at 385 (explaining court order requirements reflect reasonable suspicion standard); *see also* Oza, *supra* note 90, at 1044-45 (noting email can be read without probable cause after 180 days).

100. *See* 18 U.S.C. § 2703(b)(1)(B) (discussing requirement of notice).

101. *See id.* § 2705 (providing rules for delaying notice). The statute provides that notice to a subscriber may be delayed by no more than ninety days in the following circumstances:

> (A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or
>
> (B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

Id. The statute continues by listing the situations that qualify as adverse results. *See id.*

102. *See id*. (allowing government to delay providing notice).

103. *See* Kennedy, *supra* note 71, at 151 (describing lesser protection of information stored on RCS than ECS).

> ECPA's lesser level of protection for information stored on RCSs threatens to disincentivize businesses and individuals from migrating to cloud computing applications. As ECPA is written, communications stored on an ECS are protected by a probable-cause warrant requirement if they are

have to notify the subscriber for ninety days.[104] In order to delay notice, the government must show that the delay is necessary to prevent "(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."[105] Ultimately, this procedure allows the government to obtain the content of an individual's email in certain circumstances without either a search warrant or providing any notice to that person that his or her privacy rights are being invaded.[106]

D. The Warshak *Decision*

The Sixth Circuit's decisions in the *Warshak* cases provide an illustrative example of the way §§ 2703 and 2705 can be used to compel the disclosure of an individual's email without a showing of probable cause or notice to the subscriber.[107]

In *Warshak*, the government gained access to over 27,000 emails from Warshak's personal account after obtaining a court order pursuant to § 2703 of the SCA.[108] Further, the government utilized § 2705 to delay providing notice to Warshak.[109] The statute provides that notice may only be delayed for up to ninety days, however, Warshak was not told that the government had obtained access to his email for over one year.[110] When Warshak was ultimately informed, he filed for a preliminary injunction to prohibit the government from further using the SCA to obtain copies of his emails without a probable cause

> unopened or stored for less than 180 days. Communications stored on an RCS are never protected by a probable-cause warrant requirement.

Id. (footnotes omitted).

104. *See* 18 U.S.C. § 2705 (outlining ninety day delay); United States v. Hart, No. 08-109-C, 2009 WL 2552347, at *16 (W.D. Ky. Aug. 17, 2009) (stating police obtaining Yahoo! records by subpoena or court order can provide delayed notice).

105. 18 U.S.C. § 2705 (2012) (setting forth reasons government may delay notice of email disclosure).

106. *See* Robison, *supra* note 68, at 1208 n.90 (describing government's ability to delay notification). "Without meaningful guidance from the Supreme Court, lower courts are in disarray with respect to privacy interests in computer networks. Federal courts cannot reach consensus on the privacy protections applicable to e-mail; for instance, a circuit split currently exists over the categorization of e-mail within the Stored Communications Act." *Id.* at 1233.

107. *See* Warshak v. United States (*Warshak II*), 532 F.3d 521 (6th Cir. 2008) (en banc) (second consideration of case); Warshak v. United States (*Warshak I*), 490 F.3d 455 (6th Cir. 2007) (first consideration of case), *rev'd en banc*, 532 F.3d 521 (6th Cir. 2008); Warshak v. United States, No. 1:06-CV-357, 2006 WL 5230332 (S.D. Ohio July 21, 2006) (district court's consideration of case), *aff'd in part*, *vacated in part*, *remanded by*, 490 F.3d 455 (6th Cir. 2007), *rev'd en banc*, 532 F.3d 521 (6th Cir. 2008); *see also Warshak III*, 631 F.3d 266 (6th Cir. 2010) (third consideration of case); Bowman, *supra* note 13, at 826-28 (describing importance of *Warshak* decision).

108. *See Warshak III*, 631 F.3d at 282.

109. *See Warshak*, 2006 WL 5230332, at *1 (noting delayed notice allowed by magistrate judge).

