3-1-2008

United States v. Forrester: An Unwarranted Narrowing of the Fourth Amendment

Schuyler Sorosky

UNITED STATES V. FORRESTER: AN UNWARRANTED NARROWING OF THE FOURTH AMENDMENT

Schuyler B. Sorosky[*]

I. INTRODUCTION

The Framers lived in a world where web pages, browsers, and hyperlinks were unimaginable. Before the advent of telephones, computers, or even postage stamps, eighteenth-century America was a land of primitive technology and finite modes of communication. When the Framers drafted the Constitution and, specifically, the Fourth Amendment, they never envisaged our modern-day world of cyberspace.

Today, the Internet has become a primary means of communication and an indispensable tool for gathering information and exchanging ideas. As such, the so-called "online revolution" has generated several questions regarding Fourth Amendment searches and seizures that the Framers never anticipated. One much-debated issue involves the extent to which the government can probe into one's online activity, including web searches and electronic mail communications, consistent with the Fourth Amendment.[1]

The Framers drafted the Fourth Amendment to bar unreasonable government searches and seizures so as to safeguard individuals' privacy interests.[2] This right "to be let alone" is a well-established tenet of American society.[3] However, in today's digital world, where

---

[*] J.D. Candidate, May 2009, Loyola Law School, Los Angeles; B.A., History, University of California, Berkeley. Special thanks to Professor Marcy Strauss and the editors of the Loyola of Los Angeles Law Review for their suggestions. Most importantly, I would like to thank my family for all of their love and support.

1. *See In re* United States for Orders Authorizing the Use of Pen Registers, 515 F. Supp. 2d 325, 337–39 (E.D.N.Y. 2007).

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

3. *See* Katz v. United States, 389 U.S. 347, 360 (1967) (coining the phrase "expectation of privacy"); *see also* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L.

individuals can communicate with the mere click of a mouse and surveillance techniques have reached an unprecedented level, "there exists a fear that new technologies are eroding Fourth Amendment protections."[4] It is in this context that courts are faced with determining the appropriate application of the Fourth Amendment to the realm of cyberspace.

In *United States v. Forrester*,[5] the Ninth Circuit addressed the issue of what constitutes a Fourth Amendment search in the context of the Internet.[6] In *Forrester*, the court held, as a matter of first impression, that the use of computer surveillance techniques did not amount to a search within the meaning of the Fourth Amendment.[7] Specifically, the court held that surveillance techniques that enabled the government to discern the to/from addresses of a defendant's e-mail messages, the Internet Protocol ("IP") addresses of the websites the defendant visited, and the total volume of data transmitted to and from the defendant's account, were constitutionally sound investigative measures.[8] By this ruling, the Ninth Circuit improperly sanctioned an unwarranted narrowing of Fourth Amendment protections guaranteed by the Constitution.

This Comment argues that the Ninth Circuit erred in holding that these computer surveillance techniques do not trigger the protections of the Fourth Amendment. Part II presents a brief background of the factual and procedural history of *Forrester*. Part III provides the historical framework leading up to the case, including a discussion of the reasonable expectation standard the U.S. Supreme Court has

---

REV. 193, 195–96 (1890) (footnote omitted) (discussing in depth the privacy interests enjoyed by individuals).

4. Ric Simmons, *Technological Change and the Evolution of Criminal Law: Why 2007 is Not Like 1984: A Broader Perspective on Technology's Effect on Privacy and Fourth Amendment Jurisprudence*, 97 J. CRIM. L. & CRIMINOLOGY 531, 533 (2007) (discussing the effect of technological advances on Fourth Amendment cases and arguing for an appropriate balance between an individual's right to privacy and the government's interest in law enforcement); *see* Meir S. Hornung, Note, *Think Before You Type: A Look at Email Privacy in the Workplace*, 11 FORDHAM J. CORP. & FIN. L. 115, 118 (2005) (discussing privacy interests regarding e-mail communications in the workplace).

5. 495 F.3d 1041 (9th Cir. 2007), *reh'g denied*, 2008 WL 60506 (Jan. 7, 2008).

6. *Forrester*, 495 F.3d. at 1043.

7. *Id.* at 1048.

8. *Id.* at 1048–49. It is important to note that while I challenge the court's ultimate holding in *Forrester*, I agree with the court's ruling that surveillance techniques that enable the government to learn the volume of data transmitted to and from a defendant's account are constitutionally sound.

developed to address Fourth Amendment issues. Part IV discusses the Ninth Circuit's reasoning leading to its determination that the government's computer surveillance techniques did not amount to a Fourth Amendment search. Part V analyzes the errors the court made in its application of the reasonable expectation standard to the government's surveillance techniques in *Forrester*. Specifically, this section argues that the Ninth Circuit erroneously analogized the government's computer surveillance techniques to the use of a pen register and to surveillance of physical mail.[9] Part VI examines the implications this decision might have on future cases, focusing on the narrower role the Fourth Amendment might play in a modern technological world. Lastly, this Comment concludes that the Fourth Amendment should protect individuals' privacy interests in online activity and that courts should create new standards for judging Fourth Amendment claims involving Internet searches and electronic communications.

