Brigham Young University Journal of Public Law

Volume 22 | Issue 2 Article 9

3-1-2008

Internet Search and Seizure in *United States v. Forrester*: New Problems in the New Age of Pen Registers

Deborah Buckner

Internet Search and Seizure in *United States v. Forrester*: New Problems in the New Age of Pen Registers

I. INTRODUCTION

Katherine Kressman Taylor's well-known short story, "Address Unknown," depicts two business associates and friends who are corresponding through letters.[1] Max is a Jew living in America and conducting their shared business venture of selling artwork. The other correspondent, Martin, lives in Nazi Germany and sympathizes with the Nazi cause. Max becomes hostile after Martin refuses to hide Max's younger sister Griselle from Nazi troops, and she is killed.[2] In retaliation, Max starts writing strange codes in his letters to Martin that appear as numbers and names of paintings. The codes look highly suspicious and are designed to make it appear as if Martin is a member of an underground movement smuggling Jews out of the country. Martin responds with confusion and asks Max to stop writing him the strange letters because his mail is being monitored by the Nazi regime.[3] The letters continue, becoming more frequent and extreme. Martin writes back infuriated. He tells Max that he has no anti-Nazi sentiments and feels that Max is trying to sabotage him. The story ends with a returned letter from Max stamped "addressee unknown," implying that Martin had been captured by the Nazi regime.[4]

Taylor's story is a depiction of the Nazi government's control over civilian communication during its years of European domination. Other governments have had similar authority to confiscate and search the public's mail and other communication at will. The Framers of the United States Constitution contemplated the danger of infringement of freedom presented by governments with unbridled control over citizen property and communication. The Framers wrote the Fourth Amendment to protect the people against these abuses of government power and to safeguard certain liberties:

1. Katherine Kressman Taylor, *Address Unknown*, *in* THE ELOQUENT SHORT STORY 232 (Lucy Rosenthal ed., 2004).

2. *Id.* at 250–51.

3. *Id.* at 252–55.

4. *Id.* at 256.

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Although the example of government control in Taylor's story is an extreme one, it illustrates the dangers of too much government interference—interference that must be checked. The fine line between public welfare and individual privacy has become much more attenuated as the country's tools for accessing communication and information have become more expansive. The innovation of the telephone and the Internet has required modern legislatures to draw a line where government control ends and individual privacy begins regarding communication sent through channels provided by private corporations.

In 2008, *United States v. Forrester* presented a new question to the judiciary regarding the search and seizure of private communication: can law enforcement entities access IP numbers[5] and email to and from addresses used by a private citizen without first proving probable cause?[6] While the Ninth Circuit answered in the affirmative,[7] the Court's analysis raises questions about the rectitude of the government accessing channeling information in private communications.

Part II of this case note discusses the use of pen registers and the history of their statutory regulation. Part III describes the facts of *United States v. Forrester*. Part IV outlines the Court's reasoning in that case. Part V discusses and argues against the Court's holding that channeling information falls outside a citizen's reasonable expectation of privacy.[8] Part VI disputes the Court's assertion that the seizure of IP and email to/from addresses does not violate a citizen's right to keep the contents of communications private.

5. IP numbers are "[t]he numerical sequence that serves as an identifier for an Internet server. An IP address appears as a series of four groups of numbers separated by dots. The first group is a number between 1 and 255 and the other groups are a number between 0 and 255, such as 192.135.174.1. Every server has its own unique address." Dictionary.com, s.v. "IP Address," *available at* http://dictionary.reference.com /browse/IP%20Address (last visited Dec. 21, 2007).

6. United States v. Forrester, 512 F.3d 500 (9th Cir. 2008).

7. *Id.* at 1050.

8. *Id.* at 1048.

II. PEN REGISTERS AND THE HISTORY OF THEIR REGULATION

Pen registers record or decode "dialing, routing, addressing, or signaling information"[9] transmitted through telecommunications carriers like telephone companies and Internet Service Providers (ISPs). Pen registers were originally used to record the telephone numbers dialed to and from a particular phone.[10] However, in 2001 the US Patriot Act broadened this definition to include devices that could track routing information over the Internet.[11]

Statutes and case law have established protections against the seizure of telephone and Internet communications. Under 18 U.S.C.A. §2511, the Electronic Communications Privacy Act (ECPA), it is illegal for employees of these telecommunications carriers to intercept and disclose any wire, oral, or electronics communications including routing information.[12] However, telecommunications carriers are required to carry pen registers or similar technology that allow the interception of wire and electronic communications upon the issue of a court order.[13]

In the past, government agents who applied for such a court order had to prove probable cause. In *Katz v. United States*, the Supreme Court stated that search and seizure does not apply only to physical property. It can apply to other communications including communication transmitted through a telephone.[14] Generally, probable cause is required in order to clear the constitutional bar for search and seizure.[15] This standard was reflected in Title III, the Federal Wiretap Act, which set procedures for authorization of surveillance of oral, wire, and electronic communications.[16] This Act required a showing of probable cause before

9. *In re* Application of U.S. for an Order Authorizing use of A Pen Register and Trap on (XXX) Internet Service Account/User Name, *(xxxxxxx@xxx.com)*, 396 F. Supp. 2d 45, 47 (D. Mass. 2005) [hereinafter *Pen Register Application*] (A pen register is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication."); *see also* 47 U.S.C.A. § 1002; 18 U.S.C.A. §§ 3121–27.