110. *See id.* at *2 (stating Warshak notified more than one year after the disclosure occurred).

warrant.[111] Warshak also argued that the procedure of compelling disclosure and delaying notice was unconstitutional because it violated his Fourth Amendment rights.[112] The district court granted the injunction to prevent the government's use of § 2703, and the government appealed to the Sixth Circuit.[113]

In its first review of the case, the Sixth Circuit affirmed the preliminary injunction to prevent the government from obtaining Warshak's email without a search warrant.[114] The court reasoned that Warshak had a reasonable expectation that the contents of his email communications would be kept private; and thus, his Fourth Amendment rights were violated when the government obtained his emails with less than probable cause.[115] In determining whether a reasonable expectation of privacy existed, the court discussed other traditional forms of communications—such as the letters described in *Ex Parte Jackson*—concluding that there was no reason to treat letters sent in the mail any differently than messages sent online.[116] The court determined that this issue was ripe for judicial review because there was a significant risk that the government would continue its practice of obtaining Warshak's emails without a search warrant.[117]

Shortly after the preliminary junction was affirmed, the Sixth Circuit granted a rehearing en banc and ultimately vacated the preliminary injunction.[118] In a nine-to-three decision, the majority concluded that the issue was not ripe for

111. *See id.* (indicating Warshak's request for preliminary injunction).

112. *See id.* (noting Warshak's claim for Fourth Amendment violation).

113. *See* Warshak v. United States, No. 1:06-CV-357, 2006 WL 5230332, at *8 (S.D. Ohio July 21, 2006) (granting preliminarily injunction), *aff'd in part*, *vacated in part*, *remanded by*, 490 F.3d 455 (6th Cir. 2007), *rev'd en banc*, 532 F.3d 521 (6th Cir. 2008). The court further stated:

> To wit, the Court preliminary holds that 18 U.S.C. subsections §§ 2703(b)(1)(B)(ii), 2703(d) and 2705 violate the Fourth Amendment of the United States Constitution to the extent they collectively authorize the *ex parte* issuance of search and seizure orders without a warrant and on less than a showing of a probable cause.

Id.

114. *See Warshak I*, 490 F.3d 455, 475-76 (6th Cir. 2007) (affirming district court's decision), *rev'd en banc*, 532 F.3d 521 (6th Cir. 2008).

115. *See id*. at 473 (finding reasonable expectation of privacy existed).

116. *See id.* at 471-72 (drawing comparison to protection afforded to letters and bank deposit boxes); *see also Warshak III*, 631 F.3d 266, 285 (6th Cir. 2010) (highlighting similarities between historically protected forms of communication with email); Kesan et al., *supra* note 65, at 412 (commenting on Sixth Circuit's treatment of third-party doctrine). "If we accept that an email is analogous to a letter or a phone call, it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment." *Warshak III*, 631 F.3d at 286 (designating ISP as "functional equivalent" of post office or telephone company).

117. *See Warshak I*, 490 F.3d at 468 (determining issue ripe for judicial review); Scolnik, *supra* note 23, at 385 (noting Sixth Circuit did not declare statute unconstitutional but granted injunction).

118. *See Warshak II*, 532 F.3d 521, 534 (6th Cir. 2008) (en banc) (vacating grant of preliminary injunction); *see also* Scolnik, *supra* note 23, at 385-86 (discussing rehearing en banc).

review because there was no evidence that the government was seeking to obtain Warshak's emails using § 2703 of the SCA.[119] The court also cited the Supreme Court's reluctance "to invalidate statutes on their face under the Fourth Amendment," largely due to its disfavor of challenging statutes based on hypothetical questions to rationalize its decisions.[120] As a result, the Sixth Circuit held the preliminary injunction improper.[121]