II. STATEMENT OF THE CASE

In May 2001, the government began computer surveillance to investigate defendants Mark Forrester and Dennis Alba for allegedly manufacturing ecstasy.[10] The government installed a "mirror port" on Alba's account with PacBell Internet, which allowed the government to monitor Alba's internet activity.[11] Specifically, the mirror port "enabled the government to learn the to/from addresses of Alba's e-mail messages, the IP addresses of the websites that Alba visited and the total volume of information sent to or from his account."[12]

Both defendants were charged and convicted in the United States District Court for the Southern District of California of conspiracy to manufacture ecstasy and other offenses concerning defendants' operation of an ecstasy-manufacturing plant.[13] After the jury trial, the district court sentenced each defendant to 360 months

9. *Id.* at 1049–50.
10. *Id.* at 1044.
11. *Id.*
12. *Id.*
13. *Id.* at 1043.

in prison, and the defendants each appealed their convictions.[14] On appeal, Alba contended that the government's computer surveillance techniques were unlawful.[15] Particularly, Alba argued that the government's investigation of his electronic mail communications and other internet activity infringed upon his privacy rights guaranteed by the Fourth Amendment.[16]

The Ninth Circuit denied Alba's contentions.[17] The court held, as a matter of first impression,[18] that the use of such computer surveillance techniques does not constitute a search under the Fourth Amendment.[19] The court reasoned that the government's computer surveillance techniques were "analogous to the use of a pen register that the Supreme Court held in *Smith v. Maryland* did not constitute a search for Fourth Amendment purposes."[20] The court also reasoned that the government's surveillance of the to/from addresses of e-mail messages and the IP addresses of websites visited is indistinguishable from government surveillance of physical mail and, accordingly, is likewise undeserving of Fourth Amendment protection.[21]

III. HISTORICAL FRAMEWORK

In 1791, the Framers drafted the Fourth Amendment to ensure "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ."[22] As such, this provision creates constitutional protection from arbitrary

14. *Id.* at 1045. Forrester's conviction was reversed on appeal due to a Sixth Amendment violation, as the court found that Forrester's waiver of his right to counsel was not knowing or intelligent. *Id.* at 1047.

15. *Id.* at 1043.

16. *Id.* at 1048–50.

17. *Id.*

18. *Id.* at 1048 ("Neither this nor any other circuit has spoken to the constitutionality of computer surveillance techniques that reveal the to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account.").

19. *Id.* at 1050.

20. *Id.* at 1043 (citation omitted) (citing Smith v. Maryland, 442 U.S. 735 (1979)). "A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed." United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1977).

21. *Id.* at 1049.

22. U.S. CONST. amend. IV.

government probing and intrusions.[23] Particularly, the Fourth Amendment secures individuals' privacy interests in their possessions from government invasion.

A. Katz

In *Katz v. United States*,[24] the Supreme Court rejected the theory that the Fourth Amendment only applies to physical intrusions.[25] In this landmark decision, the Court acknowledged that the Fourth Amendment "protects people, not places."[26] In *Katz*, the government listened to and recorded the defendant's telephone conversation in a telephone booth.[27] The Supreme Court held that such monitoring constituted a search under the Fourth Amendment, reasoning that the government's acts "violated the privacy upon which [the defendant] justifiably relied . . . ."[28]

In addition to expanding Fourth Amendment protection beyond physical invasions, *Katz* laid the foundation for determining what constitutes a search under the Fourth Amendment.[29] In his concurrence, Justice Harlan set forth a two-prong test to determine whether government action qualifies as a search.[30] According to Justice Harlan, a search requires "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[31] Under this rubric, the key to determining whether government action constitutes a search is whether the individual had a reasonable expectation of privacy in the subject of the investigation.

---

23. *See* Thomas K. Clancy, *What Is a "Search" Within the Meaning of the Fourth Amendment?*, 70 ALB. L. REV. 1, 3 (2006) (defining a Fourth Amendment search as "any intrusion with the purpose of obtaining physical evidence or information, either by a technological device or the use of the senses into a protected interest").

24. 389 U.S. 347 (1967).

25. *Id.* at 351.

26. *Id.* at 353.

27. *Id.* at 348.

28. *Id.* at 353.

29. *Id.* at 361.

30. *Id.*

31. *Id.*

B. Smith

In *Smith v. Maryland*,[32] the Supreme Court applied the *Katz* two-part inquiry to determine whether the government's actions constituted a search.[33] In doing so, the Court concluded that the use of a pen register to record dialed telephone numbers did not constitute a search under the Fourth Amendment.[34] In applying *Katz*, the Court announced that "the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action."[35]

In *Smith*, the Court concluded that the defendant did not have the requisite expectation of privacy in the numbers he dialed to sustain a Fourth Amendment claim.[36] The Court reasoned that people do not have a subjective expectation of privacy in numbers they dial because people "realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed."[37] The Court emphasized that telephone users generally understand that they convey phone numbers to telephone companies and that, in turn, the companies have the capacity to record such numerical information for business purposes.[38] According to the Court, people have no reasonable expectation of privacy in information "voluntarily turn[ed] over to third parties"[39] and, as such, an expectation of privacy in dialed phone numbers is not one society is prepared to recognize as reasonable.[40] Taken literally, *Smith* stands for the proposition that the Fourth Amendment does not protect information accessible to a third party.