10. *Pen Register Application*, 396 F. Supp. 2d at 47.

11. *Id.*; *see also* Deborah F. Buckman, *Allowable Use of Federal Pen Register and Trap and Trace Device to Trace Cell Phones and Internet Use*, 15 A.L.R. FED. 2d 537 (2006).

12. 18 U.S.C. § 2511(3)(a) (". . . a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication . . . while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.").

13. 47 U.S.C.A. §1002 (a)(1)–(2).

14. Katz v. United States, 389 U.S. 347, 353 (1967).

15. 79 C.J.S. Searches § 58 (2008).

16. Electronic Privacy Information Center (Nov. 17, 2005), http://epic.org/privacy /terrorism/usapatriot/ [hereinafter EPIC]; *see also* Center for Democracy and Technology, Government Surveillance, *The Nature and Scope of Governmental Electronic Surveillance Activity*,

a court order was issued authorizing government surveillance.[17]

However, the standard of 'probable cause' was diminished by amendments effectuated by the US Patriot Act, which removed Title III and the ECPA's requirement of showing probable cause. Under the Patriot Act, the government only has to show that "the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[18] This sudden easing of the government's burden of proof has caused a fair amount of criticism from civil liberties groups[19] and even from some members of the legislature.[20]

Under case law, communicative content known as "routing information" has always been devoid of the requirement to prove probable cause. In *Smith v. Maryland* the United States Supreme Court found that traditional Fourth Amendment protections do not apply to telephone routing information (like telephone numbers) because of the caller's lack of a reasonable expectation of privacy in those numbers and because this information does not constitute "content."[21] *United States v. Forrester* extended this reasoning to pen registers surveying the Internet. However, this extension poses problems because information collected by pen registers, including IP addresses and email to and from addresses, are qualitatively different than typical routing information. Internet users who use IP addresses and email to and from addresses have a higher expectation of privacy in that content than in telephone numbers.

(July 2006), http://www.cdt.org/wiretap/wiretap_overview.html.

17. EPIC, *supra* note 16; *see also* Center for Democracy and Technology, Government Surveillance, *The Nature and Scope of Governmental Electronic Surveillance Activity*, (July 2006), http://www.cdt.org/wiretap/wiretap_overview.html.

18. US Patriot Act §216(a)(1)(2001).

19. The Electronic Privacy Information Center is one group who have actively opposed the US Patriot Act. Electronic Privacy Information Center website, http://epic.org/epic/about.html ("EPIC is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.").

The following comes from the EPIC website:

> The events of September 11 convinced . . . overwhelming majorities in Congress that law enforcement and national security officials need new legal tools to fight terrorism. But we should not forget what gave rise to the original opposition – many aspects of the bill increase the opportunity for law enforcement and the intelligence community to return to an era where they monitored and sometimes harassed individuals who were merely exercising their First Amendment rights. Nothing that occurred on September 11 mandates that we return to such an era.

EPIC, *supra* note 16 (quoting John Podesta, USA Patriot Act—The Good, the Bad, and the Sunset, 29 HUM. RTS. MAG. 3, 4 (2002), *available at* http://www.abanet.org/irr/hr/winter02/podesta.html (last visited Jan. 21, 2008)).

20. EPIC, *supra* note 16.

21. Smith v Maryland, 442 U.S. 735 (1979).

Additionally, IP addresses and email to and from addresses and are more suggestive of content than telephone numbers.

III. THE FACTS OF *UNITED STATES V. FORRESTER*

The defendants in *United States v. Forrester*, Mr. Forrester and Mr. Alba, were convicted of conspiring to create an Ecstasy-manufacturing operation. Evidence introduced at trial showed that they created a large laboratory to be housed in an insulated sea-land container.[22] Documents presented by the government showed that the laboratory would have created 440 kilograms of Ecstasy, which would produce an estimated profit of ten million dollars a month.[23] Alba purchased chemicals for producing the Ecstasy and Forrester met with a Swedish chemist in Stockholm to learn how to produce the drug.[24]

Government agents employed computer surveillance technologies, including a pen register[25] and trap and trace devices,[26] to track email and Internet activity of the defendants.[27] The surveillance tools were employed through the defendant's Internet Service Provider (ISP), PacBell.[28] The surveillance began after the Court authorized the investigators to install a pen register to Alba's account.[29] The government was able to see the to/from addresses of those whom Alba emailed.[30] The government was also able to access the IP addresses of Internet sites that Alba accessed.[31] This provided the government with the home pages of the websites visited by Alba. An IP address is distinct from a URL[32] because an IP address does not show the particular page of the website that the individual is accessing.[33] The monitoring results

22. United States v. Forrester, 512 F. 3d 500, 506 (9th Cir. 2008).

23. *Id.*

24. *Id.*

25. For the definition of pen register, see *supra* note 9.

26. A "trap and trace device . . . captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." *Pen Register Application*, 396 F. Supp. 2d 45, 47 (D. Mass. 2005).

