Journal of Business & Technology Law

Volume 4 | Issue 2 Article 9

The Fourth Amendment's New Frontier: Judicial Reasoning Applying the Fourth Amendment to Electronic Communications

Amanda Yellon

AMANDA YELLON*

The Fourth Amendment's New Frontier: Judicial Reasoning Applying the Fourth Amendment to Electronic Communications

INTRODUCTION

OVER THE LAST SEVERAL DECADES, COMMUNICATION technologies have proliferated[1] and the privacy protection afforded to newly emerging types of communication is uncertain.[2] Courts have demonstrated reluctance to apply traditional Fourth Amendment jurisprudence to new communication technologies[3] and statutory protections have not clarified the matter.[4] Undoubtedly, the next "frontier in

---

* J.D., University of Maryland School of Law, May 2009; B.A., Business, University of Maryland, College Park, May 2006.

1. S. REP. No. 99-541, at *2–3 (1986) (noting "tremendous advances in telecommunications and computer technologies"); Steven S. Wildman, *Welcome and Introduction to the Symposium: Second Annual Quello Telecommunications Policy and Law Symposium*, 2001 L. REV. M.S.U.-D.C.L. 217, 217–19 (discussing the "rapid rate of change in communication technolog[y]" and the ramifications of the rapid adoption of changing technology on "communication industries, the economy, and society at large").

2. *See, e.g.*, Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904 (9th Cir. 2008) (noting "[t]he extent to which the Fourth Amendment provides privacy protection for the contents of electronic communications" –such as e-mails, text messages and other means of electronic communication—is as yet "an open question"); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 808 (2004) (stating that "no one knows whether an expectation of privacy in a new technology is 'reasonable'").

3. *See generally* Katz v. United States, 389 U.S. 347 (1967); Tamar R. Gubins, Note, Warshak v. United States: *The* Katz *for Electronic Communications*, 23 BERKELEY TECH. L.J. 723, 724 (2008) (citing generally Daniel J. Solove, *The Coexistence of Privacy and Security: Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 769 (2005)) (noting that courts have demonstrated reluctance to find Fourth Amendment protection for technologies not covered by congressional acts); Kerr, *supra* note 2, at 807–09, (explaining the reluctance of judges to apply the traditional approach which requires consideration of "the importance of privacy" in the technology, "the meaning of 'reasonableness'" and ultimately a normative assessment of whether privacy should exist in the technology).

See also Stephanie Gore, *"A Rose by Any Other Name": Judicial Use of Metaphors for New Technologies*, 2003 J.L. TECH. & POL'Y 403, 408, 415 (noting that a significant number of Americans are "technophobic" and reasoning that if judges are similar to the vast number of Americans, they may be more willing to accept metaphors and analogies for new technologies rather than undertaking the task of understanding whether the metaphors and analogies fit the particular legal question before them); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶ 8 (stating that courts generally avoid or cut short "reasonable expectation of privacy analysis for modern communication because the analysis pushes [judges] beyond their [judicial] competence").

4. *See, e.g.*, Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 633 (E.D. Pa. 2001) (stating that the Electronic Communications Privacy Act ("ECPA") is known for its "lack of clarity"), *aff'd in part, vacated in*

Fourth Amendment jurisprudence" will be in determining privacy rights of users of these new modes of communication.[5]

As users of new communication technologies raise constitutional challenges to government searches and seizures of their e-mails,[6] cell-phone calls,[7] text messages,[8] voice-mail messages, and voice-over-internet protocol (VoIP) communications,[9] courts must address whether the users of such services possess a reasonable expectation of privacy in these communication mediums requiring the government to obtain a probable cause warrant prior to search or seizure.[10] Faced with the daunting prospect of determining what privacy rights exist in the new frontier, some courts have failed to thoroughly analyze new technologies under the traditional *Katz v. United States*[11] framework.[12] Instead, courts have taken refuge in the famil-

---

part, remanded by 352 F.3d 107 (3d Cir. 2004). Courts and academia have grappled with defining the relationship between the Wiretap Act (Title I) and the Stored Communications Act (Title II). *Id.*; *see* Electronic Communications Privacy Act, 18 U.S.C. §§ 2701–2712 (2006).

5. *Quon*, 529 F.3d at 904 (commenting that the application of the Fourth Circuit president to electronic communication remains a frontier that has been little explored).

6. *See* Warshak v. United States, No. 1:06-CV-357, 2006 WL 5230332, at *1 (S.D. Ohio July 21, 2006), *aff'd in part, modified in part*, 490 F.3d 455 (6th Cir. 2007), *reh'g granted en banc*, No. 06-4092, 2007 U.S. App. LEXIS 23741 (6th Cir. Oct 9, 2007), *rev'd en banc*, 532 F.3d 521 (6th Cir. 2008); *see also* United States v. Maxwell, 45 M.J. 406, 416 (C.A.A.F. 1996) (determining "whether appellant has established a reasonable expectation of privacy in the AOL e-mail system").

7. *See, e.g.*, Price v. Turner, 260 F.3d 1144, 1149 (9th Cir. 2001) (holding that the interception of "cordless telephone communications" did not violate the Wiretap Act); United States v. McNulty (In re *Askin*), 47 F.3d at 100, 101, 106 (4th Cir. 1995) (holding that government interception of communications via cordless phone did not violate the Fourth Amendment); Tyler v. Berodt, 877 F.2d 705, 705–07 (8th Cir. 1989) (holding that a neighbor's interception of the plaintiff's cordless phone calls is not a Fourth Amendment violation); United States v. Hoffa, 436 F.2d 1243, 1246–47 (7th Cir. 1970) (finding no reasonable expectation of privacy in Hoffa's cellular telephone calls "which were exposed to everyone in that area who possessed a F.M. radio receiver"). *But see* United States v. Smith, 978 F.2d 171, 180 (5th Cir. 1992) (concluding that as cell phone technology becomes more advanced and the calls become more difficult to intercept, interception may become a Fourth Amendment violation as it would be more reasonable to expect privacy).

8. *Quon*, 529 F.3d at 895.

9. *See* Daniel B. Garrie et al., *Voice Over Internet Protocol and the Wiretap Act: Is Your Conversation Protected?*, 29 SEATTLE U. L. REV. 97, 97 (2005) (noting that the privacy rights assigned to data and voice have been combined with the advent of VoIP communications such that the once clear distinction between protected voice communications and unprotected data communications is now uncertain); James M. O'Neil, *The Impact of VoIP Technology on Fourth Amendment Protections Against Electronic Surveillance*, 12 INTELL. PROP. L. BULL. 35, 42 (2007) (explaining that VoIP communications as they occur are protected by the Wiretap Act, but concluding that the status of stored VoIP communications remains unclear).

10. *See* Stephan K. Bayens, *The Search and Seizure of Computers: Are We Sacrificing Personal Privacy for the Advancement of Technology?*, 48 DRAKE L. REV. 239, 241 (2000) (citing Katz v. United States, 389 U.S. 347, 350–52, 360 (1967)). "[T]he constitutional protections embodied in the Fourth Amendment are only triggered upon a showing of a reasonable expectation of privacy." *Id.*; *see also* Horton v. California, 496 U.S. 128, 133 n.4 (1990) (noting that warrantless searches and seizures are presumptively unreasonable under the Fourth Amendment).

11. 389 U.S. 347 (1967).

12. *See* Freiwald, *supra* note 3, at 8 (explaining that the "reasonable expectation of privacy" pushes judges beyond their competence because it requires analysis of societal views about intricate technologies, and the undertaking of a normative analysis to determine if users should believe such technologies are private); Kerr, *supra* note 2, at 850 (explaining that courts confronted with the question of whether surveillance violated the Fourth Amendment typically rely on the statutory protections of the ECPA and analyze the matter no further).

iar, analogizing the new communication technology to letters,[13] post-cards,[14] and telephone calls.[15] Because long-established jurisprudence holds that reasonable expectations of privacy exist in many of these traditional communication networks, modern courts analogously conclude that the same expectation of privacy therefore exists in electronic communication networks.[16] However, comparative judicial reasoning overlooks important distinctions in the technical operations of electronic communications networks which act to limit the reasonableness of an expectation of privacy.[17] Rather than utilize ill-tailored and ill-suited analogies, *Katz* must be applied to determine whether a reasonable expectation of privacy exists in the new communication networks given the type of information communicated and to whom that information is conveyed.[18]

Although the focus of this Comment will be on the judicial tendency to apply comparative reasoning to different types of mediums, the Comment will primarily use the example case of e-mail communication to illustrate central points. I first examine the current Fourth Amendment doctrine.[19] Next, I discuss comparative reasoning and the judicial tendency to apply comparisons to emerging electronic communication technologies.[20] I then examine the technical operation of e-mail, one type of electronic communication technology,[21] and discuss the propriety of comparisons to postal mail or telephone communications given key technological distinctions between electronic communication networks and traditional communication networks.[22] Given these distinctions, I conduct a *Katz* analysis and conclude that there is generally no reasonable expectation of privacy in electronic communications.[23] Finally, in keeping with a strong judicial commitment to not allow technological advances to erode privacy protections, I propose that the judiciary must act to create an explicit exception to the disclosure principles to develop a

13. *See* United States v. Jacobsen, 466 U.S. 109, 114 (1984) (finding that an individual has an expectation of privacy in sealed packages and letters such that they are entitled to presume U.S. postal service mail carriers or other government agents cannot open the items without obtaining a warrant); *Ex parte* Jackson, 96 U.S. 727, 733 (1877) ("Letters and sealed packages . . . are as fully guarded from examination and inspection . . . as if they were retained by the parties forwarding them in their own domiciles.").

