

Automation and the Fourth Amendment

Matthew Tokson*

ABSTRACT: The Supreme Court has held that an individual relinquishes any Fourth Amendment interest in information that he or she voluntarily discloses to a third party. Known as the “Third Party Doctrine,” this controversial rule is increasingly problematic in an age where a large proportion of personal communications and transactions are carried out over the Internet. Internet users expose virtually all of the information they generate online—e-mails, web-surfing histories, search terms, and more—to online service providers. As such, many scholars have assumed that Internet information will be unprotected by the Fourth Amendment.

Yet the information disclosed to these online third parties is generally not exposed to human beings at all; rather, it is processed entirely by automated equipment. Neither courts nor scholars have squarely addressed whether disclosure to these automated third parties is sufficient to eliminate Fourth Amendment protection. However, courts have, without discussing the issue, already begun to treat automated Internet systems as the equivalent of human beings.

This Article examines how this emerging body of law threatens to deprive personal information on the Internet of effective legal protection. It offers a novel theoretical and legal analysis of information disclosure to automated Internet systems and concludes that individuals whose information is exposed only to automated systems incur no cognizable loss of privacy. It then examines available data about the behavior and privacy expectations of Internet users that reveals that they sharply distinguish between disclosure to humans and disclosure to automated systems, even if courts thus far have not. These relatively intuitive concepts have been widely overlooked, and they have potentially enormous implications in several areas of law and theory. This Article explores these implications, challenging existing privacy

* Bigelow Fellow, The University of Chicago Law School. For helpful comments and suggestions, thanks to Erica Andersen, Lisa Bernstein, Mary Anne Franks, Stephen Henderson, Orin Kerr, Saul Levmore, Jonathan Masur, Paul Ohm, Adam Samaha, Lior Strahilevitz, and workshop participants at the University of Chicago Law School and the Privacy Law Scholars Conference. Special thanks to Jacob Hamann and David Mindell for excellent research assistance.

market theories and conceptions of user behavior, and proposing a new model of Fourth Amendment privacy on the Internet.

I.	INTRODUCTION.....	583
II.	THE FOURTH AMENDMENT AND THE AUTOMATION RATIONALE	588
	A. <i>THE IMPORTANCE OF FOURTH AMENDMENT PROTECTION FOR ONLINE DATA</i>	588
	1. The Government and Personal Online Data	589
	2. The Weakness of Statutory Protection	591
	B. <i>THE THIRD PARTY DOCTRINE AND THE AUTOMATION RATIONALE</i>	596
	1. The Third Party Doctrine after <i>Katz</i>	598
	2. The Automation Rationale.....	600
III.	AUTOMATION ON THE INTERNET.....	601
	A. <i>INTERNET INFORMATION AND EXPOSURE TO AUTOMATED SYSTEMS</i>	602
	B. <i>INTERNET INFORMATION AND EXPOSURE TO HUMAN BEINGS</i>	604
IV.	THE INTERNET USER, AUTOMATION, AND PRIVACY.....	609
	A. <i>A THEORETICAL ANALYSIS OF DISCLOSURE TO AUTOMATED SYSTEMS</i>	611
	1. Privacy Theories and the Human Observer	611
	2. The Human Observer in Fourth Amendment Law.....	615
	3. The Centrality of Human Observation.....	616
	B. <i>INTERNET USER ATTITUDES AND BEHAVIOR</i>	619
	1. Internet User Survey	622
	2. Other Evidence	627
V.	DOCTRINAL AND THEORETICAL APPLICATIONS.....	629
	A. <i>THE CHOICE</i>	629
	1. The Current Confusion	631
	2. The “Rental Property” Paradigm	633
	B. <i>THE FUTURE OF KATZ ON THE INTERNET</i>	636
	1. The Content/Noncontent Alternative	636
	2. <i>Katz</i> Without the Automation Rationale and the Dangers of Analogy.....	638
	3. Burdening Law Enforcement.....	640
	4. Statutory Alternatives	642
	C. <i>THEORETICAL AND OTHER IMPLICATIONS</i>	643
	1. Future Issues in Law and Automation	643
	2. Targeted Advertising.....	644
	3. Privacy Markets.....	645
VI.	CONCLUSION	647

I. INTRODUCTION

In 1928, the Supreme Court determined that the Fourth Amendment did not apply to telephone conversations.¹ Government officials could therefore wiretap conversations at will, so long as they did not trespass on private property.² In the ensuing years, the Justice Department, and particularly the FBI, listened in on and recorded a staggering number of personal communications. From 1941 to the mid-1960s, the FBI alone recorded up to half-a-million conversations in the course of targeting at least 13,500 organizations and individuals for electronic observation.³ With oral communications unguarded by the Fourth Amendment and receiving only weak statutory protection (and not even that before 1934⁴), no conversation was off limits to federal surveillance. Federal agents eavesdropped on calls between attorneys and their clients⁵ and recorded the personal conversations of several sitting Supreme Court justices.⁶ They placed wiretaps on the telephones of celebrities, activists, journalists, and Congressmen.⁷ The FBI used the information it gathered for an extraordinary variety of purposes: to collect evidence on Mafia members, bootleggers, and potential spies;⁸ to monitor left-wing and right-wing political groups;⁹ to intimidate or discredit Congressmen investigating the FBI's activities;¹⁰ to influence the selection of the Chief Justice of the Supreme Court;¹¹ and to attempt to ruin Martin Luther King, Jr.'s reputation and induce him to commit suicide.¹² The widespread use of

1. *Olmstead v. United States*, 277 U.S. 438, 466 (1928), *overruled by* *Katz v. United States*, 389 U.S. 347 (1967), *and* *Berger v. New York*, 388 U.S. 41 (1967).