Warshak was ultimately convicted of conspiracy to commit mail fraud, bank fraud, and money laundering.[122] Warshak appealed his conviction to the Sixth Circuit, this time arguing that the government's practice of obtaining his emails with less than probable cause—and without providing adequate notice under the SCA—was unconstitutional.[123] Sitting again en banc, the Sixth Circuit agreed that the failure to provide Warshak with notice was unconstitutional.[124] The court did not reverse the district court's decision, however, reasoning that the government had relied in good faith on provisions of the SCA.[125] Thus, Warshak's conviction was affirmed.[126]

III. ANALYSIS

A. Intersection of Fourth Amendment Jurisprudence and the SCA

The goal of the SCA was to ensure that Internet customers would have privacy protections in their electronic communications.[127] When the statute was first enacted, it successfully enhanced privacy protections for Internet users.[128] The expansion of privacy rights under the statute occurred because the Internet was a new form of technology.[129] As discussed above, the Fourth Amendment does not protect against all government searches and seizures.[130] Rather, as the Supreme Court articulated in *Katz*, the Fourth Amendment is implicated where an individual manifests an expectation of privacy and society

119. *See Warshak II*, 532 F.3d at 526 (arguing unfair to assume government will conduct search again).

120. *See id.* at 529.

121. *See id.* at 534 (vacating preliminary injunction).

122. *See Warshak III*, 631 F.3d 266, 281-82 (6th Cir. 2010) (explaining procedural history).

123. *See id.* at 282 (arguing government's warrantless search and seizure of emails under SCA constituted Fourth Amendment violation).

124. *See id*. at 288 (stating government violated Warshak's Fourth Amendment rights). "Therefore, because they did not obtain a warrant, the government agents violated the Fourth Amendment when they obtained the contents of Warshak's emails. Moreover, to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional." *Id.*

125. *Id.* (finding exclusionary rule does not apply); *see also* Illinois v. Krull, 480 U.S. 340, 349-50 (1987) (holding exclusionary rule does not apply where government reasonably relied on statute).

126. *See Warshak III*, 631 F.3d at 333 (affirming conviction).

127. *See* Mulligan, *supra* note 63, at 1597 (describing architects of ECPA as visionaries in privacy protections).

128. *See id.* (explaining original goals of ECPA).

129. *See* Kerr, *supra* note 75, at 386 (noting ECPA was "impressive achievement").

130. *See supra* text accompanying notes 60-63 (discussing Fourth Amendment protections).

is willing to recognize that expectation as reasonable.[131] The enactment of the SCA was important because it increased protections for electronic communications during the early years of the Internet, when there was not yet a reasonable expectation of privacy.[132] As use of the Internet and email have become an integral part of everyday life, however, society's reasonable expectations of privacy have changed.[133]

In the face of rapidly changing technology, the SCA provisions regarding compelled disclosure of electronic communications have become outdated in a number of respects.[134] For instance, the distinction drawn in the statute between ECS and RCS hardly seems relevant today.[135] In fact, many ISPs act both as an ECS and RCS, depending on how they are handling a customer's information.[136] As the distinction is no longer relevant, its continued use is outdated.[137]

Similarly, the SCA does not require particularity, which is problematic today because it is possible to store large quantities of data in an email account.[138]

131. *See supra* Part II.B (stating applicable standard).

132. *See* Kerr, *supra* note 75, at 376-77 (noting ECPA originally functioned as stand-in for Fourth Amendment protections). When the ECPA was enacted, it "presume[d] an absence of Fourth Amendment protection." *See id.* at 390.

133. *See ECPA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 10-12 (2010) (statement of Edward W. Felten, Professor of Computer Science and Public Affairs, Princeton University) (noting changes in technology). Edward Felten described how much technology has changed since the enactment of ECPA:

> In 1986, when ECPA was passed, the Internet consisted of a few thousand computers. . . . There were no web pages, because the web had not been invented. Google would not be founded for another decade. Twitter would not be founded for another two decades. Mark Zuckerberg, who would grow up to start Facebook, was two years old.