14. *See* United States v. Van Leeuwen, 397 U.S. 249, 251 (1970) (citing *Jackson*, 96 U.S. at 733) (distinguishing protected sealed letters and packages whose contents are shielded from post cards, circulars or other printed matter sent through the mail which are unprotected).

15. *Katz*, 389 U.S. at 353 (finding that a Fourth Amendment expectation of privacy in telephone calls made from a closed telephone booth was violated when the government installed a listening device outside the telephone booth).

16. *See infra* Part II.B.

17. *See infra* Part III.B.

18. *See infra* Part IV.

19. *See infra* Part I.

20. *See infra* Part II.

21. *See infra* Part III.

22. *See infra* Part III.; Freiwald, *supra* note 3, at 7 (discussing how significant differences between telephone and electronic communications makes a straightforward analogy between the networks impractical).

23. *See infra* Part IV.; Freiwald, *supra* note 3, at 7 (concluding that in light of the technical differences between communication networks, courts must apply the *Katz* test anew).

clear doctrine for the development of privacy protections in the new frontier of electronic communications.[24]

I. FOURTH AMENDMENT JURISPRUDENCE

The Fourth Amendment to the Constitution provides the individual with the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" unless a warrant is issued "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[25] The Supreme Court has narrowed the scope of permissible warrantless "search and seizure" from a broad class under a strict textual construction of the Amendment to a substantially narrower category limited to areas in which an individual does not have a "reasonable expectation of privacy."[26]

Since settling on the broad "reasonable expectation of privacy test" enunciated in *Katz*,[27] the Court has continuously chiseled away at the scope of the Amendment's protection through doctrines limiting the reasonableness of an expectation of privacy.[28]

*A. Pre-*Katz*: Trespass Theory and the Development of Fourth Amendment Doctrine*

The Supreme Court's early Fourth Amendment doctrine strictly construed the text of the amendment to protect only against the government's physical trespasses onto the citizen's property, the warrantless search of tangible personal property, or the warrantless seizure of the person.[29] This interpretation provided scant protection to citizens, protecting only against physical trespasses onto constitutionally protected spaces, such as the home or curtilage, and seizure of the person or their tangible property such as "papers . . . and effects."[30]

---

24. *See infra* Part V.

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

26. *See generally* Robert S. Steere, Note, *Keeping "Private E-Mail" Private: A Proposal to Modify the Electronic Communications Privacy Act*, 33 VAL. U. L. REV. 231, 236–43 (1998) (summarizing the development of modern Fourth Amendment doctrine).

27. Stephen P. Jones, *Reasonable Expectations of Privacy: Searches, Seizures, and the Concept of Fourth Amendment Standing*, 27 U. MEM. L. REV. 907, 914 (1997) (explaining that the *Katz* Court adopted a broad test that allows the Amendment to adapt).

28. *See infra* Part II.B.1.; Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1576–82 (2004) (noting that subsequent application of the *Katz* "reasonable expectation of privacy" test quickly undermined its initial promise by limiting the doctrine through the business records cases).

29. Thomas K. Clancy, *What is a "Search" Within the Meaning of the Fourth Amendment*, 70 ALB. L. REV. 1, 17 (2006) (examining the literal approach taken by the Supreme Court in *Olmstead v. United States* and describing the development of Fourth Amendment doctrine).

30. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 358 U.S. 41 (1967).

Olmstead v. United States[31] epitomizes the Supreme Court's early Fourth Amendment jurisprudence. *Olmstead* examined the government's wiretap of Olmstead's telephone line from a neighboring building without any physical trespass onto Olmstead's property.[32] The majority reasoned that none of the Supreme Court's previous cases held that the Fourth Amendment was violated unless there was a physical search of the person, a seizure of his tangible effects, or an actual physical invasion of a protected area.[33] Consequently, the majority concluded that the wiretap was not a search under the Fourth Amendment for two primary reasons: 1) there was no physical invasion of a constitutionally protected area as there was no physical trespass onto Olmstead's real property and 2) there was no search of a tangible item as the wiretap searched only intangible sound.[34]

Justice Brandeis's dissent in *Olmstead* rejected the Court's "unduly literal construction" and narrow-minded view of the Fourth Amendment.[35] Justice Brandeis argued that the interpretation of the Amendment should be flexible, adapting to new means of surveillance and new means of government intrusion; methods which he argued could not be predicted by the Framers nor anticipated by the majority.[36] Justice Brandeis cautioned the Court that it was their duty to develop the Amendment in such a way as to protect against, not only means of government intrusion then known, but also "what may be" in the future.[37] Justice Brandeis reasoned that the science of government intrusion and espionage into the private lives of its citizens would not stop with the advent of wiretapping,[38] but rather would advance beyond invasions of tangible spaces such that the government could reproduce evidence in a Court of the "the most intimate occurrences of the home" without even "removing papers from secret drawers."[39]

B. Broader Fourth Amendment Protection: Katz *and the "Reasonable" Expectation of Privacy Test*

Justice Brandeis's flexible interpretation of the Fourth Amendment ultimately won out over the *Olmstead* majority's strict textual interpretation after *Olmstead* was

31. 277 U.S. 438. In *Olmstead*, the appellant, Roy Olmstead, sought to suppress, as a constitutionally impermissible search, recordings of conversations obtained by the police after a lengthy months-long wiretap of his home and office telephone line. *Id.* at 455.

32. *Id.* at 456–57.

33. *Id.* at 466.

34. *Id.* at 464 ("There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.").

35. *Id.* at 476 (Brandeis, J., dissenting).

36. *See id.* at 478; Steere, *supra* note 26, at 239–40.

37. *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting).

38. *Id.* at 474–75. See Patricia K. Holmes, Comment, *FBI's Carnivore: Is the Government Eating Away Our Right of Privacy?*, 7 ROGER WILLIAMS U. L. REV. 247 (2001) for a modern reflection on Justice Brandeis's prediction. Carnivore is an electronic surveillance device developed by the FBI. *Id.* at 249.

39. *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting).

officially discredited by the watershed decision of *Katz v. United States.*[40] *Katz* has since become the keystone of modern Fourth Amendment law.[41]

In *Katz*, the Court held that the government's use of an external listening device from outside a public telephone booth to record Katz's telephone conversation amounted to a search in violation of the Fourth Amendment.[42] The Court determined that the telephone user maintained a reasonable expectation of privacy such that, upon entering the public telephone booth and closing the door, he was "surely entitled to assume that the words he utter[ed] . . . [would] not be broadcast to the world."[43] The *Katz* majority reasoned that a more narrow interpretation of the protections afforded to a telephone user by the Fourth Amendment would ignore the vital role the telephone had come to play in private communications in modern American life.[44]

Consequently, the *Katz* Court rejected the strict interpretation afforded the Fourth Amendment in *Olmstead*, noting that the Supreme Court had departed in previous decisions from its strict textual interpretation of the Amendment[45] and expressly held that the government's activities in electronically eavesdropping and recording Katz's conversation violated the privacy upon which he "justifiably relied" in violation of the Fourth Amendment.[46] *Katz* therefore made clear that a Fourth Amendment violation is not dependent on a physical trespass onto a constitutionally protected space,[47] but rather is controlled by whether the government has violated an individual's expectation of privacy which the individual was justified in relying upon.[48]

---

40. 389 U.S. 347, 353 (1967) ("[T]he premise that property interests control the right of the Government to search and seize has been discredited." (quoting Warden v. Hayden, 387 U.S. 294, 304 (1967))).

41. *See, e.g.*, Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 382 (1974) (hailing *Katz* as a "watershed" in Fourth Amendment law); William G. Traynor, *Recent Developments, Constitutional Law—Search and Seizure—Warrantless Aerial Surveillance,* California v. Ciraolo, *106 S. Ct. 1809 (1986)*, 54 TENN. L. REV. 131, 135 (1986) (calling *Katz* the "keystone" of modern fourth amendment law).

42. *See Katz*, 389 U.S. at 353. In *Katz*, the appellant was convicted of violating a federal statute prohibiting wagering by telephone. *Id.* at 348. The government introduced evidence against the appellant including telephone conversations recorded by the FBI using an electronic listening device placed outside of the public telephone booth from which he placed his calls. *Id.* Katz challenged the validity of the government's actions recording his telephone conversations without a search warrant. *Id.* at 349–50.

43. *Id.* at 352.

44. *Id.*

45. *See id.* at 352–53 (reasoning "that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling"). The *Katz* majority cited *Warden v. Hayden*, 387 U.S. 294, 304 (1967) when discrediting *Olmstead*, contending that *Warden* had rejected the premise that property interests control Fourth Amendment application. *Id.*; Kerr, *supra* note 2, at 818 (noting that the *Katz* Court did not cite Justice Brandeis's dissent in discrediting *Olmstead*).