2. *Id.* at 457.

3. ALEXANDER CHARNS, *CLOAK AND GAVEL: FBI WIRETAPS, BUGS, INFORMERS, AND THE SUPREME COURT* 17 (1992).

4. Communications Act of 1934, ch. 652, § 605, 48 Stat. 1064, 1103-04 (codified as amended at 47 U.S.C. § 605 (2006)).

5. CHARNS, *supra* note 3, at 52; CURT GENTRY, *J. EDGAR HOOVER: THE MAN AND THE SECRETS* 372 (1991).

6. CHARNS, *supra* note 3, at 17-18; GENTRY, *supra* note 5, at 630.

7. GENTRY, *supra* note 5, at 51, 119, 137, 228-29, 237, 246, 472, 501, 680; RONALD KESSLER, *THE BUREAU: THE SECRET HISTORY OF THE FBI* 78 (2002).

8. GENTRY, *supra* note 5, at 230, 333, 346-49; KESSLER, *supra* note 7, at 78, 103.

9. GENTRY, *supra* note 5, at 137, 564; KESSLER, *supra* note 7, at 78.

10. GENTRY, *supra* note 5, at 119, 588.

11. CHARNS, *supra* note 3, at 24-31.

12. KESSLER, *supra* note 7, at 144. The FBI wrote anonymously to King and threatened to disclose evidence of his extramarital affairs to the public if he did not kill himself within thirty-four days, calling him "a colossal fraud and an evil, vicious one at that" and warning him, "There is but one way out for you. You better take it before your filthy, abnormal fraudulent self is bared to the nation." GENTRY, *supra* note 5, at 572. The FBI, which had been wiretapping King for years, shared information on King's private life with governors, ambassadors, U.N. representatives, British officials, journalists, and later, King's wife, eventually driving King into a deep depression. *Id.* at 529, 571-76.

warrantless wiretaps and bugs did not stop until the late sixties, essentially dying out following the Supreme Court's decision to reverse course after nearly forty years and declare that the Fourth Amendment does apply to private conversations in *Katz v. United States*.¹³

Today, as the Internet has begun to reshape the way we engage in commerce, politics, social relationships, and practically every aspect of modern life, we appear to be racing towards another enormous gap in legal protection for private communications. Virtually every form of personal data on the Internet, no matter how revealing, seems likely to remain unprotected by the Fourth Amendment,¹⁴ and again to receive only ineffectual statutory protection.¹⁵ The root cause is essentially the same as it was in 1928's *Olmstead v. United States*¹⁶: the difficulty of applying an older, relatively static body of law to a new and rapidly changing technology.

The applicable law was developed long before the advent of the Internet, in a series of cases involving government informants¹⁷ and, later, bank and telephone records.¹⁸ In deciding these cases, the Supreme Court created the "Third Party Doctrine," which provides that the Fourth Amendment does not apply to personal information disclosed to a third party and obtained by the government from that party. In *Smith v. Maryland*, for instance, the Court held that the Fourth Amendment did not apply to the telephone numbers that a customer dialed, because the numbers were regularly disclosed to the telephone company in the ordinary course of business.¹⁹ In an important but little-noticed portion of the opinion, the Court ruled that the telephone company's decision to automate the process of connecting telephone calls was irrelevant to the Fourth Amendment

13. 389 U.S. 347, 353 (1967); see *Berger v. New York*, 388 U.S. 41 (1967); CHARNS, *supra* note 3, at 91; KESSLER, *supra* note 7, at 60; see also CHARNS, *supra* note 3, at 77 (stating that "the good old days of agents' tapping and bugging without warrants were coming to a close" in 1966 as the Justice Department increasingly disclosed wiretapping procedures to the courts, potentially exposing the FBI to lawsuits); GENTRY, *supra* note 5, at 593-94 (stating that Hoover ordered most wiretapping and bugging to cease in 1966, due to increasing controversy over FBI wiretapping practices and coinciding with Solicitor General Thurgood Marshall's disclosure of wiretapping practices to the Supreme Court). Richard Nixon and his aides famously employed wiretapping for political purposes, but did so despite their knowledge that the program was clearly illegal. This limited program of clandestine wiretapping was orchestrated directly by the White House and Nixon's reelection committee rather than through official channels. See, e.g., CARL BERNSTEIN & BOB WOODWARD, *ALL THE PRESIDENT'S MEN* 270 (1974).

14. See, e.g., Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 528-29 (2006); Peter P. Swire, *Katz Is Dead. Long Live Katz.*, 102 MICH. L. REV. 904, 910-13 (2004).