---

32. 442 U.S. 735 (1979).

33. *Id.* at 740 (explaining that Harlan's two-part inquiry is used to determine whether the government invaded an individual's privacy interests).

34. *Id.* at 745–46.

35. *Id.* at 740.

36. *Id.* at 745.

37. *Id.* at 742.

38. *Id.* at 743.

39. *Id.* at 744. I will refer to this concept throughout this Comment as the "third party argument" or the "third party doctrine."

40. *Id.* at 743.

IV. REASONING OF THE COURT

In *United States v. Forrester*, the Ninth Circuit held that the government's computer surveillance techniques did not constitute a Fourth Amendment search because the defendant did not have a reasonable expectation of privacy in the to/from addresses of his e-mail messages or in the IP addresses of websites he visited.[41] In reaching its decision, the court analogized the government's computer surveillance practices to other types of surveillance techniques that the Supreme Court has held do not infringe upon privacy interests.[42] First, the Ninth Circuit analogized the government's computer surveillance techniques to the use of a pen register, which the Supreme Court held in *Smith* is a constitutionally permissible investigative device.[43] Second, the court analogized the government's surveillance of e-mail addresses to government surveillance of physical mail.[44]

A. The Court's Analogy to the Use of Pen Registers in Smith

1. Diminished Expectation of Privacy in Information Turned Over to Third Parties

Although the Supreme Court's 1979 *Smith* decision predates the internet revolution, the Ninth Circuit relied on *Smith* in reaching its decision in *Forrester*. Specifically, the Ninth Circuit determined that the computer surveillance techniques used by the government are "constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*."[45] The court reasoned that "e-mail and Internet users, like the telephone users in *Smith*, rely on third-party equipment in order to engage in communication."[46] The court emphasized that just as the telephone users in *Smith* had no expectation of privacy in the numbers they dialed due to their "imputed knowledge" that their calls are completed through third-party telephone company equipment,[47] internet users likewise have

41. 495 F.3d 1041, 1048–49 (9th Cir. 2007).

42. *Id.* at 1049.

43. *Smith*, 442 U.S. at 745–46; *Forrester*, 495 F.3d at 1049.

44. *Forrester*, 495 F.3d at 1049.

45. *Id.*

46. *Id.*

47. *Id.*

no expectation of privacy in the to/from addresses of their e-mail communications or the IP addresses of websites they search "because they should know that these messages are sent and these IP addresses are accessed through the equipment of their Internet service provider and other third parties."[48] The court asserted that both communication by Internet and communication by telephone require turning information over to third parties.[49]

2 Surveillance Did Not Reveal the Underlying Content of the Communications

The Ninth Circuit also analogized the use of computer surveillance techniques in *Forrester* to the use of a pen register in *Smith*, finding that neither mode of surveillance reveals any underlying content of the communication involved.[50] The *Smith* court reasoned that pen registers do not violate any reasonable expectation of privacy because they do not acquire the actual content of the telephone conversation at issue.[51] Instead, pen registers merely obtain the telephone number associated with a particular call, without revealing anything more about the communication itself.[52]

In *Forrester*, the Ninth Circuit reasoned that computer surveillance is indistinguishable from the use of a pen register because "e-mail to/from addresses and IP addresses constitute addressing information and reveal no more about the underlying contents of communication than do phone numbers."[53] The court explained that when the government determines the telephone numbers an individual has dialed, it may learn the identity of the parties to which the numbers correspond, but it may not uncover the actual content of the conversations.[54] Likewise, the court noted that "when the government obtains the to/from addresses of a person's e-mails or the IP addresses of websites visited, it does not find out the contents of the messages or the particular pages on the websites the

48. *Id.*
49. *Id.*
50. *Id.*
51. Smith v. Maryland, 442 U.S. 735, 741–42 (1979).
52. *Id.* at 741.
53. *Forrester*, 495 F.3d at 1049.
54. *Id.*

person viewed."[55] According to the court, the government can merely speculate about the contents of the underlying communication in either situation:[56]

> At best, the government may make educated guesses about what was said in the messages or viewed on the websites based on its knowledge of the e-mail to/from addresses and IP addresses—but this is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed.[57]

Thus, the court determined that, like the pen register, the computer surveillance techniques at issue were constitutionally sound and did not amount to a search under the Fourth Amendment.[58]

B. The Court's Analogy to Physical Mail

In *Forrester*, the Ninth Circuit also analogized e-mail communications to physical mail.[59] In drawing this comparison, the court noted: "In a line of cases dating back to the nineteenth century, the Supreme Court has held that the government cannot engage in a warrantless search of the contents of sealed mail, but can observe whatever information people put on the outside of mail, because that information is voluntarily transmitted to third parties."[60] The court reasoned that "[e]-mail, like physical mail, has an outside address 'visible' to the third-party carriers that transmit it to its intended location, and also a package of content that the sender presumes will be read only by the intended recipient."[61] Accordingly, the court concluded that "[t]he privacy interests in these two forms of communication are identical" because "[t]he contents may deserve

55. *Id.*

56. *Id.*

57. *Id.*

58. *Id.* at 1050.