Id. at 12. Professor Orin Kerr elaborated on these developments in an article published in early 2014, explaining "[t]he cost of storing a single gigabyte of data has dropped from about eighty-five thousand dollars in 1984 to about five cents in 2011." Kerr, *supra* note 75, at 391. Similarly, in the mid-to-late 1990s free email services generally came with two megabytes of storage space, whereas today similar services, such as Gmail, come with upwards of fifteen gigabytes of storage—"about seventy-five hundred times more storage than was common a decade ago." *See id.* at 392.

134. *See* Kennedy, *supra* note 71, at 161 (stating statute is essentially unusable); Kerr, *supra* note 75, at 386 (discussing outdated "dichotomies" of SCA); *see also* Brown, *supra* note 13, at 305-06 (explaining ECPA must change to fit evolving constitutional interpretation).

135. *See* Kerr, *supra* note 75, at 395-98 (explaining outdated distinction in statute between ECS and RCS).

136. *See* Kerr, *supra* note 5, at 1215 (describing overlapping classification of ISPs); Mulligan, *supra* note 63, at 1568 (noting ISP can act as ECS or RCS). Professor Kerr has observed this nuance, as "[a] provider can act as an RCS with respect to some communications, an ECS with respect to other communications, and neither an RCS nor an ECS with respect to other communications." Kerr, *supra* note 5, at 1215-16.

137. *See* Kerr, *supra* note 5, at 1215 (explaining multifunctional ISPs as difficult to classify). "The distinction between providers of ECS and RCS is made somewhat confusing by the fact that most network service providers are multifunctional. They can act as providers of ECS in some contexts, providers of RCS in other contexts, and as neither in some contexts as well." *Id.*

138. *See* Kerr, *supra* note 75, at 383-84 (describing lack of particularity requirement leading to all-or-

When the government obtains email communications using the procedures of the SCA, there should be a limit imposed on the amount of materials that can be accessed.[139] Finally, and most importantly, allowing any email communications to be accessed by the government under a standard less than probable cause is unconstitutional.[140] Despite these significant deficiencies, the courts and legislature have been reluctant to update the framework for analyzing Internet privacy protections and the time has come to reform the SCA to account for changing technology.[141]

B. A Reasonable Expectation of Privacy for Email Content Should Be Recognized by the Supreme Court

Although the Supreme Court has been applying the two-step inquiry articulated in *Katz* to Fourth Amendment issues for decades, the Court has not yet decided whether there is a reasonable expectation of privacy with regard to the contents of an individual's email account.[142] There is strong evidence that a reasonable expectation of privacy exists regarding email content.[143] This is particularly true in light of the flexibility of the *Katz* test, which allows for

nothing disclosure determinations).

139. *See id.* at 393 (reflecting on large amount of data now stored making access to email more invasive).

140. *See Warshak III*, 631 F.3d 266, 288 (6th Cir. 2010) (compelled disclosures violated defendant's Fourth Amendment rights); *In re* Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts, Nos. 13-MJ-8163-JPO, 13-MJ-8164-DJW, 13-MJ-8165-DJW, 13-MJ-8166-JPO, 13-MJ-8167-DJW, 2013 WL 4647554, at *4 (D. Kan. Aug. 27, 2013) (noting compelled disclosures too expansive).

141. *See* Mulligan, *supra* note 63, at 1572 (stating Congress did not envision current role of technology in society).