15. See *infra* Part II.A.2.

16. 277 U.S. 438 (1928).

17. See, e.g., *Lopez v. United States*, 373 U.S. 427 (1963); *On Lee v. United States*, 343 U.S. 747 (1952).

18. *Smith v. Maryland*, 442 U.S. 735 (1979); *United States v. Miller*, 425 U.S. 435 (1976).

19. 442 U.S. at 744.

inquiry.²⁰ Rather, the automated equipment was merely the “modern counterpart” of the human operators who had personally completed calls for telephone customers for decades.²¹

The Third Party Doctrine precedents, and *Smith* in particular, are problematic in an age where an ever-growing proportion of personal communications and transactions are carried out over the Internet. Internet users, now comprising eighty percent of U.S. citizens,²² generate enormous amounts of personal data online, virtually all of it accessible to third-party Internet service providers (“ISPs”) or websites. E-mails, web-surfing histories, credit card and address information, and search term records are all routinely stored by online entities and are potentially available to the government, or even to private parties that purchase customer information for marketing purposes.²³ With the Fourth Amendment inapplicable to this mass of easily obtainable personal information, government investigators could monitor the communications of individuals and organizations on an unprecedented scale.²⁴

While *Smith* and the Third Party Doctrine were heavily criticized even before the Internet age,²⁵ the drumbeat of criticism has intensified²⁶ as scholars have begun to recognize that the Doctrine may allow collecting vast amounts of personal online data at very low cost. These scholars have a

20. *Id.* at 744–45.

21. *Id.* at 744.

22. CTR. FOR THE DIGITAL FUTURE, USC ANNENBERG SCH., THE DIGITAL FUTURE PROJECT 2009, at 29 (2009).

23. See Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1093–94 (2002); *infra* Part III.A.

24. See *infra* notes 26, 53.

25. See, e.g., Gerald G. Ashdown, *The Fourth Amendment and the “Legitimate Expectation of Privacy,”* 34 VAND. L. REV. 1289, 1315 (1981); Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1254–56 (1983); Scott E. Sundby, *“Everyman”’s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1757–58 (1994).

26. See, e.g., CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 151–64 (2007); Jack M. Balkin, Essay, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 19 (2008); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL’Y 211, 242–44 (2006); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 976 (2007); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 113–14 (2008); Solove, *supra* note 23, at 1137–38; Andrew J. DeFilippis, Note, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1092 (2006); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶¶ 46–49, <http://str.stanford.edu/pdf/freiwald-first-principles.pdf>; Matthew D. Lawless, Note, *The Third Party Doctrine Redux: Internet Search Records and the Case for a “Crazy Quilt” of Fourth Amendment Protection*, 2007 UCLA J.L. & TECH. 2, ¶¶ 9–12, http://www.lawtechjournal.com/articles/2007/02_070426_lawless.pdf.

point. The Doctrine, although highly unlikely to be overturned,²⁷ certainly favors law-enforcement interests and poses a threat to privacy on the Internet. This Article argues, however, that an even greater threat is posed by courts' failure to distinguish between the disclosure of personal information to automated equipment and disclosure to a human being. Indeed, this failure, which has received little attention in the privacy literature, can be blamed for much of the persistent confusion among courts (and scholars) as to how to determine whether the Fourth Amendment protects personal online data.

The conflation of disclosure to automated Internet systems with disclosure to human beings may lead unwitting courts to drastically underprotect personal information transmitted over the Internet. In fact, courts have already begun to do so, holding that the Fourth Amendment does not apply to Internet protocol ("IP") addresses,²⁸ e-mail to/from information, information about the volume of data transmitted to a user,²⁹ name, address, and credit card information,³⁰ and even the contents of a user's e-mails³¹ on the basis of their disclosure to automated equipment. Simply put, the "automation is irrelevant" rationale of *Smith* threatens to undermine privacy rights in Internet data and potentially in all new communications technologies, present and future.

This Article challenges the premises of the automation rationale. It contends that users whose information is exposed only to automated Internet systems incur no loss of privacy and only a minimal risk of eventual exposure of their personal information to humans.³² The Article then examines available data about the behavior and privacy expectations of

27. See *United States v. Jacobsen*, 466 U.S. 109, 117–22 (1984) (explicitly rejecting relational privacy arguments). The Doctrine has been used in numerous cases since *Smith*, and is often applied broadly. See, e.g., *United States v. Knotts*, 460 U.S. 276, 280–85 (1983); *United States v. Cormier*, 220 F.3d 1103, 1108 (9th Cir. 2000); *United States v. Daccarett*, 6 F.3d 37, 50 (2d Cir. 1993), *superseded by statute*, Civil Asset Forfeiture Reform Act of 2000, Pub. L. 106-185, 114 Stat. 202; see also Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 Harv. C.R.-C.L. L. Rev. 435, 460 (2008) (arguing that the Doctrine is unlikely to be reversed given the Court's reluctance in recent years to extend the protections of the Fourth Amendment).

28. "Internet Protocol addresses" are sequences of numbers assigned to each computer or other Internet-enabled device that is active on a network. They generally consist of four parts, separated by periods, such as 199.239.137.200, the IP address of the *New York Times* website.