27. *Forrester*, 512 F.3d at 505.

28. *Id.*

29. *Id.*

30. *Id.*

31. *Pen Register Application*, 396 F. Supp. 2d at 47.

32. A URL means "Uniform Resource Locator: a protocol for specifying addresses on the Internet," Dictionary.com, s.v. "URL," http://dictionary.reference.com/browse/URL (last visited Mar. 12, 2008). It is "an Internet address (for example, *http://www.hmco.com/trade/*), usually consisting of the access protocol (*http*), the domain name (*www.hmco.com*), and optionally the path to a file or resource residing on that server (*trade*)." *Id.*

33. *Forrester*, 512 F.3d 500 at 510.

showed that Alba had sent several emails to Forrester and had accessed certain chemical websites.[34] Based on these results and other pieces of evidence, Forrester and Alba were convicted of conspiracy to manufacture and distribute ecstasy.[35] Alba appealed on the ground that the government's surveillance of his Internet activity violated his Fourth Amendment right against search and seizure.[36]

IV. THE COURT'S REASONING

The Ninth Circuit held that government surveillance of IP addresses and email to and from addresses does not violate a private party's Forth Amendment rights.[37] The Court found that individuals do not have a reasonable expectation of privacy in IP addresses and email to and from addresses. It also held that this is routing information, not content (which is protected under Supreme Court precedent). The Court cited the Supreme Court's reasoning in *Smith v. Maryland* to support its holding.

A. The Court Holds IP Addresses and Email To and From Addresses Have No Expectation of Privacy

Under the Fourth Amendment, an action does not constitute a search if there is no reasonable expectation of privacy.[38] In *Smith v. Maryland*, the Supreme Court determined that the use of a pen register to track which phone numbers were dialed from a particular residence was not a violation of the Fourth Amendment because, upon turning this information over to a telephone company, an individual no longer has an "expectation of privacy."[39] The Court reasoned that, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[40]

The Court reasoned that individuals know that employees at phone companies have access to and must use channeling information such as telephone numbers to place phone calls. Individuals who use the phone, therefore, waive their right to privacy over that channeling information by freely handing it over to the telephone company.[41] The Court in

34. *Id.*

35. *Id.* at 506.

36. *Id.*

37. *Id.* at 513.

38. *See* Illinois v. Andreas, 463 U.S. 765, 771 (1983); Osburn v. State, 44 P.3d 523, 526 (Nev. 2002).

39. Smith v. Maryland, 442 U.S. 735, 751–52 (1979).

40. *Id.* at 743–44.

41. *Id.* at 742.

Forrester used the same reasoning to hold that individuals who use the Internet have no expectation of privacy because they freely relay IP addresses and email to and from addresses to ISPs to enable the ISP to run the information through the right servers in order to send email messages or access the website.[42]

B. The Court Holds IP Addresses and Email To and From Addresses Are Not Communicative Content

The Court also cited the Supreme Court's comment that the use of pen registers without a warrant is constitutional because the registers cannot access the *content* of the communications.[43] Under Supreme Court precedent in *Katz v. United States*, communicative content cannot be accessed by the government unless the government first obtains a warrant.[44] The Court said that the government surveillance in this case was similar to that of *Smith*.[45] In *Smith*, the Court found that telephone numbers are routing information and do not consist of the content of a communication and are, therefore, immune to the restrictions set in *Katz*.[46] The *Forrester* Court found that email to and from addresses and IP addresses are analogous to telephone numbers because they are routing information and government officials accessing this information would be unable to view the content of the email messages or websites.[47]

C. The Outcome of Forrester

Thus, the *Forrester* Court held that because there is no reasonable expectation of privacy in IP and email to and from addresses that are freely given to an ISP, and because pen registers do not enable the government to view the contents of the emails or websites, there was no search, and Fourth Amendment protections do not apply.[48] Therefore, the evidence the government gathered through the pen register and presented at trial did not need to be suppressed.[49]

42. United States v. Forrester, 512 F.3d 500, 509–10 (9th Cir. 2008).

43. *Id.*

44. Katz v. United States, 389 U.S. 347 (1967) (holding there is a legitimate expectation of privacy in the contents of a telephone conversation).