142. *See Warshak III*, 631 F.3d at 284 (recalling two-step inquiry in Fourth Amendment cases); *see also* Mulligan, *supra* note 63, at 1577 (explaining *Katz* has dominated Fourth Amendment jurisprudence); Pikowsky, *supra* note 55, at 30 (describing *Katz* as presently accepted standard); Couillard, *supra* note 29, at 2208 (stating current standard). In *Warshak*, the Sixth Circuit explained: "This standard breaks down into two discrete inquiries: 'first, has the [target of the investigation] manifested a subjective expectation of privacy in the object of the challenged search? Second, is society willing to recognize that expectation as reasonable?'" *Warshak III*, 631 F.3d at 284 (alteration in original) (citing California v. Ciraolo, 476 U.S. 207, 211 (1968)) (citations omitted) (internal quotation marks omitted); *see also In re Applications for Search Warrants*, 2013 WL 4647554, at *3 (summarizing lack of Supreme Court jurisprudence on privacy rights related to email); Bagley, *supra* note 7, at 170-71 (explaining challenges of current Fourth Amendment analysis). The difficulties of applying the *Katz* framework include:

> [P]eople are expanding their privacy expectations from the physical confines of their home to that of password-protected accounts for everything from online banking to Internet-based word processing. Users even divulge personal information with an expectation of privacy when conducting search engine queries. However, current case law leaves more questions than answers about the extent of Fourth Amendment protections.

Id.

143. *See In re Applications for Search Warrants*, 2013 WL 4647554, at *3-4 (describing case law and concluding reasonable expectation of privacy exists).

changes in protections based on what society deems reasonable over time.[144] Only the Sixth Circuit has considered the issue directly, concluding that the expectation of privacy does exist.[145]

The third-party doctrine is the most significant obstacle that may prevent the Supreme Court from recognizing a reasonable expectation of privacy for email.[146] Because email content is shared with third parties, such as ISPs, it can be argued that there is no reasonable privacy expectation.[147] This reasoning is not persuasive because of the ubiquitous role of email in modern society.[148]

Although the Supreme Court has not yet addressed this issue, it likely will do so in the near future.[149] The Supreme Court should, and most likely will, recognize this expectation of privacy with regard to the contents of an individual's email account.[150] It is particularly important for the Court to rule on this specific issue because of its implications to the SCA.[151] It is currently easier to justify disclosing email documents with less than probable cause

144. *See* Matlach, *supra* note 21, at 424 (stating changes in conceptions of privacy accounted in flexible *Katz* standard).

145. *See Warshak III*, 631 F.3d at 284 (stating Warshak expected emails would remain private and society should recognize this as reasonable privacy right). In *Warshak*, the government ordered the content of the defendant's email to be copied and saved by the ISP beginning in 2004. *See id.* at 283. The defendant did not become aware that this was going on until 2006. *See id.* At trial, the emails were used as evidence to convict Warshak on a variety of charges, including mail and wire fraud, which resulted in a twenty-five year prison sentence. *See id.* at 281. On appeal, the Sixth Circuit held that there is a reasonable expectation of privacy with respect to the content of an email account, and thus, Warshak's Fourth Amendment rights had been violated. *See id.* at 288. In describing privacy expectations for the content of an email account, the Sixth Circuit opined:

> Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place. 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. Commerce has also taken hold in email. Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointments. In short, 'account' is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life. By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities.

Id. at 284.

146. *See supra* notes 63-69 and accompanying text (discussing third-party doctrine and possible application to emails).

147. *See* Kerr, *supra* note 65, at 563 (explaining third-party doctrine).

148. *See id*. at 563-65 (opining third-party doctrine should not preclude privacy protections for email).

149. *See In re* Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts, Nos. 13-MJ-8163-JPO, 13-MJ-8164-DJW, 13-MJ-8165-DJW, 13-MJ-8166-JPO, 13-MJ-8167-DJW, 2013 WL 4647554, *3-4 (D. Kan. Aug. 27, 2013) (acknowledging lack of Supreme Court guidance on issue).

150. *See* Mulligan, *supra* note 63, at 1585-86 (applying *Katz* framework and suggesting Fourth Amendment protections apply to email).