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

47. *Id.* "[T]he Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures . . . ." *Id.*

48. *Id.*

> The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus consti-

While the majority's opinion held that Katz had a justifiable expectation of privacy, it was Justice Harlan's concurrence that set out the two-fold analysis now synonymous with *Katz*.[49] Harlan clarified the Supreme Court's holding, explaining that an individual has a justifiable or reasonable expectation of privacy where the individual has 1) "exhibited an actual (subjective) expectation of privacy;" and 2) where society is prepared to recognize the individual's expectation as objectively reasonable.[50] Both elements must be present in order for the protections of the Fourth Amendment to apply.[51] Harlan concluded that both prongs were met in *Katz* because the society recognized the public telephone booth as a place where an occupant's expectation of privacy was reasonable, and Katz subjectively acted to preserve his right to privacy by shutting the telephone booth door behind him.[52]

In *Kyllo v. United States*,[53] the Supreme Court reaffirmed its commitment to adapting to society's expectations of privacy, recognizing that technological advances cannot be allowed to whittle away at society's expectation of privacy as against the government.[54] *Kyllo* required the Court to consider an investigator's use of a thermal imaging device to measure whether the amount of heat emanating from a home was consistent with the amount of heat required to grow marijuana indoors.[55] The *Kyllo* Court expressed its belief that an impermissible search occurs when sense enhancing technology not in general public use is used by the government to intrude upon the home and the government is therefore able to obtain information that it otherwise could not have obtained without a physical intrusion.[56] In dicta, the Court noted that its decision sought to preserve the degree of privacy against the government that existed when the Framers adopted the Fourth

---

> tuted a 'search and seizure' within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.

Id.

49. *See* Kerr, *supra* note 2, at 822 & n.113 (discussing Justice Harlan's understanding of the "expectation of privacy" framework).

50. *Katz*, 389 U.S. at 361 (Harlan, J., concurring). Justice Harlan offered an example of the application of this two-fold analysis, identifying the home as an area where society has recognized an individual's expectation of privacy as objectively reasonable, but noted that an individual has not conducted himself in a manner consistent with an actual expectation of privacy if he engages in activities inside the home in "plain view" of the public. *Id.*

51. *See* Cecil J. Hunt, II, *Calling in the Dogs: Suspicionless Sniff Searches and Reasonable Expectations of Privacy*, 56 CASE W. RES. L. REV. 285, 313 (2005) (explaining that the expectation of privacy test consists of two inquiries and both must be satisfied to qualify for Fourth Amendment protection).

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

53. 533 U.S. 27 (2001).

54. *Id.* at 34.

55. *Id.* at 29. The Ninth Circuit had held that Kyllo possessed "no subjective expectation of privacy because he had made no attempt to conceal the heat escaping from his home, and even if he had, there was no objectively reasonable expectation of privacy because the imager 'did not expose any intimate details of Kyllo's life,' only 'amorphous "hot spots" on the roof and exterior wall.'" *Id.* at 31 (citations omitted).

56. *Id.* at 34–35.

Amendment.[57] Permitting this intrusion, the Court stated, would permit "technology to erode the privacy guaranteed by the Fourth Amendment."[58]

Since settling on the *Katz* "reasonable expectation of privacy test," the Court has whittled away at the scope of the Amendment's protection.[59] The Court's Fourth Amendment jurisprudence since *Katz* reasons that disclosure of information to third parties makes an expectation of privacy objectively unreasonable[60] and that a user's expectation of privacy is unreasonable if the user has agreed to terms of service granting a third party access to the communication.[61]

1. *Limiting Reasonableness: Assumption of the Risk and Third Party Doctrine*

Two doctrines which limit the "reasonableness" of an expectation of privacy are assumption of the risk and the third party doctrine.[62] *Katz* itself cautioned that information "knowingly expose[d] to the public" would not be entitled to Fourth Amendment protection.[63] Indeed, a well settled Fourth Amendment principle is that where an individual reveals private information to another, he assumes the risk that the information will be revealed by the other to the government.[64] Thus, the primary circumstance where an individual forfeits his Fourth Amendment protection is where the individual "knowingly exposes" the information to a third party or the general public.[65]

No Fourth Amendment protection exists for information disclosed to the general public.[66] In *Oliver v. United States*,[67] the Court found no Fourth Amendment protection where narcotics agents, acting on reports of a marijuana growing opera-

---

57. *Id.* at 34.

58. *Id.*

59. *See infra* Parts I.B.1–2.; *see also* Mulligan, *supra* note 28, at 1577–82 (noting that the subsequent application of the *Katz* reasonable expectation of privacy test quickly undermined its initial broad promise by limiting the doctrine through the business records cases).

60. *See* Andrew J. DeFilippis, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1099 (2006) (explaining that the Court's decision in *United States v. Miller* was the first enunciation of the third party doctrine). Under this "third party doctrine" the Court has generally held that a user's expectation of privacy is objectively unreasonable where the user has disclosed information to a third party. *Id.*; *see also infra* Part I.B.1.

61. *See infra* Part I.B.2.

62. *See* DeFilippis, *supra* note 60, at 1100 (explaining that *Miller*, *Smith*, and their progeny rely on both the third party doctrine and a closely related doctrine of assumption of the risk). Assumption of the risk was first articulated in *Hoffa v. United States*, 385 U.S. 293 (1966), decided a year before *Katz*. *Id.*

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

64. Matthew D. Lawless, Comment, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 2007 UCLA J.L. & TECH. 1, 7; Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 528 (2006); *see also* Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 518–19 (2005).

65. *See Katz*, 389 U.S. at 351; *see also* Lawless, *supra* note 64, at 7; Solove, *supra* note 64, at 528; Henderson, *supra* note 64, at 518 (explaining the development of the third party doctrine).

66. *See, e.g.*, *Katz*, 389 U.S. at 351 (stating that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection").

67. 466 U.S. 170 (1984).

tion, went to the defendant's farm and saw a field of marijuana growing on the defendant's farm.[68] The Court reasoned that open fields are not an area protected by the Fourth Amendment because fences and "no trespassing" signs fail to bar the public from freely viewing open fields.[69] Thus, the Court found that the defendant had no reasonable expectation of privacy because he knowingly exposed his illegal operation to the public.[70]

Similarly, there is no Fourth Amendment protection where a communication is made to another because the communicator has "assumed the risk" the confidant will provide the information to the government.[71] This assumption of the risk doctrine was clearly articulated in *Hoffa v. United States*.[72] In *Hoffa*, the Supreme Court held that a defendant was not entitled to Fourth Amendment protection for statements made by Hoffa to a government informant.[73] The Court reasoned that Hoffa had assumed the risk that any information gained by the informant would be shared with the authorities.[74] In so holding, the Supreme Court crystallized the doctrine that the Fourth Amendment does not protect the content of the conversation of a speaker against the misplaced trust of his confidant because the recipient can be compelled by subpoena to testify.[75] In *United States v. White*,[76] the Court considered whether the government could be prohibited from obtaining information revealed by White to an undercover narcotics informant wearing a radio transmitter[77] where the suspect had made the disclosure on the assumption that the recipient would use the information for a limited purpose and the recipient was in a position of trust and confidence.[78] The majority opinion reasoned that White did not have a valid Fourth Amendment claim because, although White must have had a subjective expectation that his conversation was private, his expectation was not objectively reasonable as "one contemplating illegal activities must realize and risk that his companions may be reporting to the police."[79] Thus, the content of communications are not protected where the communicator has revealed content to the

68. *See id.* at 179 (finding no expectation of privacy because fields were open to view by the general public).

69. *Id.*

70. *See id.*

71. *See* Hoffa v. United States, 385 U.S. 293, 303 (1966) (explaining that there is no violation of the Fourth Amendment where a government informant obtains incriminatory statements in a conversation with the defendant because the risk that a friend will reveal that information to the government is "the kind of risk we necessarily assume whenever we speak" (quoting Lopez v. United States, 373 U.S. 427, 465 (1963))).

72. 385 U.S. 293. *See* DeFilippis, *supra* note 60, at 1100–01.

73. *Hoffa*, 385 U.S. at 302–03.

74. *Id.*

75. *Id.* at 302.

76. 401 U.S. 745 (1971).

77. *Id.* at 746–47.

78. United States v. Miller, 425 U.S. 435, 443 (1976) (citing *White*, 401 U.S. at 752).

79. *White*, 401 U.S. at 752.