45. *Forrester*, 512 F.3d at 509.

46. Smith v. Maryland, 442 U.S. 735, 741 (1979).

47. *Forrester*, 512 F.3d at 509–10.

48. *Id.* at 510.

49. *Id.*

V. DO INDIVIDUALS HAVE A REASONABLE EXPECTATION OF PRIVACY IN IP ADDRESSES AND EMAIL TO AND FROM ADDRESSES?

In order for information to be covered under the Fourth Amendment, a plaintiff must prove both that she had an expectation of privacy and that this expectation is one that society is prepared to recognize as reasonable.[50] Although judicial precedent is somewhat limited in the area of Internet communications, the courts have held that certain types of Internet communications enjoy an expectancy of privacy while others do not. Before *Forrester*, no other circuit court had addressed the issue of IP addresses and email to and from addresses. However, there are strong policy reasons why this particular type of information should enjoy an expectancy of privacy.

A. Historical Court Treatment of Internet Communications and the Reasonable Expectancy of Privacy

In the area of Internet communications, courts have held that there are many types of communications that do have a reasonable expectation of privacy. Courts have held that the content of email communications are protected because there is a reasonable expectation of privacy when those emails are stored with, or sent through, a commercial Internet Service Provider (ISP).[51] The Court in *United States v. Maxwell* held that people sending and receiving real time messages, like instant messages, have a reasonable expectancy of privacy because once the message is sent it is lost forever.[52] The Court analogized these real time messages to telephone conversations which are clearly covered by the Fourth Amendment.[53] A confidentiality agreement provided by the ISP, while not guaranteeing a constitutional expectation of privacy, is strong evidence that the user had a reasonable expectation of privacy in their online communications.[54]

On the other hand, courts have held there is not a reasonable expectation of privacy when an individual has accessed the Internet at the place of her employment.[55] Also, there is no expectation of privacy on university computers or networks[56] or on a city network without

50. *Smith*, 442 U.S. at 740; *see also* Bond v. United States, 529 U.S. 334, 338 (2000).

51. United States v. Maxwell, 45 M.J. 406, 417–18 (C.A.A.F. 1996); *see also* Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007).

52. *Maxwell*, 45 M.J. at 418.

53. *Id.* at 469–71.

54. *Id.* at 417.

55. *See* United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000).

56. *See* United States v. Butler, 151 F. Supp. 2d 82, 84 (D. Me. 2001) (holding that there was

password protection.[57] Online bulletin boards[58] and chat rooms[59] also have no expectation of privacy. Subscriber information, account information, or other "non-content" information conveyed to third parties are viewed as destroying the privacy expectation as well.[60]

The courts have not articulated a test to determine what information enjoys a reasonable expectation of privacy. Courts make this determination by looking at precedent and evaluating, on a case-by-case basis, common sense arguments to determine whether ". . . an intrusion infringes upon constitutionally protected personal and societal values."[61]

B. Individuals Do Have a Reasonable Expectancy of Privacy with Internet IP Addresses and Email Addresses

United States v. Forrester is the first circuit court case to address whether individuals have a reasonable expectation of privacy for channeling information such as email to and from addresses and IP addresses.[62] The Court relied on *Smith v. Maryland* to hold that people do not have a subjective expectation for privacy when they willfully give information over to third parties such as telephone companies.[63] However, there is evidence that many people don't believe they are waiving their right to privacy when they transmit communications to third party corporations. The dissenting opinions in *Smith* make this assertion for telephone communications. Also, the common practice of users and Internet service providers suggests that there is an even greater expectation of privacy for Internet communications than for telephone communications.

no legitimate expectation of privacy where a defendant downloaded child pornography using a university's Internet capacity and stored the pornography on the computer's hard drive).

57. *See* United States v. Barrows, 481 F.3d 1246 (10th Cir. 2007).

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

59. *See* United States v. Charbonneau, 979 F. Supp. 1177, 1185 (S.D. Ohio 1997); Commonwealth v. Proetto, 771 A.2d 823, 833 (Penn. 2001); United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996).

60. *See* United States v. D'Andrea, 497 F. Supp. 2d 117, 120 (D. Mass. 2007); Freedman v. American Online Inc., 412 F. Supp. 2d 174, 182–83 (D. Conn. 2005); United States v. Sherr, 400 F. Supp. 2d 843, 848 (D. Md. 2005); United States v. Cox, 190 F. Supp. 2d 330, 332 (N.D. N.Y. 2002); U.S. v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000); United States v. Hambrick, 55 F. Supp.2d 504, 507 (W.D. Va 1999); In re Property of Forgione, 908 A.2d 593, 607 (Conn. Super. Ct. 2006); House v. Com., 83 S.W.3d 1, 12 (Ky. Ct. App. 2001); State v. Evers, 175 N.J. 355, 441–42 (2003).