29. See *United States v. Forrester*, 512 F.3d 500, 509 (9th Cir. 2008).

30. See, e.g., *United States v. Perrine*, 518 F.3d 1196 (10th Cir. 2008); *United States v. Hambrick*, No. 99-4793, 2000 WL 1062039 (4th Cir. Aug. 3, 2000); *Freedman v. Am. Online, Inc.*, 412 F. Supp. 2d 174 (D. Conn. 2005).

31. See *Rehberg v. Paulk*, 598 F.3d 1268, 1281 (11th Cir. 2010) ("A person [has no] reasonable expectation of privacy in emails, at least after the email is sent to and received by a third party."), *vacated*, 611 F.3d 828 (11th Cir. 2010); *In re United States*, 665 F. Supp. 2d 1210, 1222 (D. Or. 2009).

32. See *infra* Part IV.

Internet users that reveals that they do in fact sharply distinguish between disclosure to humans and disclosure to automated systems, even if courts thus far have not.

This Article contends that the extension of the automation rationale is inconsistent with both a sound conception of privacy and with well-established sources of Fourth Amendment doctrine. It identifies how the automation rationale arose from the unique context of telephone routing and argues that it can easily be limited to the facts of *Smith*. The Article demonstrates that, contrary to the assertions of most privacy scholars,³³ virtually all forms of Internet information may be protected by the Fourth Amendment. It develops a new, more accurate model of Internet user behavior and privacy expectations in online data and employs it to reform current approaches to Fourth Amendment law on the Internet.

Part II discusses the importance of Fourth Amendment protection for private online data and describes the development of the Third Party Doctrine and the automation rationale of *Smith*. Part III describes how nearly every form of data generated by Internet users is exposed to third parties' automated systems and is regularly scanned and stored for a variety of purposes. It examines how network administrators, websites, and third-party marketers use personal data, and evaluates the risk of actual disclosure of this data to human employees. Part IV analyzes common characteristics of various theories of privacy and privacy violations, and argues that Internet users do not suffer a cognizable privacy harm in the absence of some eventual disclosure to a human observer. It examines data on consumer behavior that indicates that Internet users share this conception of privacy. It also reports the results of a novel survey designed to measure users' attitudes towards disclosing their personal information to humans and automated systems. Part V uses this analysis to examine how courts' conflation of disclosure to automated systems with disclosure to human beings threatens online privacy. It proposes an alternative approach that incorporates a more accurate conception of consumer and online service provider behavior. It then addresses potential objections and doctrinal obstacles, and discusses the implications of its proposals for Internet privacy scholarship and the future direction of the law governing new technologies.

33. See *supra* note 26 (listing articles); see also DANIEL J. SOLOVE, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INTERNET AGE* 202 (2006); Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 *HASTINGS L.J.* 805, 812-16 (2003); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 *GEO. WASH. L. REV.* 1557, 1563 (2004).

II. THE FOURTH AMENDMENT AND THE AUTOMATION RATIONALE

A. *THE IMPORTANCE OF FOURTH AMENDMENT PROTECTION FOR ONLINE DATA*

Approximately eighty percent of Americans (248 million adults and children)³⁴ use the Internet, most of them on a daily basis.³⁵ These Internet users generate enormous quantities of data, much of it stored by their online service providers. E-mails, web-surfing histories, cloud computing documents, search terms, and credit-card information are all retained by online service providers, often for long periods of time.³⁶

These trillions of bytes of information can often be linked to the IP address and then the name and home address of the individual user. Such information can be used (and has been used) to create detailed personality profiles of users,³⁷ to predict consumer behavior and target advertisements to individual users,³⁸ and to gain insights into a user's life, both online and offline. And the information available can be profoundly revealing. E-mails and instant messages have become one of the primary means of interpersonal communication in today's society, and according to surveys of Internet users, they are central to many Americans' social relationships.³⁹ Users create detailed profiles on online dating websites, rent movies, express controversial or offensive opinions in blog posts and comments, search for driving directions to their friends' homes, volunteer for political campaigns or causes, and purchase virtually every kind of item available in the offline world. Over a third of Internet users have visited the websites of support groups or sites about specific medical conditions or other personal situations.⁴⁰ Roughly forty percent of users—over 100 million Americans—

34. CTR. FOR THE DIGITAL FUTURE, *supra* note 22, at 29; see *U.S. Population Clock*, U.S. CENSUS BUREAU, <http://www.census.gov/population/www/popclockus.html> (last visited Oct. 26, 2010).

35. *Online Activities, Daily*, PEW INTERNET & AM. LIFE PROJECT, <http://www.pewinternet.org/Trend-Data/Online-Activities-Daily.aspx> (last visited Oct. 26, 2010).

36. See *infra* Part III.A.

37. See Charles Duhigg, *What Does Your Credit Card Company Know About You?*, N.Y. TIMES, May 17, 2009, § 6 (Magazine), at 40; Erika S. Koster, *Zero Privacy: Personal Data on the Internet*, COMPUTER LAW., May 1999, at 7, 7, available at <http://www.oppenheimer.com/uploadedFiles/News/ZeroPrivacy%20Koster%20may%201999.pdf>.