151. *See In re Applications for Search Warrants*, 2013 WL 4647554, at *7 (noting difficulty of conducting Fourth Amendment analysis).

because courts do not know with certainty whether there are Fourth Amendment implications to searches of email content.[152]

C. Federal Courts Struggle To Apply SCA to Email Disclosures

If the Supreme Court finds that a reasonable expectation of privacy exists in email, the Fourth Amendment analysis will apply.[153] Thus, in order to conduct a search of email, there will have to be probable cause.[154] The provisions of the SCA that allow the government to compel an ISP to disclose email content without obtaining a search warrant create a problem under the Fourth Amendment.[155] The Sixth Circuit's decision in *Warshak* reflects this problem of harmonizing the Fourth Amendment with the SCA.[156] The three opinions the Sixth Circuit wrote in this case demonstrates the challenges courts face in reconciling Fourth Amendment protections with the SCA.[157]

The *Warshak* case reveals the significant confusion about applying the SCA within the boundaries of the Fourth Amendment.[158] In particular, it reflects two key concerns regarding the government's ability under the SCA to mandate disclosure of email content with less than probable cause.[159] It shows the need for the Supreme Court to declare that an individual does have a reasonable expectation of privacy in the contents of their email.[160] Additionally, it shows the need for the legislature to amend this provision of the SCA to prevent information protected by the Fourth Amendment from being obtained with a showing of less than probable cause.[161]

D. Aspects of SCA Must Be Revisited

Similar to the Federal Wiretap Act, the SCA reflects the state of technology

152. *See infra* Part III.D (noting difficulty in applying current SCA framework).

153. *See supra* Part II.B (articulating applicable standard).

154. *See* U.S. CONST. amend. IV (requiring probable cause for search warrants).

155. *See, e.g.*, Kerr, *supra* note 75, at 386-91 (detailing deficiencies of SCA); Couillard, *supra* note 29, at 2211-19 (analyzing leading email privacy cases); Scolnik, *supra* note 23, at 382-87 (discussing lack of privacy protection under SCA).

156. *See supra* Part II.D (detailing Sixth Circuit's consideration of *Warshak* case).

157. *See Warshak III*, 631 F.3d 266 (6th Cir. 2010); *Warshak II*, 532 F.3d 521 (6th Cir. 2008) (en banc); *Warshak I*, 490 F.3d 455 (6th Cir. 2007), *rev'd en banc*, 532 F.3d 521 (6th Cir. 2008); Warshak v. United States, No. 1:06-CV-357, 2006 WL 5230332 (S.D. Ohio July 21, 2006) (District Court's consideration of case), *aff'd in part*, *vacated in part*, *remanded by*, 490 F.3d 455 (6th Cir. 2007), *rev'd en banc*, 532 F.3d 521 (6th Cir. 2008).

158. *See* Scolnik, *supra* note 23, at 386 (noting impact of *Warshak* decisions). "Although the panel's initial decision is no longer in force, its reasoning regarding the underlying constitutional issue is still persuasive. . . . Recognizing that Warshak had a reasonable expectation of privacy in the messages would extend Fourth Amendment protections to them and render § 2703 of the SCA unconstitutional." *Id.*

159. *See supra* Parts III.A, III.B (discussing need for Supreme Court clarification and legislative amendments to SCA).

160. *See supra* Part III.B (detailing need for Supreme Court decision on expectation of privacy in email).

161. *See supra* Part III.A (arguing legislature needs to update SCA).

at the time it was enacted.[162] This makes it difficult to apply the SCA given the changing uses of technology in society.[163] It is time to make changes to this framework as its application to email is outdated.[164] As it stands, allowing the government to use § 2703 of the SCA to compel an ISP to disclose content to the government with less than probable cause appears to be unconstitutional.[165]

The SCA's unconstitutional procedure for compelling email disclosures is particularly problematic because courts will not apply the exclusionary rule where this procedure is used, even if the court believes that a defendant's Fourth Amendment rights have been violated.[166] When a court does not find a reasonable expectation of privacy, an individual's rights are at heightened risk.[167] If there is a reasonable expectation of privacy to email, as this Note has argued, then the provisions in the SCA that allow the government to obtain disclosures with less than probable cause are troubling.[168]