"general public" or has assumed the risk that his confidant may be compelled to testify.[80]

In the same way, if a communication is made in such a way that a member of the general public can access the content of the communication, there is no Fourth Amendment protection in the communication.[81] For example, federal courts examined whether a Fourth Amendment reasonable expectation of privacy existed in the content of cellular telephone communications in *United States v. Hoffa*.[82] In *Hoffa*, the United States Court of appeals for the Seventh Circuit relied on the broad statement in *Katz* that information "knowingly expose[d] to the public" would not be protected by the Fourth Amendment in finding Hoffa possessed no reasonable expectation of privacy in the content of the calls he placed from his cellular telephone as the calls "were exposed to everyone in that area who possessed a F.M. radio receiver or another automobile telephone tuned in to the same channel."[83]

Governed by the same disclosure principles, the Supreme Court's combined precedents in *United States v. Miller*[84] and *Smith v. Maryland*[85] recognize that an individual has no reasonable expectation of privacy if he has disclosed non-content information to a party who maintains the information in a record kept in the ordinary course of business for a legitimate business purpose.[86] In *Miller*, the Supreme Court examined whether the government had illegally seized, pursuant to a defective subpoena, the financial records of a bank depositor including deposit slips, statements, checks, and other account information.[87] The Court concluded that the government had not intruded upon any area in which there was a Fourth Amendment interest because the bank customer had no reasonable expectation of privacy in financial records which were not his private papers, but rather were business records of the bank.[88] The Supreme Court concluded that Miller's records were not "private papers" within the purview of Fourth Amendment because he

80. *See supra* notes 66–79 and accompanying text.

81. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (stating that "conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable"); United States v. McLeod, 493 F.2d 1186, 1188 (7th Cir. 1974) (holding that no reasonable expectation of privacy existed where federal agents overheard McLeod discussing illegal wagering when such statements were made in the open and were audible to the agents). *See generally* United States v. Hoffa, 436 F.2d 1243 (7th Cir. 1970) (finding no expectation of privacy in mobile telephone communications that can be monitored by the general public using ordinary F.M. radio receivers).

82. 436 F.2d 1243.

83. *Id.* at 1247.

84. 425 U.S. 435 (1976).

85. 442 U.S. 735 (1979).

86. *See infra* notes 87–95 and accompanying text; Lawless, *supra* note 64, at 1, 10 (explaining that *Miller* and *Smith* formalized the Fourth Amendment doctrine stating that the "Amendment does not prohibit the government from obtaining information revealed to a third party" (citing *Smith*, 442 U.S. at 734–35)).

87. 425 U.S. at 436–37.

88. *Id.* at 440.

could not assert ownership or possession of his bank's records.[89] The Court relied on its line of cases regarding misplaced trust and compelled disclosure to reason that Miller had "assumed the risk," by revealing his financial records to a third party—the bank—and therefore this information could be conveyed by the bank to government.[90]

Similarly, in *Smith* the Court considered whether an individual's Fourth Amendment rights were violated by the government's use of a pen register to capture the telephone numbers dialed from an individual's home telephone.[91] The Court held that an individual had relinquished his legitimate expectation to privacy in the telephone number dialed because he knowingly disclosed the numeric digits dialed to the telephone company.[92] The Court determined that Smith failed to behave in a manner consistent with an expectation of privacy in the numbers dialed because Smith knew the digits must be conveyed to the telephone company to direct the call.[93] Specifically, the Court reasoned that the numeric information was not entitled to an expectation of privacy because the user knowingly conveyed the information to the company in order to make the call, knew that the phone company had facilities to record this information, and knew that the company recorded the information to fulfill a variety of legitimate business purposes.[94] The Court distinguished *Smith* from *Katz* because *Katz* involved the government's acquisition of the contents of communication, while the pen register at issue in *Smith* merely captured non-content information—the numeric digits dialed.[95]

2. *Limiting Reasonableness: Contractual Relinquishment*

Another circumstance where the expectation of privacy announced in *Katz* is limited is when an individual has relinquished the expectation of privacy contractually, by agreeing to terms or conditions that communications may be monitored, or audited.[96] Such relinquishment means the individual cannot reasonably maintain a legitimate expectation of privacy.[97] Primarily, this topic has been addressed in the context of computer and electronic communications by federal courts struggling to

89. *Id.*

90. *Id.* at 443.

91. *Smith*, 442 U.S. at 736–38.

92. *Id.* at 743–44.

93. *Id.* at 743.

94. *Id.* at 745 (discussing the ability of telephone companies to record the numbers dialed for legitimate billing purposes).

95. *Id.* at 741 (explaining that a pen register is distinguishable from a listening device, such as the device utilized in *Katz*, because a pen register is designed such that it cannot capture the contents of the communication).

96. *See, e.g.*, United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (holding that a federal employee possessed no legitimate expectation of privacy where his government employer's policy stated that internet use would be "audit[ed], inspect[ed], and/or monitor[ed]"); *see also* Robert I. Webber, Note, *The Privacy of Electronic Communications: A First Step in the Right Direction*, 1 J.L. & TECH. 115, 129 (1986) (explaining that a subjective expectation of privacy may be altered by contract).

97. *See* Webber, *supra* note 96, at 129.

apply *Katz* where a user has accepted contractual terms with their ISP, employer or other third party regarding privacy in electronic communications.[98] For example, if a user has consented to a contractual policy which grants the network administrator or employer unlimited access to a user's computer, the user has extinguished any subjectively reasonable expectation of privacy.[99] Similarly, if the system contains a disclaimer stating that personal communications are not private, the disclaimer will defeat claims of Fourth Amendment protection.[100]

In *United States v. Simons*, the United States Court of Appeals for the Fourth Circuit held that a government employee had no reasonable expectation of privacy in files on an office computer because the government employer had reserved the right to "audit, inspect, and/or monitor" such files.[101] The court reasoned that the employee lacked any subjective expectation of privacy in the files downloaded from the Internet in light of the employer's Internet policy.[102] Similarly, in *Muick v. Glenayre Electronics*,[103] the United States Court of Appeals for the Seventh Circuit found that an employer's notice that it could inspect employee laptops rendered illegitimate any expectation of privacy the employee may have had in the computer.[104]

However, the United States Court of Appeals for the Ninth Circuit came to the opposite result when it considered the expectation of privacy of a college student in files stored on his personal computer attached to the university network.[105] In *United States v. Heckenkamp*, the government did not challenge that Heckenkamp had a subjectively reasonable expectation of privacy in his computer and dormitory room, and the court solely addressed whether Heckenkamp's expectation of privacy

98. *See, e.g.*, United States v. Heckenkamp, 482 F.3d 1142 (9th Cir. 2007) (examining a college student's expectation of privacy in files downloaded off the university network where the university did not have a monitoring policy); Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (explaining that a system operator's posting of a disclaimer stating that personal communications on a computer bulletin board were not private defeated Fourth Amendment claims); *Simons*, 206 F.3d at 398 (examining a Fourth Amendment claim of a federal employee after a government employer with a monitoring policy found pornographic materials on his work computer).

99. *Cf. Heckenkamp*, 482 F.3d at 1147 (concluding that a student is entitled to an expectation of privacy where the University network policy provided assurances that computer and electronic files would generally be free from access by anyone other than the authorized users and made limited exceptions to maintain network operations).

100. *See Guest*, 255 F.3d at 333 (citing *Simons*, 206 F.3d at 398) (finding that a user lacks a privacy interest in his internet search records where his/her employer has posted a privacy disclaimer regarding computer files).

101. *Simons*, 206 F.3d at 398. The Court held that the employee did not have a objectively reasonable expectation of privacy in internet search records made from his workplace computer in view of the employer's computer usage policy. *Id.* The policy specified the types of data that would be monitored, including e-mail, Internet, and electronic file transfers, and specified the ways in which the data would be retrieved, including audit and inspection. *Id.*

102. *Id.*; *see also* Michelle Hess, Note, *What's Left of the Fourth Amendment in the Workplace: Is the Standard of Reasonable Suspicion Sufficiently Protecting Your Rights?*, 15 FED. CIRCUIT B.J. 255, 274 (2005).

103. 280 F.3d 741 (7th Cir. 2002).

104. *Id.* at 743.

105. United States v. Heckenkemp, 482 F.3d 1142, 1143–46 (9th Cir. 2007).

in his computer was objectively reasonable.[106] The court concluded that his expectation of privacy was objectively reasonable because there was no announced monitoring policy on the university's computer network.[107] In dicta, the *Heckenkamp* court cautioned, however, that privacy expectations would be reduced if the user was advised that information transmitted through the network is not confidential and that the systems administrators may monitor communications.[108]

II. THE USE OF COMPARISON

The question of what reasonable expectations of privacy exist in new communications technologies and whether the privacy guaranteed by the Fourth Amendment will protect users of these systems remains open.[109] Courts addressing the issue have applied comparative reasoning to find reasonable expectations of privacy in new communications.[110]

A. The Role of Comparison

Comparison is one of the central tools used to organize thought.[111] Legal reasoning is prone to the use of metaphors[112] and analogy,[113] as seen by the great reliance in the American legal system on the role of precedent in the judicial process.[114] Legal decisions often "hinge[ ] on the [persuasive] use of metaphors [and analogies], which have a unique power to color the court's analysis."[115]

When judges are faced with new technologies, specifically in areas of first impression, they are particularly prone to relying on metaphorical or analogical reasoning.[116] Reliance on such reasoning, rather than undertaking to gain a true understanding of the technology at issue, creates the potential that an "easy" com-

106. *Id.* at 1146.

107. *Id.* at 1147.