38. *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 503–04 (S.D.N.Y. 2001); Duhigg, *supra* note 37; Ellen Nakashima, *Some Web Firms Say They Track Behavior Without Explicit Consent*, WASH. POST, Aug. 12, 2008, at D1; Farhad Manjoo, *For Sale: Your Browser History*, SLATE, Aug. 19, 2008, <http://www.slate.com/id/2198119>.

39. According to a 2009 poll, most Internet users said that the Internet was important or very important in maintaining social relationships; only 28% said it had no importance. CTR. FOR THE DIGITAL FUTURE, *supra* note 22, at 129.

40. Press Release, Pew Internet & Am. Life Project, Pew Research Ctr., 86% of Internet Users Want To Prohibit Online Companies from Disclosing Their Personal Information Without Permission (Aug. 21, 2000), <http://www.pewinternet.org/Press-Releases/2000/86-of-Internet-Users-Want-to-Prohibit-Online-Companies-From-Disclosing-Their-Personal-Inf.aspx>.

visit pornographic websites each month.⁴¹ Activist groups from the Iraq War protestors to the Tea Partiers have relied on the Internet to spread information and coordinate activities.⁴² Citizens in four states have even used the Internet to vote in state elections, as have soldiers stationed abroad.⁴³ In all, personal online data can reveal virtually everything about an Internet user, from her political affiliation to her geographic location, medical history, sexual preference, or taste in music.

1. The Government and Personal Online Data

The wealth of personal information on the Internet could, of course, be useful to the government. Although law-enforcement officials have not attempted to collect personal online data on suspects as a regular investigative practice, local, state, and federal officers have used such data as evidence in a large and ever-growing number of cases over the past ten years—and the evidence is very seldom suppressed on grounds of violating constitutional or statutory law.⁴⁴ And law enforcement's use of online data is actually far more extensive than the many reported cases reflect.⁴⁵ ISPs receive tens of thousands of requests each year for users' online data; some ISPs have entire departments of employees tasked with complying with these

41. See David Crary, *Battle Brews as Porn Moves into Mainstream*, BREITBART (Apr. 1, 2006, 4:11PM), http://www.breitbart.com/article.php?id=D8GNep902&show_article=1.

42. See, e.g., *UFPJ Nonviolent Direct Action Working Group Call to Action*, UNITED FOR PEACE & JUSTICE, <http://www.unitedforpeace.org/article.php?list=type&type=125> (last visited Oct. 26, 2010); TEA PARTY PATRIOTS, <http://www.teapartypatriots.org/> (last visited Oct. 27, 2010).

43. Rebekah K. Browder, Comment, *Internet Voting with Initiatives and Referendums: Stumbling Toward Direct Democracy*, 29 SEATTLE U. L. REV. 485, 496–97 (2005) (describing five examples of Internet voting, in Alaska, Arizona, Washington, and Michigan, and by military personnel living abroad).

44. See, e.g., *Rehberg v. Paulk*, 598 F.3d 1268, 1282 (11th Cir. 2010), *vacated*, 611 F.3d 828 (11th Cir. 2010); *United States v. Perrine*, 518 F.3d 1196, 1199 (10th Cir. 2008); *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008); *United States v. Meeks*, 290 F. App'x 896, 900 (6th Cir. 2008); *United States v. Fuller*, 77 F. App'x 371, 376 (6th Cir. 2003); *United States v. Simons*, 206 F.3d 392, 398–99 (4th Cir. 2000); *In re United States*, 665 F. Supp. 2d 1210, 1212 (D. Or. 2009); *In re United States*, 534 F. Supp. 2d 585, 586 (W.D. Pa. 2008), *vacated*, No. 08-4227, 2010 WL 3465170 (3d Cir. Sept. 7, 2010); *United States v. Ogden*, Cr. No. 06-20033-STA, 2008 WL 4982756, at *3 (W.D. Tenn. Nov. 18, 2008); *United States v. D'Andrea*, 497 F. Supp. 2d 117, 123 (D. Mass. 2007); *United States v. Sherr*, 400 F. Supp. 2d 843, 848 (D. Md. 2005); *United States v. Jones*, 364 F. Supp. 2d 1303, 1307 (D. Utah 2005); *United States v. Aldahondo*, No. CRIM 03-0107(DRD), 2004 WL 170252, at *2 (D.P.R. Jan. 15, 2004); *United States v. Cox*, 190 F. Supp. 2d 330, 332 (N.D.N.Y. 2002); *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1111 (D. Kan. 2000); *Hause v. Kentucky*, 83 S.W.3d 1, 12 (Ky. Ct. App. 2001); *Washington v. Townsend*, 57 P.3d 255, 265 (Wash. 2002); *infra* note 45.