59. *Id.* at 1049–50.

60. *Id.* *See* United States v. Van Leeuwen, 397 U.S. 249, 253 (1970) (holding that postal service authorities can detain mail if the package appears suspicious); *Ex parte* Jackson, 96 U.S. 727, 733 (1877) (noting that the content on the outside of mail is not protected from inspection); United States v. Hernandez, 313 F.3d 1206, 1209–10 (9th Cir. 2002) (noting that one has no reasonable expectation that postal service workers will not view the exterior of mail).

61. *Forrester*, 495 F.3d at 1050.

Fourth Amendment protection, but the address and size of the package do not."[62]

V. ANALYSIS

The Ninth Circuit should have characterized the government's computer surveillance techniques in *Forrester* as a search under the Fourth Amendment. In analogizing the government's surveillance methods to the use of a pen register and comparing electronic communications to physical mail, the court inaccurately determined that internet users do not have a legitimate expectation of privacy in their online activity. This error exposes the court's misunderstanding of the nature of the Internet and could lead to an improper narrowing of Fourth Amendment protections as applied to modern communication methods.

A. The Court's Erroneous Analogy to the Use of Pen Registers in Smith

The Ninth Circuit erred in analogizing the government's use of computer surveillance techniques in *Forrester* to the use of a pen register in *Smith*. First, the court mistakenly analogized communication by Internet to communication by telephone in that both modes of communication involve information voluntarily turned over to third parties.[63] Unlike a pen register, the computer surveillance techniques employed by the government in *Forrester* encroached upon the defendant's reasonable expectation of privacy, notwithstanding the presence of a third party internet service provider. While telephone users may not have an expectation of privacy in the telephone numbers they dial, internet users indubitably have a legitimate expectation of privacy in the e-mail addresses of parties with whom they communicate and in the IP addresses of the websites they visit. Further, courts should not apply *Smith*'s third-party doctrine when people have no viable choice but to reveal information to a third party.

Second, the court incorrectly reasoned that the computer surveillance techniques in *Forrester*, like the pen register in *Smith*,

62. *Id.*

63. *Id.* at 1049.

did not reveal any content of the actual communications involved.[64] Unlike straightforward telephone numbers, IP addresses do, in fact, convey content beyond the mere numbers displayed. This Comment discusses some examples of such exposed content in further detail in Part V.A.2.

1. Individuals Have a Legitimate Expectation of Privacy in Online Communications, Even if Turned over to Third Parties

The Ninth Circuit incorrectly applied *Smith*'s third-party argument to online communications. The court's reasoning is flawed because the court neglected to recognize that people have a legitimate expectation of privacy in their online communications and web searches, regardless of the fact that internet service providers have the potential to monitor such activity. Instinctively, internet users presume their web communications are private and, therefore, do not anticipate that clandestine government agents or internet service providers will tap into their personal online ventures. The mere possibility that a third party with the requisite expertise can learn information pertaining to an internet user's web activity does not eliminate an expectation of privacy.[65]

a. The Court's Misunderstanding

First, the court's analogy is unfounded because the nature of the Internet is fundamentally different from the third-party telephone switching equipment in *Smith*, due in part to the "non-intuitive manner by which e-mails 'travel.'"[66] Unlike other modes of communication, "e-mails are not relayed from station to station completely intact"[67] as, for example, a dialed telephone number would be. Rather, all information transmitted over the Internet is broken down into individual parts that are subsequently transmitted

64. *Id.*

65. *See* Casey Holland, Note, *Neither Big Brother Nor Dead Brother: The Need for a New Fourth Amendment Standard Applying to Emerging Technologies*, 94 KY. L.J. 393, 408–09 (2005–06) (arguing that people still have expectations of privacy in electronic communications despite the ability of certain persons with the requisite technical expertise to view them).

66. Jim W. Ko, Comment, *The Fourth Amendment and the Wiretap Act Fail to Protect Against Random ISP Monitoring of E-Mails for the Purpose of Assisting Law Enforcement*, 22 J. MARSHALL J. COMPUTER & INFO. L. 493, 507 (2004) (arguing that both the Fourth Amendment and the Wiretap Act provide poor defenses against the unprecedented threat to privacy in the Computer Age).