108. *Id.*

109. *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904 (9th Cir. 2008) ("The extent to which the Fourth Amendment provides protection for the contents of electronic communications in the Internet age is an open question.").

110. *See infra* Part II.B.

111. *See* Gore, *supra* note 3, at 403 (noting that it is well established in both cognitive sciences and linguistics that metaphors are one of the primary tools individuals use to organize thought).

112. A metaphor is "a figure of speech in which a word or phrase literally denoting one kind of object or idea is used in place of another to suggest a likeness or analogy between them . . . ." MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 780 (11th ed. 2005).

113. An analogy is an "inference that if two or more things agree with one another in some respects they will prob[ably] agree in others[.]" MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 44 (11th ed. 2005).

114. *See* Gore, *supra* note 3, at 405.

115. Gustavo Enrique Schneider, Warshak v. United States*: Fourth Amendment Risk Analysis in the 21st Century*, 48 JURIMETRICS 357, 360 (2007) (citing Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Informational Privacy*, 53 STAN. L. REV. 1393 (2001)).

116. Jonathan H. Blavin, & I. Glenn Cohen, Note, *Gore, Gibson, and Goldsmith: The Evolution of Internet Metaphors in Law and Commentary*, 16 HARV. J.L. & TECH. 265, 267 (2002); Gore, *supra* note 3, at 409.

parison will be adopted by the court despite that it is often ill-tailored to the particular task at issue.[117]

Thus, one of the pitfalls of comparative reasoning is its seductiveness, which allows a person to take refuge in familiar patterns of reasoning and blinds a person to dissimilar or inconsistent qualities which favor a different conclusion.[118] The use of metaphorical reasoning in cases dealing with emerging technologies is epitomized by the United States Court of Appeals for the Armed Forces opinion in *United States v. Maxwell.*[119]

B. Using Comparison in Determining Expectations of Privacy

In *Maxwell*, the FBI obtained a search warrant to search AOL's master list of users in order to ascertain the identity of a screen name holder[120] who had sent e-mails containing child pornography on the AOL system.[121] Upon discovering the identity of the individual involved in sending the e-mails, the agent learned that the screen name holder, Maxwell, was a member of the U.S. Air Force, and sought a warrant to search Maxwell's quarters.[122] In the subsequent search of Maxell's computer, the Air Force obtained numerous images depicting child pornography.[123] After he was charged, Maxwell sought suppression of the evidence obtained from the FBI's search of his AOL account and computer.[124] In ruling on the validity of the searches, the United States Court of Appeals for the Armed Forces first considered the threshold question of whether Maxwell had "a reasonable expectation of privacy in the AOL e-mail system."[125]

The court found that Maxwell had a reasonable expectation of privacy in e-mails on the AOL system.[126] Rather than examining the underlying subjective and objective expectations of privacy per the *Katz* framework, the *Maxwell* court reasoned that e-mail was no different than first class mail and telephone calls, both of which are protected by the Fourth Amendment, and consequently concluded e-mail must also be protected by the Fourth Amendment.[127]

First, the court reasoned that e-mail was similar to postal mail, in that "if a sender of first-class mail seals an envelope and addresses it to another person, the

117. *See* Gore, *supra* note 3, at 403.
118. *See id.*
119. 45 M.J. 406 (C.A.A.F. 1996).
120. *Id.* at 413.
121. *Id.* at 412.
122. *Id.* at 414.
123. *Id.*
124. *Id.* at 415. Maxwell contended that the warrant issued by the federal magistrate should be held constitutionally invalid for three reasons; 1) "the typographical error in the warrant authorizing a search of 'REDDEL' in place of 'Redde 1' [Ready One] invalidates the search of the 'Redde1' files; 2) . . . the warrant was overly broad . . . ; [and] 3) . . . the seizure of the 'Zirloc' materials" was not permissible under the warrant. *Id.*
125. *Id.* at 416.
126. *Id.* at 417.
127. *Id.* at 417–18.

sender can reasonably expect the contents to remain private and free from the eyes of the police absent a search warrant founded upon probable cause."[128] Next, the court reasoned that e-mail was also similar to telephone communications in that "the maker of a telephone call has a reasonable expectation that police officials will not intercept and listen to the conversation; however, the conversation itself is held with the risk that one of the participants may reveal what is said to others."[129] Reasoning analogously from these parallels, the court stated "the transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant."[130] However, the court cautioned once the transmissions were received by the recipient, the transmitter would no longer control its destiny.[131]

The *Maxwell* court noted the similarity between e-mail transmissions and traditional forms of communication, despite the ISP's ability to access the contents of the e-mail message.[132] Because a sender of a first class piece of mail maintains an expectation of privacy during the pendency of its receipt by the sender, and because a telephone user maintains an expectation of privacy during the transmission of the call, the court explained that an e-mail user whose e-mail is stored on the AOL system also maintains an expectation of privacy.[133]

The *Maxwell* court is not alone in its interpretation of "reasonable" expectations of privacy in the context of new communications.[134] The United States Court of Appeals for the Ninth Circuit espoused a similar pattern of reasoning to determine whether a reasonable expectation of privacy existed in text message communications.[135] In *Quon v. Arch Wireless Operating Co.*, the Ninth Circuit considered Quon's 42 U.S.C. § 1983 suit alleging that the city's audit of his text messages on a work-provided two-way text-enabled device was an unlawful search and seizure in violation of his Fourth Amendment rights.[136] At the onset, the *Quon* court acknowledged that the extent to which the Fourth Amendment provides protection for the contents of electronic communications was "an open question."[137] The court saw "no meaningful distinction between text messages and letters," reasoning that text messages, much like letters and e-mails, would not support a reasonable expectation of privacy in the information used to direct a text message to its intended recipient, in the same way as *Smith* found no reasonable expectation of privacy in

128. *Id.* at 417.
129. *Id.* at 418.
130. *Id.*
131. *Id.*
132. *Id.* at 417–18.
133. *See id.*
134. *See infra* notes 135, 141, 150–52 and accompanying text.
135. *See* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905 (9th Cir. 2008).
136. *Id.* at 899.
137. *Id.* at 904.

the number dialed to send a telephone call.[138] However, without further analysis, the court concluded, "users do have a reasonable expectation in the content of their text messages vis-à-vis the service provider."[139] In this way, the court implicitly reasoned that the content information contained in a text message was necessarily analogous to, and entitled to the same protection as, the content information of a telephone call.[140]

Likewise, in *Warshak v. United States*,[141] the United States District Court for the Southern District of Ohio considered the grant of a preliminary injunction preventing the government from seizing Warshak's e-mails from his ISP.[142] The court considered metaphors offered by each side. Warshak argued that his e-mail was a "closed package,"[143] "container,"[144] "letter"[145] that could not be searched without a probable cause search warrant.[146] The United States argued that letters and e-mails were fundamentally different and the privacy expectation in letters entrusted to third party mail carriers was different than the privacy expectation in e-mails entrusted to commercial ISPs.[147] Instead, the government contended that e-mails entrusted to commercial ISPs were like "postcards,"[148] as ISPs contractually reserve and exercise rights to open, delete, monitor, scan, and otherwise access account subscriber's e-mails.[149] The district court was ultimately persuaded that Warshak's metaphor was more appropriate,[150] and concluded that Warshak was likely to suc-

138. *Id.* at 905.

139. *Id.*

140. *See id.*

141. No. 1:06-CV-357, 2006 WL 5230332 (S.D. Ohio July 21, 2006). The case arose during the course of the government's criminal investigation of Appellee, Steven Warshak, and his company Berkeley Premium Nutraceuticals, Inc. *Id.* at *2. During the government's investigation, it utilized two separate *ex parte* orders under 18 U.S.C. § 2703(d) to compel Warshak's Internet Service Providers ("ISPs") to disclose all stored content and account information from Warshak's e-mail accounts. *Id.* at *1–2. In both instances, a judge issued a 2703(d) order after the government met the low burden of stating "specific and articulable facts" showing reasonable grounds to believe that the information sought was "relevant and material to an ongoing criminal investigation" of the defendant. *Id.* at *3. Simultaneously, the government utilized another ECPA provision to delay notification of the disclosure to Warshak for a period of ninety days. *Id.* The delayed notification provision was authorized upon the government's claim that notice to Warshak of the disclosures would "seriously jeopardize" the criminal investigation. *Id.* The 2703(d) orders were issued under seal, preventing Warshak's ISPs from informing him of existence of the order, the investigation against him, or disclosure itself. *Id.* Over a year later and without any renewals of the ninety day delayed notification period, Warshak was finally notified of the 2703(d) orders which compelled his ISPs to turn over the contents of his e-mail accounts. *Id.* Subsequently Warshak filed a complaint against the United States in the District Court for the Southern District of Ohio alleging that the compelled disclosure of his e-mail without a probable cause warrant violated his Fourth Amendment rights. *Id.* at *4.

142. *Id.* at *1.

143. *Id.* at *7.

144. *Id.*

145. *Id.* at *8.

146. *Id.*

147. *Id.*

148. *Id.* (citing United States v. Van Leeuwen, 397 U.S 249, 251 (1970)).