45. Often the use of such online data in criminal trials is not challenged, either because the police do not introduce it as evidence but use it to obtain other evidence, or because the applicable statute contains no exclusionary rule, see *infra* Part II.A.2, and the Fourth Amendment is thought not to apply.

requests.⁴⁶ In addition, both the House and Senate Judiciary Committees are currently considering legislation that would require all Internet providers, and even operators of Wi-Fi access points, to keep every user's Internet records for two years in order to aid potential investigations.⁴⁷

The prospect of widespread collection of Internet data by the government has also raised concerns about the use of online surveillance for illegitimate purposes.⁴⁸ As discussed above,⁴⁹ government agencies have a long history of surveilling private citizens and political organizations. The COINTELPRO program of the mid-20th century was explicitly designed to "influence political choices and social values" in the service of combating an amorphous threat of domestic communist influence.⁵⁰ Such a program was easily abused—wiretaps were frequently ordered for strategic political purposes, and the information gleaned from these and other wiretaps was used to influence, intimidate, or discredit political opponents.⁵¹

Even if the chances of politically motivated Internet surveillance are currently slim, it would nonetheless be alarming if the government were able to access vast stores of private online data at will. And the possibility of politically motivated surveillance may not be as remote as it appears⁵² simply because Internet surveillance does not require an expensive, highly

46. Saul Hansell, *Online Trail Can Lead to Court*, N.Y. TIMES, Feb. 4, 2006, at C1 (noting that AOL receives nearly one thousand requests—usually subpoenas rather than warrants—per month for online data, and employs more than a dozen people to handle them); Nick Summers, *Walking the Cyberbeat*, NEWSWEEK, May 18, 2009, at E6, available at <http://www.newsweek.com/2009/04/30/walking-the-cyberbeat.html> (reporting that Facebook receives ten to twenty police requests per day); Christopher Soghoian, *8 Million Reasons for Real Surveillance Oversight*, SLIGHT PARANOIA (Dec. 1, 2009, 7:00 AM), <http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html> (stating that Verizon receives "tens of thousands" of requests for customers' online data each year).

47. See H.R. 1076, 111th Cong. (2009), available at <http://www.govtrack.us/congress/bill.xpd?bill=h111-1076>; S. 436, 111th Cong. (2009), available at <http://www.govtrack.us/congress/bill.xpd?bill=s111-436>; Declan McCullagh, *Bill Proposes ISPs, Wi-Fi Keep Logs for Police*, CNET (Feb. 19, 2009, 10:45 PM), http://news.cnet.com/8301-13578_3-10168114-38.html. Note that Europe has already passed legislation requiring ISPs to maintain Internet records for two years.

48. See SOLOVE, *supra* note 33, at 200–02; *supra* note 26.

49. See *supra* Part II.

50. SENATE SELECT COMM. ON GOVERNMENTAL OPERATIONS, BOOK III: SUPPLEMENTAL DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, at 4 (1976).

51. See *supra* notes 5–12 and accompanying text.

52. Note that the FBI's extensive wiretapping was not widely publicized until 1966, decades after the formal wiretapping program began in 1931. See CHARNS, *supra* note 3, at 19–20, 77. And, of course, a change of administration, another major terrorist attack on U.S. soil, or the rise of a competing global superpower could all increase the risk of pervasive monitoring of U.S. citizens' Internet communications and personal data. See Rubenfeld, *supra* note 26, at 160–61.

classified government program to be both pervasive and powerful.⁵³ In 2006, the Bush Administration attempted to influence the Department of Justice to investigate questionable claims of voter fraud in several battleground states and then fired and replaced several U.S. Attorneys who failed to pursue the claims.⁵⁴ Other Administration officials illegally politicized the hiring of federal prosecutors at the Department of Justice.⁵⁵ The depth and amount of information a U.S. Attorney, or other federal prosecutor with subpoena power could obtain about an individual's or group's online activities may be virtually unlimited in the absence of Fourth Amendment protection.⁵⁶ Even a single motivated official with access to such information could inflict significant political damage upon disfavored politicians or activists.⁵⁷ Recent legal controversies demonstrate that this possibility is far from remote. A state attorney general running for governor recently subpoenaed the account information of Twitter users and bloggers who criticized him.⁵⁸ And prosecutors have used subpoenas to obtain an individual's personal e-mails and then given the e-mails to politically connected private parties as a "favor."⁵⁹

2. The Weakness of Statutory Protection

Six years after the Supreme Court's declaration in *Olmstead v. United States* that the Fourth Amendment did not prohibit wiretapping or bugging private conversations, Congress passed the Communications Act of 1934. Section 605 of the Act provided that "no person not being authorized by the sender shall intercept any communication *and* divulge or publish the

53. The cost of monitoring e-mails, web surfing, and search terms would be dramatically lower than that of operating an equivalent number of wiretaps. *See, e.g.*, Patricia L. Bellia, *The Memory Gap in Surveillance Law*, 75 U. CHI. L. REV. 137, 153–66 (2008); Koster, *supra* note 37, at 7.

54. *See, e.g.*, Dan Eggen & Amy Goldstein, *Voter-Fraud Complaints by GOP Drove Dismissals*, WASH. POST, May 14, 2007, at A4.

55. *See, e.g.*, Carrie Johnson, *Internal Justice Report Cites Illegal Hiring Practices*, WASH. POST, July 29, 2008, at A1.

56. *See infra* Part II.A.2.