67. *Id.*

individually through various paths.[68] As such, one could conclude that "a reasonable expectation of privacy does exist for e-mail transmissions as to the relay stations, because an individual relay station only receives fragments of any given e-mail, and the only feasible locations from which a particular message can be intercepted are the sender's and recipient's host computers."[69] Accordingly, as Professor Ric Simmons points out, application of *Smith*'s third-party argument to the realm of cyberspace "would give the government the power to monitor every piece of electronic mail that is sent through the internet, since every electronic transmission that is sent from one person to another travels through numerous switching computers, each of which are independent third parties and any of which have the capability of recording the addresses and the content of the transmissions."[70]

Second, the court fails to recognize that individuals have a greater expectation of privacy in their online activity than in the telephone numbers they dial because unlike telephone numbers, neither e-mail addresses nor IP addresses of websites visited are displayed on monthly internet bills. As such, internet users have no reason to believe that internet service providers actually monitor online activity or maintain records of such activity in the ordinary course of business. In fact, at least one district court has recognized that individuals have a greater expectation of privacy in information that does not appear on monthly bills.[71] The United States District Court for the Eastern District of New York rejected the theory that the presence of third-party intermediaries with potential access to information negates a reasonable expectation of privacy,

68. *Id.*

69. *Id.*; *see also* Holland, *supra* note 65, at 410 ("E-mails are not like telephone calls which are terminated if the recipient does not respond. Unless an e-mail recipient's computer is on and actively receiving packets at the time the e-mail arrives, it must necessarily be placed in electronic storage on some third party's system.").

70. Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1339 (2002) (arguing that courts should apply the *Katz* test as it was originally intended by only considering the result of the search, rather than the method).

71. *In re* United States for Orders Authorizing the Use of Pen Registers, 515 F. Supp. 2d 325, 337–39 (E.D.N.Y. 2007) (determining that the use of a pen register to collect information regarding post-cut-through dialed digits—numbers dialed after a call goes through—infringes upon privacy interests, reasoning in part that such information is not kept in the ordinary course of business and does not appear on monthly bills).

acknowledging that changes "in technology [do] not alter the mandates of the Fourth Amendment."[72]

Further, the use of password protections shows that internet users have an expectation of privacy in their online and e-mail activity.[73] Most individuals implement password devices requiring the entry of a password before logging onto one's computer. Passwords are also universally used when accessing one's e-mail account. While passwords are usually required when accessing computers and e-mail accounts, passwords are usually not required when using other modes of communication—namely, the telephone. Hence, the widespread use of passwords indicates that internet users have a reasonable expectation of privacy in their online activity since through such passwords, individuals restrict public access to information on their computer and in their email accounts.[74] As a result, internet users do not anticipate that anyone will gain access to their specific online endeavors.

b. Courts Should Not Apply Smith*'s Third-Party Argument to the Internet*

Further, courts should decline to apply *Smith*'s third-party argument when individuals have no viable choice but to reveal information to a third party. In that regard, the *Forrester* court's analysis is flawed because it underestimates the fundamental role the Internet plays in contemporary society.[75] In *Katz*, the Supreme Court noted that the communications at issue were guaranteed Fourth Amendment protection because "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[76]

---

72. *Id.* at 339.

73. *See* Randolph S. Sergent, Note, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181, 1200 (1995) ("Reliance on protections such as individual computer accounts, password protection, and perhaps encryption of data should be no less reasonable than reliance upon locks, bolts, and burglar alarms, even though each form of protection is penetrable.").

74. *See* Trulock v. Freeh, 275 F.3d 391, 403–04 (4th Cir. 2001) (discussing that the use of password protections may indicate an expectation of privacy).

75. *See* Jayni Foley, Note, *Are Google Searches Private? An Originalist Interpretation of the Fourth Amendment in Online Communication Cases*, 22 BERKELEY TECH. L.J. 447, 465 (2007) (analyzing privacy protections for Internet searches).

76. 389 U.S. 347, 352 (1967).

Likewise, in his dissent in *Smith*, Justice Marshall emphasized the importance of acknowledging the widespread use of the telephone in conducting a Fourth Amendment analysis.[77] According to Marshall, a third-party intermediary capable of accessing information can negate a reasonable expectation of privacy only when the defendant exercises some choice in allowing the third party to tap into his or her communications.[78] Marshall argues that "unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. . . . It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative."[79] Thus, according to Marshall's theory, the third-party argument should not apply when a defendant relies on a mode of communication and has no choice but to continue using that mode, despite the existence of a third-party intermediary.

Courts should adopt Justice Marshall's reasoning and conclude that information conveyed to third parties via the Internet should not eliminate a reasonable expectation of privacy when individuals have no feasible choice but to reveal such information to a third party. Similar to the telephone, the Internet is now a "personal [and] professional necessity."[80] In both personal and professional life, the Internet plays a vital role in modern communication.[81] As such, in accordance with Justice Marshall's discussion, *Smith*'s third-party argument should not apply to internet activity because an individual would need to forgo using what has become a virtual necessity in modern society in order to evade the risk of surveillance. As the Sixth Circuit noted in a recent decision, "[i]t goes without saying that like the telephone earlier in our history, e-mail is an ever-increasing mode of private communication, and protecting shared communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past."[82]

---

77. 442 U.S. 735, 750 (1979) (Marshall, J., dissenting).

78. *Id.* at 749.

79. *Id.* at 750.

80. *Id.*

81. *See* Foley, *supra* note 75, at 465 (discussing that "[c]ontent disclosure to Google or other search engines is practically inevitable in order to participate in modern life").

82. Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007).