61. 79 C.J.S. *Searches* § 20 (updated Dec. 2007); s*ee also* California v. Ciraolo, 476 U.S. 207 (1986); Oliver v. United States, 466 U.S. 170 (1984); United States v. Hendrickson, 940 F.2d 320 (8th Cir. 1991).

62. United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008).

63. *Id.* at 509.

1. The Smith *dissenting opinions and their application to Internet communication*

The dissenting opinions in *Smith* suggest strong policy reasons for why communications handed to third parties should retain some expectation of privacy. These policy reasons support the assertion that Internet communications, including IP addresses and email to and from addresses, maintain a reasonable expectation of privacy.

In his dissenting opinion in *Smith v. Maryland*, Justice Marshall stated that even assuming that individuals know that phone company employees view the phone numbers they dial, "it does not follow that they expect this information to be made available to the public in general or the government in particular. Privacy is not a discrete commodity, possessed absolutely or not at all."[64] Citizens regularly entrust personal information to companies with the expectation that such information will be kept confidential. Justice Marshall continued, "Those who disclose certain facts to a bank or a phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[65]

Similar reasoning applies in Internet transactions. Just because an individual hands sensitive information to a corporation, it does not follow that the individual loses the expectation that this information will be kept confidential. Credit card numbers, social security numbers, and medical histories are just a few examples of information given to online companies, accompanied by an expectation of privacy. Consumers realize that some corporations, such as banks, hospitals, and insurance companies, perform functions that consumers cannot perform for themselves. In these situations consumers must give their private information in order to receive these services. By sharing sensitive information with the institutions, consumers do not indicate a reduced expectation of privacy, but rather show trust in the corporation's assurances of confidentiality.

Justice Marshall also criticized the Court's reasoning that an individual who conveys information to these third parties "assumes the risk" of disclosure to the government.[66] Justice Marshall stated that assuming risk implies that the parties making the communication have a choice.[67] Individuals who place telephone calls don't have the option of placing a call that doesn't go through a telephone company. Therefore,

64. Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting).
65. *Id.*
66. *Id.*
67. *Id.*

the only choice they have is either to make a call through a telephone company and open their communications to government surveillance or forgo making phone calls at all. This is an impracticable choice for, as Justice Marshall said, making telephone calls is "a personal and professional necessity."[68]

The Court in *Forrester* created the same dilemma identified by Justice Marshall in *Smith*. Under the Court's reasoning, users have to choose between refraining from Internet usage or submitting to government surveillance. In reality, this is not much of a choice. Like telephone calls, the Internet has become a personal and professional necessity. Few would, or arguably *could*, choose to forgo the benefits provided by the Internet even if they were aware that they may be watched. However, it is doubtful that individuals know they are opening themselves to government surveillance every time they log onto the Internet. Even assuming individuals were aware that their private communications could be monitored by the government, this does not mean individuals who use the Internet are consciously assuming a risk or waiving their expectation of privacy since, as Justice Marshall said, assuming risks requires a practicable choice.[69]

Justice Stewart, joined by Justice Brennan, also dissented from the *Smith* opinion. Stewart commented that the rationale used by the *Smith* majority has no sound application. He stated that an individual not only hands over telephone numbers to a company when making a call; the individual also gives the company access to their phone conversations.[70] Following the Court's line of reasoning—that anything handed to a third party is no longer expected to be private—the government should have access to the content of the individual's conversation as well: a position which squarely conflicts with the Fourth Amendment.[71]

Stewart also cited *Katz* as holding that there is a greater expectation of privacy depending upon the context in which the communication was made. In *Katz* the Court stated that this expectation is greater if telephone calls are made from private areas such as a telephone booth, one's home, or one's office.[72] Likewise, Internet communications are regularly made

68. *Id.*

69. *Id.*

70. *Id.* at 746–47 (Stewart, J., dissenting).

71. *Id.*; *see* Katz v. United States, 389 U.S. 347 (1967) (holding that there is a legitimate expectation of privacy in the contents of a telephone conversation).

72. *Id.*; Katz v. United States, 389 U.S. 347, 352 (1967). The Court in *Katz* says, "We have never suggested that this concept [of constitutionally protected areas] can serve as a talismanic solution to every Fourth Amendment problem." However, in its reasoning the Court did regard the context as a pertinent consideration in determining whether there is a reasonable expectation of privacy.

from one's home or private office. The Court in *Forrester* declined to look at the objective circumstances surrounding the location of the defendant when he made Internet communications and whether the location would have suggested a greater expectation of privacy from the user. It is likely that, since the pen register was installed on Alba's personal PacBell account[73], many of the Internet communications that the government surveyed were in Alba's home. The Court, however, chose to establish a standard that applies uniformly to all Internet communications, regardless of their context.