57. For instance, investigators might read through a politician's e-mails and search-term records or develop a detailed personality profile based on an activist's web-surfing history and online purchase records. They could also threaten to leak information about these individuals' private online activities in order to influence or intimidate them. To be sure, these are worst-case scenarios—yet equivalent tactics were employed with alarming frequency during the wiretapping era.

58. Zachary Roth, *Penn. AG Subpoenas Twitter: A Move To Silence Critics?*, TALKING POINTS MEMO (May 20, 2010, 9:09 AM), http://tpmmuckraker.talkingpointsmemo.com/2010/05/penn_ag_subpoenas_twitter_a_move_to_silence_critic.php?ref=fpblg.

59. *See* *Rehberg v. Paulk*, 611 F.3d 828, 835 (11th Cir. 2010). After Rehberg criticized the managers of a local hospital, district attorneys investigated plaintiff's actions as a favor to the managers, with whom they allegedly had political connections. Without impaneling a grand jury, the prosecutors issued subpoenas to Rehberg's ISP requesting his personal e-mails, which they turned over to private investigators hired by the hospital.

existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person.”⁶⁰ The language appeared to prohibit all government wiretapping or eavesdropping, but the key sentence contained one small ambiguity: the use of the word “and.” The FBI, by then engaged in fairly extensive wiretapping operations, argued that the statute did not prohibit wiretapping so long as the government did not divulge the wiretaps in court.⁶¹ Although this conflicted with the rationales of several previous Supreme Court cases,⁶² it was not explicitly barred by the cases’ narrow holdings. Further, the Attorney General’s office assured the FBI that it would not prosecute its officers for violating § 605.⁶³ The Communications Act of 1934 thus did little to prevent the government from wiretapping and bugging citizens on an unprecedented scale. Rather, the dramatic expansion of the government’s wiretapping programs mostly occurred during the three decades *after* the passage of strongly worded antiwiretapping legislation.

The Electronic Communications Privacy Act (“ECPA”), which regulates access to oral, telephone, and electronic communications, arguably has more teeth than the Communications Act of 1934, which failed to prevent the government from wiretapping citizens on a massive scale.⁶⁴ Unlike the 1934 Act, it provides a private right of action for most violations,⁶⁵ and, most importantly, has no obvious loophole allowing political surveillance. However, the ECPA’s overall scheme of protection is weak and riddled with gaps and exceptions.

For instance, the portions of the ECPA that govern stored electronic data do not apply to e-mail or Internet services that are not open to the public, such as university or workplace Internet services.⁶⁶ Thus, the government can obtain e-mails sent to or from a user’s university or

60. Communications Act of 1934, ch. 652, § 605, 48 Stat. 1064, 1104 (codified as amended at 47 U.S.C. § 605 (2006)) (emphasis added).

61. KESSLER, *supra* note 7, at 60. Actually, the FBI first tried to continue introducing the fruits of wiretaps in criminal trials but was twice rebuffed by the Supreme Court. *See Weiss v. United States*, 308 U.S. 321 (1939); *Nardone v. United States (Nardone I)*, 302 U.S. 379 (1937).

62. *See Weiss*, 308 U.S. 321; *Nardone I*, 302 U.S. 379; *Nardone v. United States (Nardone II)*, 308 U.S. 338 (1939).

63. CHARNS, *supra* note 3, at 23.

64. *See supra* text accompanying note 4.

65. 18 U.S.C. §§ 2520(a), 2707(a) (2006).

66. COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP’T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 125–26, 128 (3d ed. 2009), available at <http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf>; Patricia L. Bellia, *Surveillance Law Through Cyberlaw’s Lens*, 72 GEO. WASH. L. REV. 1375, 1424 (2004).

workplace account, or web-surfing histories logged by university or workplace accounts, without any statutory limitations.⁶⁷

The ECPA also provides little protection to electronic information classified as “noncontent”—that is, information that does not “concern[] the substance, purport, or meaning of [a] communication.”⁶⁸ The government can intercept noncontent information (such as e-mail to/from addresses) in real time so long as they certify to the court that the noncontent information is relevant to an ongoing criminal investigation.⁶⁹ Courts do not actually inquire into whether the certification is legitimate;⁷⁰ there is, at present, essentially no judicial scrutiny for such surveillance. Noncontent subscriber information, including name, home address, billing information, and the user’s IP address, can be obtained with a grand jury or administrative subpoena. Subpoenas can be validly issued for almost any purpose,⁷¹ and in practice, a federal prosecutor who has convened a grand jury can subpoena documents at will, even without prior grand jury authorization.⁷² Practically speaking, prosecutors can issue quasi-official subpoenas even without impaneling a grand jury.⁷³

67. Students often use their university Internet accounts in the same manner as they would a private account with an ISP. Despite the lack of statutory protection, it is likely that most universities would require investigators to obtain a subpoena before turning over student Internet records, rather than turning them over voluntarily upon an informal request. However, such subpoenas are easily obtained. *See infra* note 72. Workplace Internet accounts are often subject to extensive monitoring by employers, *see, e.g.*, *United States v. Simons*, 206 F.3d 392, 395–96 (4th Cir. 2000), but a privacy analysis of workplace accounts is beyond the scope of this Article.

68. *See* 18 U.S.C. § 2510(8).