While the Sixth Circuit, as well as the Supreme Court, have had an opportunity to rule on this exact issue, both avoided stating a definitive answer.[169] The Supreme Court must tackle the issue of the SCA head on, as certain federal district court judges have done.[170] As Judge Coffman, of the Western District of Kentucky wrote: "In this age not only of rapidly expanding usage of electronic communications, but also of rapidly expanding mechanisms by which electronic communications can take place, the extent of any Fourth Amendment protection for the contents of emails is not yet a fully-formed area of the law."[171] It is time for the federal courts to clarify the Fourth Amendment rights of email users by holding it unconstitutional for the government to use §

162. *See* Kerr, *supra* note 5, at 1213-14 (reflecting on state of technology at SCA's enactment); Kerr, *supra* note 75, at 378 (opining ECPA hard to understand without looking at 1980s technology); Robison, *supra* note 68, at 1204-05 (explaining SCA is rooted in past understandings of technology). Professor Kerr has insightfully noted that the SCA essentially "[froze] into the law the understandings of computer network use as of 1986." Kerr, *supra* note 5, at 1214. This is particularly clear in the SCA's employment of a distinction between ECS and RCS. *See id.* (explaining ECS and RCS in context of 1980s computer technology).

163. *See* Kennedy, *supra* note 71, at 145-47 (comparing technological advancement prompting enactment of ECPA to situation today); Mulligan, *supra* note 63, at 1558 (noting adequacy of privacy standards questioned due to changing technology). "If anything, the years since ECPA's enactment have seen an even greater number of dramatic, disruptive developments in the technologies and services available to users of electronic communications." Kennedy, *supra* note 71, at 145.

164. *See supra* Part II.D (explaining problem with existing statute).

165. *See* Mulligan, *supra* note 63, at 1584 (noting government can access communication with less than probable cause). "One notable problem arises, however, due to the text of the Stored Communications Act, which permits disclosure not only by warrant, but also by *ex parte* court order, or by administrative subpoena." United States v. Hart, No. 08-109-C, 2009 WL 2552347, at *23 (W.D. Ky. Aug. 17, 2009).

166. *See* Illinois v. Krull, 480 U.S. 340, 349-50 (1987) (holding exclusionary rule does not apply where government reasonably relied on statute).

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

168. *See Hart*, 2009 WL 2552347, at *22-23 (stating the SCA's provisions are likely problematic).

169. *See supra* Part II.D (describing consideration of SCA in *Warshak* and lack of Supreme Court guidance).

170. *See supra* Part III.C (explaining unconstitutionality of § 2703 of SCA).

171. United States v. Hart, No. 08-109-C, 2009 WL 2552347, at *22 (W.D. Ky. Aug. 17, 2009).

2703 of SCA to avoid obtaining a probable-cause warrant.[172]

IV. CONCLUSION

While the SCA at one time provided privacy protections for users of email, it is evident that the law has not kept pace with changes in technology. Individuals now have reasonable expectations that the content of their email will be protected against unreasonable searches and seizures by the government. The SCA, however, allowed the government to compel an ISP to disclose a subscriber's email with less than probable cause because it was created at a time when society was not prepared to recognize a privacy expectation with respect to online communications. While this was permissible when there was not Fourth Amendment protection for email communications, the provision is now unconstitutional. There is now a reasonable expectation of privacy with respect to email content. In order to most effectively rectify the problem, the Supreme Court must explicitly recognize the existence of Fourth Amendment protections for email content. Similarly, the legislature must act to amend the statute and prevent the government from using administrative subpoenas or court orders to compel an ISP to disclose constitutionally protected information.

Joy L. Backer

172. *See supra* Part III.C (describing problems with SCA).