Moreover, *Smith*'s third-party argument is based, in part, on the doctrine of assumption of risk.[83] The theory holds that if an individual shares information with a third party, that individual assumes the risk that such data may be exposed to the government.[84] In cases of online browsing and electronic communications, however, people intuitively presume such activity is private. Internet users neither voluntarily provide information to third-party internet service providers nor contemplate that their private endeavors will be so exposed. In that sense, internet users cannot really assume a risk of exposure when they are not conscious of such a risk. After all, as one commentator has pointed out, the Internet "would be fundamentally altered if every user's search was recorded, mapped to an IP address, and delivered to the government."[85]

c. The Presence of a Third-Party Intermediary is Not a "Deal Breaker"

In any event, courts have found that individuals can have a reasonable expectation of privacy even when a third party is present.[86] For instance, in *Katz*, the Supreme Court acknowledged that an individual is "entitled to assume that the words he utters into the mouthpiece [of a telephone] will not be broadcast to the world."[87] Although *Katz* involved protection of the actual content of the speech in question, the Court acknowledged an expectation of privacy notwithstanding the fact that the telecommunications carrier is a third party that could potentially access such communication.[88] It follows, then, that the presence of a third party is not a "deal-breaker" with regard to expectations of privacy; if it were, the Court in *Katz* would have determined that the defendant did not have a reasonable expectation of privacy in his telephone conversations.

---

83. *Smith*, 442 U.S. at 749–50.

84. *Id.*

85. Foley, *supra* note 75, at 465.

86. *See, e.g.*, Katz v. United States, 389 U.S. 347 (1967) (holding that an individual has a reasonable expectation of privacy in his telephone conversations when using a public telephone). It is essential to note that in *Katz*, the Court does not specifically refer to the third-party telecommunications carrier. Regardless, it is a given that the telecommunications carrier is an always-present entity in telephone communications. The Court's failure to address the third-party telecommunications carrier is evidence that a privacy analysis does not hinge on the presence of such a carrier.

87. *Id.* at 352.

88. *Id.*

Similarly, in *Warshak v. United States*,[89] the Sixth Circuit acknowledged that individuals have a reasonable expectation of privacy in the content of e-mails sent or received through a commercial internet service provider.[90] Regardless of the fact that the case involved e-mail content, the court reasoned that the presence of an intermediary with the ability to access information does not negate an expectation of privacy in online activity.[91] The court recognized that the third-party argument presents a potential slippery slope since, if taken literally, "phone conversations would never be protected, merely because the telephone company can access them; letters would never be protected, by virtue of the Postal Service's ability to access them; [and] the contents of shared safe deposit boxes or storage lockers would never be protected, by virtue of the bank or storage company's ability to access them."[92] According to the court, "the service provider's control over the files and ability to access them under certain limited circumstances will not be enough to overcome an expectation of privacy . . . ."[93]

d. Forrester *is Unlike the "No Expectation of Privacy" Cases*

Forrester is distinguishable from cases where courts have found an individual has no expectation of privacy in electronic communications. First, courts have found no expectation of privacy in online activity when an individual intends to convey information to the public.[94] For example, in *Guest v. Leis*,[95] the Sixth Circuit held that individuals have no expectation of privacy in material posted on

89. 490 F.3d 455 (6th Cir. 2007).

90. *Id.* at 473 (holding that individuals have a reasonable expectation of privacy in e-mail communications).

91. *Id.*

92. *Id.* at 470.

93. *Id.* at 473; *see also* United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007), *cert. denied*, 128 S. Ct. 635 (2007) (recognizing that a university student had a reasonable expectation of privacy in his computer files, regardless of the fact that the student's computer was logged onto the university's network); Curto v. Med. World Commc'ns, Inc., No. 03CV6327(DRH), 2006 U.S. Dist. LEXIS 29387, at *24 (E.D.N.Y. May 15, 2006) (noting that in the context of attorney-client confidentiality, an employee has a reasonable expectation of privacy in e-mails and personal documents created and sent from his or her home but stored on a company laptop because it was reasonable for the employee to believe such e-mails and documents were confidential).

94. *See, e.g.*, Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001).

95. *Id.*

electronic bulletin boards, reasoning that such information is intended for public viewing.[96] Likewise, in *Warshak*, the court recognized the distinction between such public postings, where an individual lacks a reasonable expectation of privacy, and e-mail communications, where an individual has a reasonable expectation of privacy.[97] The court explained that "public disclosure of material to an untold number of readers distinguishes bulletin board postings from e-mails, which typically have a limited, select number of recipients."[98]

Second, courts have found that internet users have no expectation of privacy when they are explicitly warned that their online activity is subject to monitoring.[99] For example, in *United States v. Simons,*[100] the Fourth Circuit held that an employee lacked a reasonable expectation of privacy in the electronic files on his office computer because his employer had explicitly warned employees that such files were routinely inspected.[101] Similarly, in *United States v. Angevine,*[102] the Tenth Circuit held that a university professor who used a campus computer to download child pornography had no reasonable expectation of privacy in his internet activity because the school had warned its employees that it regularly monitored activity on the university's network.[103]

In *Forrester*, the defendant neither posted information on an electronic bulletin nor received an explicit warning that his online activity would be monitored.[104] Instead, the defendant merely engaged in electronic communications and website browsing on his personal computer in the privacy of his own home.[105] As such, the defendant had a reasonable expectation of privacy in his online activity, which should not be negated by the existence of a third-party internet service provider.