149. *Id.*

150. *Id.* at *9.

ceed on the merits of his Fourth Amendment claim.[151] While recognizing that "emails [sic] sent through and stored on the servers of commercial ISPs are obviously distinguishable in many respects from both sealed letters and postcards physically mailed via public or private carrier,"[152] the district court hung its hat on the similarities between letters and e-mails.

III. DISSECTING THE COMPARISONS

The aforementioned courts are correct in identifying that e-mails and text messages are similar to other forms of communication.[153] In fact, telephones, cellular phones, voice-mail, postal mail, text messaging, and e-mail share a common goal—to create a communication network.[154] All communication networks send and receive two types of information: content information and envelope information.[155] Content information refers to the contents of the communicated message whereas envelope information is a type of non-content information which is used to deliver the message to its intended recipient.[156] For example, the mail system operates on these principles: content information refers to the message intended for the recipient (the letter inside the envelope)[157] and envelope information refers to the addressing information used by postal officials to direct the mail to its intended recipient (the name, street address, and postal zip code).[158] Although the analogies between new forms of communication—such as e-mail, and letters or telephone calls—appear straightforward, significant distinctions exist between the mediums.[159] Primarily, these distinctions involve differences with regard to whom the message is disclosed and what information is disclosed.[160] These differences are especially important in determining the "reasonableness" of an expectation of privacy. Failure to examine the technical differences between the communications renders any "reasonable expectation" analysis incomplete. As an example, the next section will briefly explain

151. *Id.* at *11.

152. *Id.* at *9.

153. *See, e.g.*, United States v. Maxwell, 45 M.J. 406, 417–18 (C.A.A.F. 1996) (stating that "[e]-mail transmissions are not unlike other forms of modern communication"); *see also* O'Neil, *supra* note 9, at 36. VoIP uses a data network to transmit a telephone call over the internet in a digital format. *Id.* The information is replicated from one router to another until it arrives at the recipient's telephone, leaving a data trail indefinitely in cyberspace storage. *Id.*

154. *See* Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 611 (2003) ("The fundamental purpose of a communications network is to send and receive communications.").

155. *Id.*; *see also* Johnny Gilman, Comment, *Carnivore: The Uneasy Relationship Between the Fourth Amendment and Electronic Surveillance of Internet Communications*, 9 COMMLAW CONSPECTUS 111, 122 (2001).

156. Kerr, *supra* note 154, at 611.

157. *Id.*

158. *Id.*

159. *See infra* Part III.B.; *see also* Freiwald, *supra* note 3, at 4.

160. *See infra* Parts IV.A.–B.

the technical operation of e-mail communications, as exemplary of emerging communication networks.[161]

A. *Technological Background*

E-mail is a type of digital technology network which sends envelope and content information from one computer to another computer.[162] E-mails are made up of two types of data packets, packet headers and body packets, which are sent and received by computers over the Internet.[163] The envelope information appears in the packet header.[164] The non-content information in the packet headers contains the e-mail addresses of the sender and recipient, the addresses of the computers (Internet Protocol addresses), and information about what type of message is attached.[165] A second type of data packet, the body packet, contains the communication's message.[166]

Both the packet header and body packet must be revealed to the ISP to communicate and send the message.[167] Generally speaking, the packet header and body packets will travel separately, each taking the shortest path possible, through an interconnected network of computers to reach their destination at the ISP server where the packets are "reassembled."[168] During this process, the contents of the communication travel through a series of routers operated by a multitude of different entities and copies of the contents are left behind on third party routers which can access the contents at a later time.[169] Because data is transferred in clear text, the third parties with access to the communication can read them.[170] When the packets arrive at their final destination, the receiving computer will discard the packet header and keep content information contained in the body packet.[171] The recipient of the communication may download the message onto a local drive and delete it from the ISP server, may read and delete the e-mail from the ISP's server, or may retain the message on the ISP server as a backup copy.[172] VoIP and SMS text

161. *See infra* Part III.A.

162. *See* Kerr, *supra* note 154, at 613.

163. *See id.* at 612–14; *see also* Gilman, *supra* note 155, at 122.

164. Kerr, *supra* note 154, at 612–13.

165. *See id.* at 614.

166. *See* Gilman, *supra* note 155, at 122.

167. *See* Kerr, *supra* note 154, at 614 (stating that "while an email [sic] travels across the Internet, both the envelope and content information of emails [sic] travel across the Internet as payloads of individual packets").

168. *See* U.S. Telecom Ass'n v. F.C.C., 227 F.3d 450, 464 (D.C. Cir. 2000).

169. Schneider, *supra* note 115, at 371. At the very least four copies of the e-mail message exist ("one each on the sender's hard drive, the sender's service, the recipient's server, and the recipient's hard drive"). *Id.*; *see also* Mulligan, *supra* note 28, at 1563 (citing OFFICE OF TECH. ASSESSMENT REPORT, U.S. CONGRESS, ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES (1985)); *see infra* App. A.

170. Mulligan, *supra* note 28, at 1563.

171. Kerr, *supra* note 154, at 614.

172. *See* Mulligan, *supra* note 28, at 1563.

messaging communications travel across networks in data packets in a similar way.[173]

B. *Imperfect Comparisons*

Despite the unique technological characteristics of new forms of electronic communications,[174] courts are likely to compare the new technologies to traditional communication networks.[175] However, courts should analyze the propriety of these comparisons.[176] The central distinction between e-mail and its analog counterparts, postal and telephone communications, is that electronic communications are inherently more vulnerable to interception than other forms of communication.[177] This vulnerability stems from multiple sources.[178]

First, unlike letters or telephone calls which are transmitted by either the postal service or telephone company, the e-mail travels through multiple third parties before reaching the receiving ISP.[179] In contrast, letters and telephone calls pass directly to the intermediaries who utilize the non-content envelope information to direct the communication to its intended recipient.[180] Second, each of the "handlers" who have access to the e-mail during transmission may access the content of the communication.[181] While the intermediaries who handle letters and telephone calls have the ability to access the content of the communication, there is a presumption that intermediaries "will not do so as a matter of course."[182] Whether such a presumption would apply to third party handlers (rather than ISPs) who transmit the communication, is unlikely.[183] Third, e-mails are unlike traditional forms of communication because of their potential to exist indefinitely in multiple

---

173. VoIP is a technology for transmitting analog voice signals (telephone calls) into digital data that is sent in packets over Internet protocol rather than through the traditional telephone network indistinguishable in form from other data transmissions over the Internet. *See* Garrie et al., *supra* note 9, at 100–01, 105; *see also* O'Neil, *supra* note 9, at 36. As data packets containing the voice communications travel through the Internet, the data is replicated from one router to the next until it arrives at the listener's phone. *Id.* Consequently, a data trail of the communication remains indefinitely. *Id.*

174. *See infra* notes 179–85 and accompanying text.

175. *See* Megan Connor Bertron, Note, *Home is Where Your Modem Is: An Appropriate Application of Search and Seizure Law to Electronic Mail*, 34 AM. CRIM. L. REV. 163, 186 (1996).

176. *Id.*; *see also* R. Scot Hopkins & Pamela R. Reynolds, *Redefining Privacy and Security in the Electronic Communication Age: A Lawyer's Ethical Duty in the Virtual World of the Internet*, 16 GEO. J. LEGAL ETHICS 675, 683–84 (2003) (stating that simple analogy trivializes differences between e-mail and postal mail and fails to account for differences in cyber space).

177. *See* Schneider, *supra* note 116, at 372.

178. Mulligan, *supra* note 28, at 1562–63.

179. *See id.*; *infra* App. A.

180. I use the term "handler" in this Comment to refer to third parties through which the data packets travel during transmission.

181. *See* Schneider, *supra* note 116, at 374 (citing Henderson, *supra* note 64, at 523).

182. *See* Warshak v. United States, 490 F.3d 455, 471 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008).