These dissenting opinions present strong reasoning to rebut the ruling of the majority's opinion in *Smith* (that communications handed to third parties have no expectation of privacy). Likewise, these same policy reasons, as expressed by the dissent, support the notion that Internet communications, though given to third parties, should retain a reasonable expectation of privacy.

2. Internet communication carries a stronger reasonable expectation of privacy than telephone communications.

There are several differences between Internet communications and telephone communications that suggest that individuals have a greater expectation of privacy for their Internet communications. Many common practices of Internet Service Providers and Internet users suggest this greater expectation.

One such practice is privacy agreements. Many corporations, and increasingly, online corporations, have privacy agreements assuring customers that they will keep their information confidential. This added assurance of security increases customer confidence, inducing many individuals to overcome the fear of making transactions with personal information released to the organizations. As acknowledged by the Court in *U.S. v. Maxwell*, a privacy agreement is an indication that an individual has a greater expectancy of privacy.[74]

Additionally, legislation such as the Electronic Communications Privacy Act (ECPA)[75] gives the public more reason to expect privacy when making a phone call or giving information over the Internet. The Act provides that employees working for communication services cannot obtain or divulge the contents of any communication.[76] It also provides

73. United States v. Forrester, 512 F.3d 500, 505 (9th Cir. 2008).

74. United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996).

75. 18 U.S.C.A. § 2511.

76. 18 U.S.C.A. § 2511 3(a) ("A person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication . . . while in

that such information can only be acquired by obtaining a court order or a warrant.[77] This and other privacy legislation gives the public a reasonable expectation of privacy in regard to their Internet communications.

The practice of sending billing and use records is another difference between phone companies and ISPs that suggest a higher expectation of privacy. Professor Steven M. Bellovin,[78] professor of computer science at Columbia University, opined that the reasoning of the court in *United States v. Forrester* is far too broad.[79] He comments that the applicability of pen registers to the Internet introduces several privacy problems that do not exist with telephone corporations—problems that the Court in *Forrester* does not address.[80]

Bellovin remarks that customers of telephone corporations regularly receive telephone bills in the mail with a record of all of the telephone numbers dialed throughout the month.[81] These bills put the customer on notice that the numbers are actually being recorded for corporate records. In fact, the notice provided by monthly bills is something that the Court in *Smith* identified as increasing the reasonable expectation of privacy.[82] An ISP, on the other hand, does not give its customers such a record, so the customer may be ignorant that such records exist. Bellovin believes that the public is generally unaware of how ISPs work and that many customers may believe that their routing information is kept far more private when submitted through an ISP than when dialed through a telephone corporation.[83] Therefore, these individuals may have a heightened expectation of privacy when they use the Internet.[84]

The Court in *Forrester* erred in presuming that the public has no expectation of privacy when it hands private information to corporations. Many consumers give confidential information to corporations with an understanding that the corporation will keep it from being accessed by private parties. This understanding is reflected in the ECPA. The Court also failed to account for the potential differences in the public's expectation of privacy for information given to telephone companies as

transmission on that service to any person or entity other than the addressee or intended recipient of such communication or an agent of such addressee or intended recipient.").

77. 18 U.S.C.A. § 2511 2(a)(ii)(A)–(B).

78. Steven M. Bellovin biography (Feb. 15, 2008), http://www.cs.columbia.edu/~smb /informal-bio.html.

79. Steven M. Bellovin Blog, SMBlog for July 7, 2007, http://www.cs.columbia.edu/~smb /blog/2007-07/2007-07-07.html [hereinafter Bellovin Blog].

80. *Id.*

81. *Id.*

82. *See* Smith v. Maryland, 442 U.S. 735, 742 (1979).

83. Bellovin Blog, *supra* note 79.

84. *Id.*

opposed to Internet routing information.[85] These differences include the public's lack of awareness that ISPs actually record their routing information and the fact that some individuals don't use ISP's or other corporations to route information through the Internet.

VI. ARE INTERNET IP ADDRESSES AND EMAIL TO AND FROM ADDRESSES COMMUNICATIVE CONTENT?

The Court in *Katz* found that it was against the Fourth Amendment for police to seize the contents of a telephone communication.[86] This has also been applied to the contents of Internet communication. For example, 18 U.S.C.A. § 3121 limits the information that a government agency may acquire through a pen register to "dialing, routing, addressing, and signaling information" and forbids obtaining the contents of any wire or electronic communication.[87] The Court in *United States v. Maxwell*, explicitly ruled that there is an expectation of privacy in the contents of emails stored by ISPs and that the government cannot access the contents of these emails without first receiving a warrant.[88] The Court in *United States v. Forrester* stated that "pen registers do not acquire the *contents* of communications" and that the information the pen registers do pick up (routing information such as Internet IP addresses and email to and from addresses) are not content.[89] The *Forrester* Court also said that email to and from addresses and IP addresses are indistinguishable from addresses on physical mail.[90]