---

96. *Id.*

97. Warshak v. United States, 490 F.3d 455, 472 (6th Cir. 2007).

98. *Id.*

99. *See, e.g.*, United States v. Angevine, 281 F.3d 1130, 1134 (10th Cir. 2002); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000).

100. *Simons*, 206 F.3d 392.

101. *Id.* at 398.

102. *Angevine*, 281 F.3d 1130.

103. *Id.* at 1134–35.

104. 495 F.3d 1041, 1044 (9th Cir. 2007).

105. *Id.*

2. Surveillance of IP Addresses *Does* Reveal Content

In *Forrester*, the Ninth Circuit erroneously determined that the government's computer surveillance techniques are analogous to a pen register in that neither reveals any content of the communication involved.[106] Although the court's reasoning as applied to e-mail addresses has merit, the court's analysis concerning IP addresses is fundamentally flawed. Admittedly, e-mail addresses, like telephone numbers, reveal the party with whom a particular communication takes place, without revealing the substantive content of the actual conversation. However, IP addresses can, in fact, disclose content.

The IP addresses of websites a person visits can reveal a great deal of personal information, including the individual's interests and how he or she surfs the web.[107] According to Professor Ric Simmons, in today's overwhelmingly technological world, "the rise of the personal computer and the Internet has allowed individuals to stay in the privacy of their own home to conduct many activities which formerly had to be done in public."[108] As such, when people browse the Internet, they may visit web pages to conduct business, shop online, communicate with others, read articles, watch movies, or carry out errands from home. Hence, while IP addresses merely consist of a list of letters or numbers, they can, in fact, reveal a great deal about a person, including "the names of stores at which a person shops, the political organizations a person finds interesting, a person's sexual fetishes and fantasies, her health concerns, and so on."[109] IP addresses also reveal the topics an individual researches and, in turn, may reveal a person's "interests, hobbies, or agendas," which he or she likely intended to remain private.[110] Accordingly, such personal information disclosed by IP addresses is more akin to

106. *Id.* at 1049.

107. Posting of Daniel J. Solove to Concurring Opinions, http://concurringopinions.com/archives/2007/07/the_fourth_amen.html (July 7, 2007, 11:35 EST).

108. Simmons, *supra* note 4, at 540. "An individual today can browse and shop online for any item she might want, from clothing to cooking utensils to pornography; she can access and download almost any kind of picture, political treatise, song, or book; she can even 'develop' her own digital pictures, insert them into a pamphlet she is writing, and print multiple copies of the pamphlet for distribution later. Only twenty years ago, almost any of these tasks would require the average person to leave her home and personally visit any number of other businesses . . . ."). *Id.* (footnotes omitted).

109. Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1287 (2004).

110. Foley, *supra* note 75, at 447.

the telephone communication at issue in *Katz* than to the mere telephone numbers dialed in *Smith*.[111] Here, like in *Katz*, the surveillance reveals actual content and, as a result, deserves Fourth Amendment protection.[112]

B. The Court's Analogy to Physical Mail: Who Is the Mailman on the Internet?

The Ninth Circuit erred in determining that computer surveillance of e-mail addresses is "conceptually indistinguishable from government surveillance of physical mail."[113] The court's reasoning is tenuous; it assumes that the same privacy interests exist between electronic mail and physical mail merely because both entail an address visible to a third party.[114] That is, in the case of electronic mail, the address of the sender or recipient is visible to internet service providers, and in the case of physical mail, the address written on the outside of an envelope or package is visible to the mailman.[115] The Ninth Circuit's reasoning is erroneous because there is no mailman on the Internet.

In today's technological world, physical mail and electronic mail are fundamentally different mediums. While a postal service employee must inevitably see the address written on the outside of an envelope in order to deliver the mail to the intended recipient, there is no corresponding mailman for e-mail. In comparison to physical mail, there is no tangible third party who reads e-mail addresses in the realm of cyberspace; a mailman is a far more concrete entity than an abstract internet service provider.

Moreover, the postal system is generally a public service, while electronic mail is a private enterprise. When an individual sends a letter or package through the postal service, he or she intuitively knows that the envelope or box will be viewed by postal service

111. *Id.* at 470.

112. In United States v. Forrester, 495 F.3d 1041, 1049 n.6 (9th Cir. 2007), the court distinguishes an IP address from a URL. According to the court, "[a] URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person's Internet activity." *Id.* This argument is flawed. Even if an IP address does not reveal the particular section of a website an individual visits, it discloses the identity of the website, which reveals content in and of itself.

113. *Id.* at 1049.

114. *Id.* at 1049–50.

115. *Id.*

employees working in the public system. However, when an individual sends an e-mail, especially from a personal computer, he or she anticipates that the only person viewing the sender's or recipient's address is the party on the other end of the communication.[116] As such, the *Forrester* court erred in holding that the government's surveillance of e-mail addresses is analogous to government surveillance of physical mail.