183. *See* Kerr, *supra* note 154, at 628 (explaining how courts are likely to use the disclosure principle when extending Fourth Amendment protections to electronic communications).

locations.[184] Unlike analog telephone conversations which are transmitted over telephone lines and are ephemeral in nature, digital copies of e-mails may be stored indefinitely by multiple third parties and by ISPs.[185]

IV. APPLYING *KATZ* TO ELECTRONIC COMMUNICATIONS

Courts should not rely on past applications of the "reasonable expectation of privacy" test to traditional communications mediums to examine Fourth Amendment protections of new modes of communication. Instead, *Katz* must be re-applied and careful attention given to the technological aspects of each communication network. Particularly, courts must examine 1) if content or non-content information is disclosed;[186] 2) to what type of third party the information has been disclosed;[187] and 3) if the individual relinquished any expectation of privacy contractually.[188]

Faithfully applying *Katz* and the disclosure principles, courts will find that Fourth Amendment protection generally does not exist in the new frontier of electronic communications as the law currently stands.[189] If non-content information is revealed to any third party or intermediary, no Fourth Amendment protection will apply to the non-content information disclosed.[190] If content information is revealed, the court must analyze whether the information is conveyed directly to an intermediary; if so, the presumption exists that the intermediary will not disclose the communication and Fourth Amendment protection will apply.[191] However, if the content information is revealed to a non-intermediary third party, the disclosure principle extinguishes Fourth Amendment protection.[192] Finally, if Fourth Amendment protection has not been extinguished under the proceeding analysis, a court must consider whether the user has acted in a manner inconsistent with a reasonable expectation of privacy by consenting to a contract or other policy limiting an otherwise reasonable expectation of privacy.[193]

A. *What Type of Information Is Conveyed to Others*

First, the court must examine what type of information has actually been conveyed by the user by determining if non-content information or content information was

184. *See* Mulligan, *supra* note 28, at 1562.
185. *Id.* at 1562–63.
186. *See infra* Part IV.A.
187. *See infra* Part IV.B.
188. *See infra* Part IV.C.
189. *See infra* Parts IV.A.–C.
190. *See infra* Part IV.A.
191. *See infra* Part IV.B.
192. *See infra* Part IV.B.
193. *See infra* Part IV.C.

conveyed.[194] It is this distinction between content and non-content information which explains the different results in *Katz* and *Smith*.[195]

In *Katz*, the Supreme Court recognized a heightened Fourth Amendment protection for the content of telephone conversations despite the fact that the telephone company could access the content of the conversation.[196] The Court refused to allow telephone users expectations of privacy in the content of their conversation to be diminished merely by the phone company's ability to access the content of the communication.[197] As made clear by *Katz*, content information receives a special heightened protection under the Fourth Amendment.[198]

The heightened protection provided to content information is distinguished from the treatment of non-content information. Under the precedents of *Smith*, *Miller*, and *Guest v. Leis*,[199] if non-content information is revealed to a third party or intermediary, no Fourth Amendment protection will apply under the disclosure principle.[200] In *Smith*, the Court distinguished the telephone number dialed by the user, a type of non-content information, from the content of the telephone call at issue in *Katz*, and held that the number dialed was unprotected by the Fourth Amendment.[201] More recently, the United States Court of Appeals for the Sixth Circuit adhered to this content-non-content distinction in *Guest* when it found that the non-content subscriber information revealed to the ISP by the user was not protected as the user had disclosed this non-content information to the ISP.[202]

Analyzing e-mail communications under this framework, it is clear that e-mail discloses both content information and non-content information to intermediaries and to third parties.[203] Consequently, non-content, such as the "to/from" address of the e-mail will not receive Fourth Amendment protection.[204] However, because the content of communications receives a heightened protection, the court must proceed to the second inquiry by analyzing the type of third party to whom the information has been disclosed.[205]

---

194. *See* Kerr, *supra* note 154, at 628–29.

195. *See* Warshak v. United States, 490 F.3d 455, 470 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008). *Compare* Katz v. United States, 389 U.S. 347 (1967), *with* Smith v. Maryland, 442 U.S. 735 (1979).

196. *Warshak*, 490 F.3d at 471.

197. *Smith*, 442 U.S. at 746 (Stewart, J., dissenting) (discussing *Katz*).

198. *Warshak*, 490 F.3d at 471.

199. 255 F.3d 325 (6th Cir. 2001).

200. *See id.* at 335–36; *see also Smith*, 442 U.S. at 741.

201. *Smith*, 442 U.S. at 741.

202. *Guest*, 255 F.3d at 335–36.

203. Kerr, *supra* note 154, at 614 (explaining that both content and envelope (non-content) information must be transmitted to successfully send e-mail from sender to recipient).

204. *Id.* at 628; *see also* United States v. Miller, 425 U.S. 435 (1976) (finding no expectation of privacy in bank depositor's financial records); *Smith*, 442 U.S. 735 (finding no expectation of privacy in the numeric digits dialed to transmit a telephone call to a recipient).

205. *See* Kerr, *supra* note 154, at 628–29.

B. Identity of Parties with Whom the Communication Was Disclosed—The Third Party Doctrine

At the second level of analysis, the court must determine if content information was revealed to an intermediary or to a non-intermediary third party.[206] Content information received by the general public as in *Hoffa*,[207] and intermediaries such as the telephone company in *Katz*,[208] receive different Fourth Amendment treatment.[209] If content information is revealed to an intermediary, the presumption exists that the intermediary will not disclose the communication and the Fourth Amendment will apply.[210] It is this presumption which permits a user to maintain their expectation of privacy despite the technical ability of an intermediary—such as the telephone company in *Katz* or the United States Postal Service—to access the communication.[211]

Katz clearly supports the proposition that disclosure of a communication to an intermediary does not eviscerate a reasonable expectation of privacy.[212] In *Katz*,[213] the Supreme Court held that a telephone user maintained an expectation of privacy against the eavesdropping of the government despite the fact that the content of the telephone call was transmitted, and therefore disclosed, to the telephone company intermediary.[214] While, generally speaking, sharing the content of communications with a third party would eliminate any reasonable expectation of privacy,[215] the Court recognized an exception for intermediaries.[216] The *Warshak* court noted the assumption of the risk doctrine "d[id] not necessarily apply . . . to an intermediary that merely has the ability to access the information sought by the government" because of the shared societal expectation that the intermediary "will not do so as a matter of course."[217] Otherwise, the court found that a reasonable expectation of

206. *Id.*

207. *See* United States v. Hoffa, 436 F.2d 1243, 1246 (7th Cir. 1970). Any member of the general public could use the F.M. radio receivers to overhear conversations made from a mobile telephone. *Id.*

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

209. *Compare Katz*, 389 U.S. 347 (finding a reasonable expectation of privacy despite that the content of the communication being revealed), *with Hoffa*, 436 F.2d 1243 (finding no expectation of privacy in cell phone communication where the content of communication revealed to the public through radio transmission available to anyone in the vicinity with a radio receiver).

210. *See Katz*, 389 U.S. 347 (finding a reasonable expectation of privacy despite that the content of the communication was revealed to the telephone company); Warshak v. United States, 490 F.3d 455, 471 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008).

211. *See supra* note 210 and accompanying text.

212. *See infra* note 213–16 and accompanying text.

213. *See Katz*, 389 U.S. 347; *see also Warshak*, 490 F.3d at 470 ("Clearly, under *Katz*, the mere fact that a communication is shared with another person does not entirely erode all expectations of privacy, because otherwise eavesdropping would never amount to a search.").

214. *Katz*, 389 U.S. at 352 ("One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.").

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

216. *See supra* notes 206–11 and accompanying text.

217. *Warshak*, 490 F.3d at 470–71.

privacy would always be extinguished by virtue of an intermediary's ability to access the content of telephone calls, content of mail, and the contents of safe deposit boxes.[218]

However, courts have held that no reasonable expectation of privacy exists where the individual has revealed the contents of the communication with the general public.[219] For example, in *Hoffa*, the court recognized that no Fourth Amendment protection exists where information is disclosed to non-intermediary parties who can access the content of the communication.[220] In *Hoffa*, the court held that there was no reasonable expectation of privacy in the content of cellular telephone communications because the conversation was broadcast via radio transmission to anyone who had a radio receiver tuned to the correct frequency.[221] Consequently, if the third party to whom content information is disclosed is a non-intermediary, no Fourth Amendment protection under a *Katz* traditional analysis will exist.[222]

In the context of e-mail communication, it is clear the content of the communication is disclosed not just to the ISP, but to any handler that comes into contact with the data packet as it travels from ISP to ISP.[223] Like the cell phone conversation in *Hoffa* that could be accessed by any member of the general public in the vicinity with a radio receiver,[224] any third party that the communication travels through can access or copy the contents of the communication.[225] Thus, a direct comparison to telephone and e-mail communication overlooks an important distinction between e-mail and other forms of communication—that is, that the e-mail is revealed, and able to be copied by any number of systems or persons through which the communication travels.[226] Under the Court's third party doctrine, the e-mail user has assumed the risk "in revealing his affairs to another, that the information will be conveyed by that person to the Government."[227] As in *Miller* and *Smith*, any subjective expectation of privacy the e-mail user has in the content of his e-mail is eviscerated because "he voluntarily turn[ed] [the communication] over to third parties."[228] As one preeminent scholar has concluded, "[i]n the Information Age, so much of what we do is recorded by third parties that the

218. *Id.* at 470.

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

220. *See* United States v. Hoffa, 436 F.2d 1243 (7th Cir. 1970) (recognizing no Fourth Amendment protection for mobile telephone conversation disclosed to all individuals in the vicinity with F.M. receivers tuned to the proper station).

221. *Id.* at 1247.

222. *See id.*

223. *See infra* App. A.

224. *Hoffa*, 436 F.2d at 1247.

225. Mulligan, *supra* note 28, at 1562–63.

226. *Id.*

227. United States v. Miller, 425 U.S. 435, 442–43 (1976).

228. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

Court's third party doctrine increasingly renders the Fourth Amendment ineffective in protecting people's privacy against government information gathering."[229]

C. *Contractual Relinquishment as Terminating Fourth Amendment Protection*

Finally, a court undertaking a *Katz* reasonable expectation of privacy analysis in electronic communications must examine if the user has relinquished privacy that may otherwise have been afforded to him by agreeing to terms or policies that allow administrators or others to monitor, and thus access, the communications.[230] Even if the electronic communications user has not disclosed content information to a non-intermediary party, he may nonetheless lose Fourth Amendment protection if he agrees to terms that provide for monitoring or auditing of his private communications.