However, unlike telephone numbers and addresses, the IP addresses and email to and from addresses obtained by an Internet pen register may contain information that suggests content. The Court in *Smith v. Maryland* stated that pen registers installed on telephones do not convey

85. In cases regarding the Internet, the judiciary has very little precedent or statutory law to apply. The Internet presents a whole new area of law where "the terrain is unsettled" and "[t]he scholarly field studying these topics is still emerging." John Palfrey, Berkman Center at Harvard Law School, http://blogs.law.harvard.edu/palfrey/2007/04/23/ (go to "Key Themes of Internet, Law and Politics 2007") (last visited January 21, 2008). Additionally, the inherent differences between the Internet and other communication devices make it difficult for the court to faithfully analogize to precedent.

86. Katz v. United States, 389 U.S. 347, 353 (1967).

87. 18 U.S.C.A. § 3121(c) (2001) ("A government agency authorized to install and use a pen register or trap and trace device . . . shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.").

88. United States v. Maxwell, 45 M.J. 406 (1996); *see also* Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007).

89. United States v. Forrester, 512 F.3d 500, 509–10 (9th Cir. 2008).

90. *Id.* at 511.

content because they ". . . disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers."[91] Thus, a typical telephone pen register generally does not reveal content. The types of pen registers used on ISP's, however, have the potential of revealing much more content than a typical telephone pen register.

Internet routing information is distinguishable from telephone numbers and mailing addresses because it is more likely to reveal content. In response to the increased government discretion regarding Internet routing information that the US Patriot Act gives, the EPIC states the following:

> The fact that the provision prohibits the capture of 'content' does not adequately take into account the unique nature of information captured electronically, which contains data far more revealing than phone numbers, such as URLs generated while using the Web (which often contain a great deal of information that cannot in any way be analogized to a telephone number).[92]

In *In re Application of U.S. for an Order Authorizing use of A Pen Register and Trap on (XXX) Internet Service Account/User Name, (xxxxxxxx@xxx.com)* (*Pen Register Application*), the Court responds to an application by the U.S. government to obtain the Court's permission to use a pen register to monitor the Internet activity of four Internet service accounts.[93] The Court gives a brief history of pen registers, writing that pen registers were typically used in telephone communications and have only recently been used to obtain Internet routing information.[94] The Court explained that the use of pen registers to track telephone communications are usually legal because they are unable to track the contents of telephone conversations; however, using pen registers to track Internet communications creates greater problems.[95] The Court listed a few potential situations where pen registers, if not limited by the ISP, could record the *contents*[96] of these

91. Smith v. Maryland, 442 U.S. 735, 741 (1979) (quoting United States v. New York Tel. Co., 434 U.S. 159, 167 (1977)).

92. EPIC, *supra* note 16.

93. 396 F. Supp. 2d 45, 46 (D.Mass. 2005).

94. A traditional "pen register" only records telephone numbers. The court in this case also refers to "mirror ports."

95. *Pen Register Application*, 396 F.Supp.2d 45, 47–48 (D. Mass. 2005).

96. "Contents," under 18 U.S.C. § 2510(8), include ". . .any information concerning the

communications.[97] Email "subject lines" could be obtained through the use of Internet pen registers, which would reveal the contents of the communications.[98] Problems would also arise if the user had put a search term into Google or another search engine.[99] The URL derived from the IP address would contain the search words the individual used.[100] This would certainly alert the Government to the "content" that the user was seeking.[101] The Court also commented that IP addresses themselves would allow the government to determine the home page of the website that the user under surveillance was accessing.[102]

The Court in *Forrester* acknowledged that the home page of a website could be accessed simply by using the IP address.[103] However, the Court reasoned, the information derived from the IP address is different from that of a URL.[104] A URL would allow a user to find the very webpage that the user under surveillance had accessed, whereas, the IP address would only allow the government to view the home page of the website and not the actual page the user was viewing. The Court used the example of the New York Times website. A URL would take you to a particular article while the IP address would only take you to www.nytimes.com, the company's home page.[105]

However, despite the fact that access to only a home page tends to reduce the ability of the government to access the specific content that the user under surveillance accessed, viewing the home page would still suggest that content. The general content of most web pages can be suggested by viewing the home page. Viewing the home page of a site that teaches someone how to cook French food would suggest that the user wanted to get some French recipes. The home page of a site on how to chemically manufacture ecstasy would imply that the individual was seeking to make it himself. Allowing IP addresses like these into evidence would implicate guilt for anyone, even individuals who may have stumbled across sites like these inadvertently.

This suggestive content does not have the benign quality of typical routing information like telephone numbers and mailing addresses.

substance, purport, or meaning of that communication."

97. *Pen Register Application*, 396 F. Supp. 2d at 48–49.

98. *Id.* at 48.

99. *Id.* at 49.