VI. IMPLICATIONS

In today's increasingly digital world, technological innovations have armed the government with the capacity to probe into private activities. For example, the government can monitor internet usage, including electronic communications and online browsing. Now, as opposed to before the advent of the Internet, individual privacy interests are especially at risk.[117]

The Ninth's Circuit's decision in *Forrester* catalyzes a narrowing of Fourth Amendment protections as applied to internet activity and modern surveillance methods. The gravamen of the harm, it seems, is the application of *Smith*'s third-party doctrine to cyberspace. In applying *Smith* to the Internet, the Ninth Circuit essentially precludes Fourth Amendment protection to any online activity due to the presence of a third-party internet service provider. Under *Forrester*, the mere existence of an internet service provider would always negate an otherwise reasonable expectation of privacy and, in turn, prohibit a finding of a search in any case involving surveillance of internet activity. Under this rubric, Fourth Amendment protections will erode as applied to information transmitted over the Internet.

A primary concern is that *Forrester*'s narrowing of Fourth Amendment protections creates a slippery slope. It is clear that e-mail and IP addresses do not receive Fourth Amendment protection from searches under *Forrester*. It is also clear that application of

116. Courts have recognized that individuals have a greater expectation of privacy in their home than in the public sphere, as individuals enjoy the right "to retreat into [one's] own home and there be free from unreasonable governmental intrusion." Kyllo v. United States, 533 U.S. 27, 31 (2001) (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)) (holding that the use of a thermal-imaging device that detects the quantity of heat in one's home constitutes a search within the meaning of the Fourth Amendment).

117. *See* Hornung, *supra* note 4, at 117–18.

Smith's third-party doctrine to future computer surveillance cases will enable courts to deny Fourth Amendment protections by merely pointing to the existence of a third party, as the Ninth Circuit demonstrated. What is unclear, however, is the extent of this power. Where will courts draw the line? The answer to this query seems to be that there is no limit on the government's ability to invoke the third-party argument in internet cases. Without boundaries, internet subscriber information, online chats, digital photographs, and the like are all susceptible to surveillance under *Forrester*'s analysis.

In addition, *Smith*'s third-party doctrine is not viable in light of modern technology because it will change how people use the Internet. For many, the World Wide Web is a forum for private conduct. Both online searches and electronic communications are intended solely for private viewing, notwithstanding the presence of an elusive internet service provider or a potential hacker. However, the *Smith* court's rule would effectively require internet users to anticipate that all of their online activity will be monitored by third parties and subsequently inspected by the government. Further, most people perceive online activity as an anonymous enterprise.[118] This sense of anonymity becomes threatened, however, when internet users realize their actions can be constitutionally tracked.[119] The Internet will be radically different if any online activity is considered fair game for government surveillance.

VII. CONCLUSION

In *Forrester*, the Ninth Circuit was faced with the challenge of determining the appropriate application of the Fourth Amendment in the context of the Internet. The court held, as a matter of first impression, that the use of computer surveillance techniques that enable the government to learn the to/from addresses of one's e-mail messages and the IP addresses of the websites one visits does not constitute a Fourth Amendment search.[120] In reaching its decision, the Ninth Circuit set the stage for an improper narrowing of the

118. *See* Shawn C. Helms, *Translating Privacy Values with Technology*, 7 B.U. J. SCI. & TECH. L. 288, 304–05 (2001) ("[A]nonymity is an essential tool in protecting free speech and action on the Internet[.]").

119. *See id.* at 290.

120. United States v. Forrester, 495 F.3d 1041, 1050 (9th Cir. 2007).

Fourth Amendment as applied to online searches and communications.

Essentially, the Ninth Circuit erred in comparing less technologically sophisticated devices, namely pen registers and physical mail, to modern surveillance methods and internet activity. First, the Ninth Circuit incorrectly analogized the government's use of computer surveillance techniques to the use of a pen register. In doing so, the court failed to recognize that individuals have a reasonable expectation of privacy in both e-mail and IP addresses, even though an internet service provider can access such information. Second, the Ninth Circuit erroneously analogized government surveillance of e-mail addresses to government surveillance of physical mail. This comparison is problematic since, unlike the public mail system, there is no tangible mailman in cyberspace.

Instead of applying traditional rules to modern technology, courts should set new standards for determining what constitutes a search in the context of the Internet. As new technologies become more prevalent and readily available, courts must focus on limiting the government's ability to use those technologies to intrude into private activities.[121] Courts should recognize that individuals have a reasonable expectation of privacy in the to/from addresses of e-mail communications and in the IP addresses of websites they visit, notwithstanding the presence of a third party. To hold otherwise misconstrues the meaning of the Fourth Amendment as interpreted by the Framers: to secure the people from unreasonable government searches. Accordingly, "[t]he law must advance with technology to ensure the continued vitality of the Fourth Amendment"[122] so as to safeguard the privacy interests the Framers avidly sought to protect.

121. *See* Clancy, *supra* note 23, at 32.

122. Wesley Coll. v. Pitts, 974 F. Supp. 374, 384 n.7 (D. Del. 1997), *aff'd*, 172 F.3d 861 (3d Cir. 1998) (quoting S. REP. NO. 95-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3557, 3559).