In *Heckenkamp*, the United States Court of Appeals for the Ninth Circuit warned that a user's "privacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that the systems administrators may monitor communications . . . ."[231] Similarly, in *United States v. Simons* the policy allowing "audit[ing], inspect[ion], and/or monitor[ing]" unwittingly terminated Fourth Amendment protection.[232] Thus, users of electronic communications systems must be wary of "terms and conditions" of use which may unintentionally terminate Fourth Amendment protections.[233]

V. DEVELOPING A *KATZ* EXCEPTION?

As the preceding *Katz* analysis suggests, a legitimate reasonable expectation of privacy in electronic communications is unlikely given the technological environment in which these communications occur.[234] However, our jurisprudence supports a flexible Fourth Amendment doctrine, which is necessary to prevent the eroding effect of advancing technologies which permit greater intrusions into the lives of citizens.[235] Rather than stretch the current *Katz* test, or apply ill-suited analogies, the Court must develop an explicit exception to its current doctrine, if privacy is to be maintained.[236]

Although the Framers of the Constitution acted to guard citizens against government intrusions into their "houses, papers, and effects,"[237] the Framers could not predict nor guard against government search and seizure of the private communi-

229. Solove, *supra* note 3, at 753.
230. *See supra* Parts I.B.1–2.
231. United States v. Heckenkamp, 482 F.3d 1142, 1147 (9th Cir. 2007).
232. United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000).
233. *See supra* notes 231–32 and accompanying text.
234. *See supra* Part IV.
235. *See infra* notes 247–49 and accompanying text.
236. *See infra* notes 250–52.
237. U.S. CONST. amend. IV.

cation networks that developed in the 200 years since.[238] When Justice Harlan announced the two pronged "reasonable expectation of privacy test," *Katz* was heralded as signaling an era of broad Fourth Amendment protection. But in the decades since its adoption, the promising future of strong Fourth Amendment protection has been weakened by the disclosure principle.[239]

Under *Katz* and the disclosure principle, users of electronic communications networks generally do not possess reasonable expectations of privacy because of the vulnerable technological environment through which the communications travel.[240] Because of this, users may be unable to avail themselves of Fourth Amendment protection where government officials engage in search and seizure of their communications. Consequently, the new frontier of electronic communications is a dangerous place for users who seek privacy for their communications.[241]

However, e-mail, text messages, and VoIP have undoubtedly each come to play an important, if not vital, role in private communications in modern American life,[242] and our Fourth Amendment jurisprudence supports ensuring protection for these forms of communications.[243] Justice Brandeis's famous *Olmstead* dissent cautioned the Court that it was its duty to develop the Amendment's flexibly, to protect against means of government intrusion into the lives of private citizens that could be invented in the future.[244] *Katz* reinforced the idea that technology could not be allowed to erode expectations of privacy.[245] *Kyllo* reaffirmed the Court's commitment to adapting to society's changing expectations of privacy, stating in dicta that technological advances could not be allowed to "whittle away" at society's expectation of privacy vis-à-vis the government.[246]

In light of our strong jurisprudential commitment to preventing the erosion of privacy by technological advances and the rapid pace at which communication technologies are developed, if the electronic communications are to receive protection it must be done through the judiciary's creation of an exception to the disclosure principles rather than through the legislative process.[247] Developing an

238. S. REP. No. 99-541, at *2 (1986).

239. *See supra* Part II.B.1.

240. *See supra* note 178 and accompanying text; *see also* Kerr, *supra* note 154, at 629 (stating that "because the contents of Internet communications are mixed together with envelope information and disclosed to the ISP, it is at least possible that courts will find that Internet users cannot have a reasonable expectation of privacy in Internet content information, much like postcards or cordless phone calls.").

241. *See supra* Part IV.

242. *See supra* note 44.

243. *See supra* notes 35–39, 44, 54, 57–58 and accompanying text; *see also infra* notes 247–49.

244. *See* Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J. dissenting).

245. *See* Katz v. United States, 389 U.S. 347, 352 (1967).

246. Kyllo v. United States, 533 U.S. 27, 34 (2001).

247. Legislative enactment is ill-suited to keep up with the changing landscape of electronic communications. Due to the rapid pace of electronic communications growth, legislative enactment is too static of a method in which to create these protections. *Cf.* United States v. McNulty (In re *Askin*), 47 F.3d 100, 105–06 (4th Cir. 1995), where the court concluded the legislature was the correct branch of government to develop the application of new technologies to the Fourth Amendment:

exception to the disclosure principles for electronic communications rather than allowing *Katz* to be stretched or to applying improper analogies to traditional communication networks[248] will create a more honest Fourth Amendment jurisprudence. The exception for electronic communications must recognize, and account for, the current impossibility of communicating through electronic communication media without revealing a message itself to non-intermediary third parties.[249] Disclosure to non-intermediary third parties should not be treated as impermissible disclosures.

CONCLUSION

Rather than analogously applying cases involving telephone or postal communications to the search and seizure of electronic communications,[250] thus ignoring important technological differences in each mode of communication,[251] courts must instead apply a reasoned analysis considering 1) the type of information revealed to third parties; 2) the nature of the third party the information was revealed to; and 3) whether the user has agreed to contractual terms limiting his Fourth Amendment rights[252] in order to more faithfully adhere to traditional Fourth Amendment reasoning in the new frontier of electronic communications.

While there are obvious similarities between these newer communications networks and traditional networks,[253] using conclusory comparative reasoning[254] fails to recognize important technological differences which distinguish these technologies,[255] especially where the technology puts content information into the hands of non-intermediary third parties.[256] Under the Supreme Court's current third party doctrine,[257] such disclosures are not entitled to the protections afforded by the Fourth Amendment.[258] Adherence to this third party doctrine establishes no reasonable expectation of privacy in many forms of electronic communications.

> In the fast-developing area of communications technology, courts should be cautious not to wield the amorphous "reasonable expectation of privacy" standard. . . . As new technologies continue to appear in the marketplace and outpace existing surveillance law, the primary job of evaluating their impact on privacy rights and of updating the law must remain with the branch of government designed to make such policy choices, the legislature . . . .

Id. at 852–53.

248. *See supra* Part III.

249. Schneider, *supra* note 115, at 376 (recognizing that the fact an electronic communications network is structurally insecure should not be dispositive in analyzing a reasonable expectation of privacy).

250. *See supra* Part II.B.

251. *See supra* Part III.B.

252. *See supra* Part IV.

253. *See supra* notes 153–58 and accompanying text.

254. *See* Gore, *supra* note 3, at 403.

255. *See supra* Part III.B.

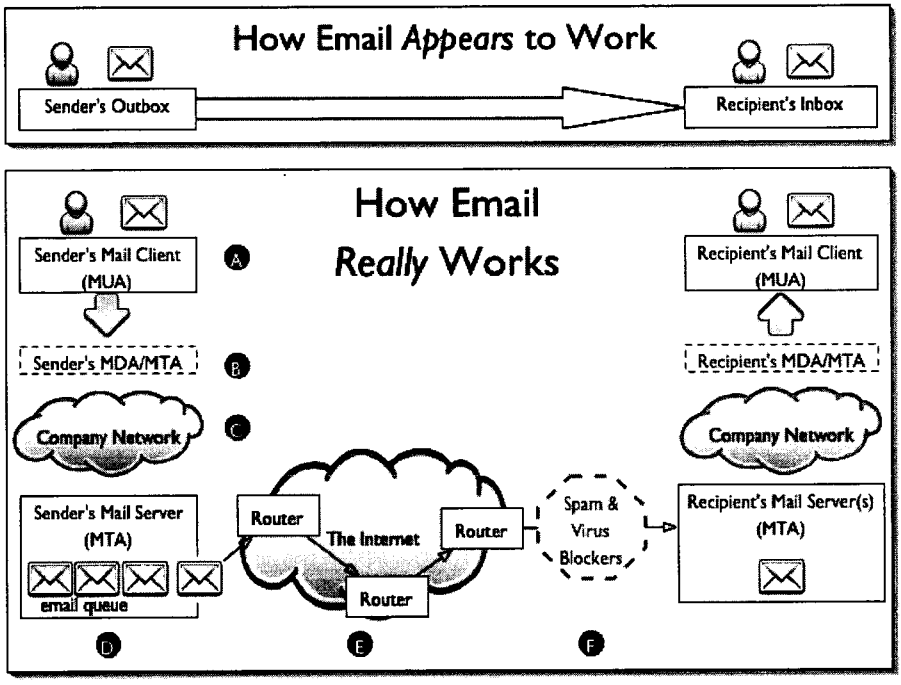
256. *See supra* Part IV.B.

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

258. *See supra* Part IV.B.

Because of the current third party doctrine, if there is to be Fourth Amendment protection for electronic communications, the Court must explicitly recognize an exception recognizing the novel technological background of electronic communications.[259]

APPENDIX A**



259. *See supra* Part V.

** http://www.oasis-open.org/khelp/kmlm/user_help/html/how_email_works.html