100. *Id.* at 49.

101. *Id.* at 49.

102. *Id.* at 48. IP addresses, if typed into the web address bar, take a user to the home page of the website that the user under surveillance was accessing.

103. United States v. Forrester, 495 F.3d 1041, 1049 (9th Cir. 2007).

104. *Id.*

105. *Id.*

Phone numbers and mailing addresses do not suggest the content of the message. Instead, the information is directive in nature. Even if the government agent intercepting this routing information were to discover the communication's destination, this would reveal *location* and not *content*. The Internet is unique in that the very form of its routing information not only reveals *location* but, in some instances, reveals *content*. It allows users to deliver and receive content from a specific location but that location is typically labeled with a director or word that describes the content of the site. While limiting the director to the home pages restricts the government's ability to see exactly what the user was viewing, it doesn't eliminate the problem that a home page typically infers the type of content viewed by the user.

While this is most typically true with IP addresses, it can also occur with email to and from addresses. Many times the local part of the address or the domain name can reveal the nature of the contents of the email. For instance, the email address for the admissions department at Montana State University is admissions@montana.edu.[106] An agent reading this information recovered by a pen register could infer that this communication involved a question involving admissions to Montana University.

The Court in *Pen Register Application* stated that because IP addresses are susceptible to revealing content, the court order to place a pen register on a specific user account needs to limit the types of information that an ISP can release to the government during surveillance.[107] In *Forrester*, the defense counsel made a motion to discover the information obtained by the government with the pen register on Alba's user account. The defense lawyer wanted the application in order to see if the order had included restricting instructions of the type required by the Court in *Pen Register Application.* He requested the application because, according to his expert—Marcus Lawson, a computer specialist and a former U.S. Customs Special Agent—". . . the intrusion on the computer traffic of Mr. Alba was extensive" and suggested that Mr. Alba's ISP used the pen register to obtain the content of Mr. Alba's Internet communications in addition to routing information.[108] The Court in *Forrester* did not go into a discussion about the precise types of information gathered by the pen register, which, according to Lawson, may have included content.

106. Montana State University information request page (Mar. 6, 2008), http://www.montana.edu/wwwnss/need_info.shtml.

107. 396 F. Supp. 2d at 48–49.

108. United States v. Alba, 2006 WL 2967374, 11 (Mar. 8, 2006) (Brief for the Appellant).

IP addresses and email to and from addresses are atypical because rather than simply direct the reader to where the content is to be sent, received, or viewed, they suggest the content of the communications themselves. This is why the courts need to be cautious when analogizing between typical routing information, like telephone numbers and mailing addresses, and Internet routing information. Courts need to also be cautious to include instructions limiting the amount of information to be obtained from an ISP with a pen register as pen registers have the capacity of revealing email subject lines and search terms.

VII. CONCLUSION

The Court concluded their opinion in *Forrester* by stating that even if the evidence obtained through the pen registers should have been suppressed it would be a harmless error not to suppress. The Court explained:

> The evidence obtained through the computer surveillance was never introduced at trial and was used only as a minor portion of the government's application for a court order authorizing imaging and keystroke monitoring. There was more than enough other evidence in that application to generate probable cause even if the to/from addresses of Alba's emails, the IP addresses he accessed and the volume of data transmitted to or from his account had been suppressed. The discussion of the computer surveillance . . . revealed only that Alba had sent emails to Forrester and accessed certain chemical websites.[109]

The results from the pen register, as well as the large amounts of other evidence, made it clear that Alba and Forrester were guilty of planning the ecstasy manufacturing operation. The Court's analysis in this case clearly produced a just result. However, their reasoning may endanger other defendants whose guilt is less apparent. The Court's failure to recognize the inherent differences between telephone and Internet communications may affect the ability of later courts to give such defendants a just result.

The Court failed to acknowledge that most members of the public do not consider giving private information to a corporate entity an invitation to offer that information to the public or government officials. It also failed to realize that although *Smith* found telephone numbers to have no expectation of privacy, many individuals may have a higher expectation

109. United States v. Forrester, 512 F.3d 500, 513 (9th Cir. 2008).

of privacy for information given electronically through ISPs than telephone companies who record those numbers in a monthly bill.

Additionally, the Court failed to recognize that IP and email addresses may be more suggestive of the content of the communication than a telephone number. Telephone numbers do not contain information such as the identity of the callers, the purport of the communication, nor whether the call was even completed.[110] In contrast Internet communications received through a pen register may more specifically identify the person who is making the communication, and may, if not checked, reveal such information as email subject lines, home pages, and search terms.

Deborah Buckner[*]

110. Smith v. Maryland, 442 U.S. 735, 741 (1979) (citing United States v. New York Tel. Co., 434 U.S. 159, 167 (1977)).

[*] J.D Candidate, April 2009, J. Reuben Clark Law School, Brigham Young University.