69. 18 U.S.C. § 3123(a)(1)–(2). For stored noncontent information, § 2703(d) of title 18 mandates a court order that requires the government entity to provide “specific and articulable facts” that provide reasonable grounds to believe that the records are “relevant and material to an ongoing criminal investigation,” establishing a standard well below either probable cause or reasonable suspicion. 18 U.S.C. § 2703(d).

70. *See* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 62 (2004).

71. COMPUTER CRIME & INTELLECTUAL PROP. SECTION, *supra* note 66, at 128 (citing *United States v. Morton Salt Co.*, 338 U.S. 632, 642–43 (1950)).

72. FED. R. CRIM. P. 17; *see* *Doe v. DiGenova*, 779 F.2d 74, 80 & n.11 (D.C. Cir. 1985); *United States v. Santucci*, 674 F.2d 624, 627 (7th Cir. 1982) (stating that U.S. Attorneys may “fill in blank grand jury subpoenas . . . without actual prior grand jury authorization”); *United States v. Kleen Laundry & Cleaners, Inc.*, 381 F. Supp. 519, 523 (E.D.N.Y. 1974) (same). Further, the existence of a grand jury is itself highly confidential. Rule 6(e) of the Federal Rules of Criminal Procedure prohibits the jurors and other persons attending the grand jury from disclosing anything about grand jury proceedings, unless ordered to do so in another judicial proceeding.

73. *See* *Rehberg v. Paulk*, 611 F.3d 828, 835–37 (11th Cir. 2010) (discussing district attorney who issued subpoenas without convening a grand jury to obtain the e-mail records of a man who criticized a hospital with which the district attorney and other officials had political connections).

The ECPA's protection of communications "content," while stronger, is undermined by several loopholes. The ECPA offers dramatically different protection for content data (such as e-mails) in short-term and long-term storage on the Internet. For e-mails in "electronic storage" for 180 days or less, the government must obtain a standard search warrant before it can access them.⁷⁴ However, the government can access e-mails stored for over 180 days with only an administrative or grand jury subpoena.⁷⁵ And even the 180-day requirement can be circumvented. The Department of Justice has interpreted the term "electronic storage" in the ECPA to apply only to e-mails stored in the process of transmission, meaning that all opened e-mails that remain on Google or Yahoo!'s servers can be accessed with a subpoena as soon as they are opened, rather than 181 days after they are sent.⁷⁶ The legislative history of the ECPA suggests that this interpretation is correct; Congress apparently did not contemplate the storage of e-mails online after they were opened.⁷⁷ In 1986, when the ECPA was passed, small businesses sometimes used third-party remote data-processing services to assist them in managing computerized data.⁷⁸ Perhaps due to the nonsensitive nature of this kind of data, Congress provided it with only minimal statutory protection.⁷⁹ Today, millions of Internet users use remote computing services such as Google Docs to create documents and spreadsheets, store personal photos, videos or other files, or to back up their entire hard drives

74. 18 U.S.C. § 2703.

75. *Id.* § 2703(a), (b)(1)(B)(i). While the statute also requires notice of the subpoena to the subscriber, it provides that the investigatory agent in charge may continually delay notice for numerous purposes including "seriously jeopardizing an investigation or unduly delaying a trial." *Id.* § 2705(a)(2). There is no judicial review of the agent's decision. *Id.* § 2705(a)(1)(B). See C. L. "Butch" Otter & Elizabeth Barker Brandt, Essay, *Preserving the Foundation of Liberty*, 19 NOTRE DAME J.L. ETHICS & PUB. POL'Y 261, 267 n.25 (2005) (arguing that § 2705's notice provisions are not an effective limit on the power to search surreptitiously).

76. COMPUTER CRIME & INTELLECTUAL PROP. SECTION, *supra* note 66, at 124-25; see Bellia, *supra* note 66, at 1418-19.

77. H.R. REP. NO. 99-647, at 63 (1986); see Bellia, *supra* note 66, at 1419. Courts are split on the question, but the government's argument is likely plausible enough to allow it to immediately obtain opened e-mails in the large majority of jurisdictions that have not decided the issue without fear of sanction. Compare *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004) (holding that opened e-mails remained in "electronic storage" under the ECPA), and *Bailey v. Bailey*, No. 07-11672, 2008 WL 324156, at *6 (E.D. Mich. Feb. 6, 2008) (same), with *United States v. Weaver*, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009) (holding that opened e-mails are not in electronic storage), *Bansal v. Russ*, 513 F. Supp. 2d 264, 276 (E.D. Pa. 2007) (same), and *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001) (same), *vacated in part, aff'd in part*, 352 F.3d 107 (3d Cir. 2004).

78. See S. REP. NO. 99-541, at 10-11 (1986), as reprinted in 1986 U.S.C.A.N. 3555, 3564-65; H.R. REP. NO. 99-647, at 23 (1986); Bellia, *supra* note 66, at 1425-26.

79. See 18 U.S.C. § 2703(b). The statute also requires notice of the subpoena. See *supra* note 75.

on remote servers.⁸⁰ Under the ECPA, all of these files, documents, and photos can be obtained with a simple subpoena, regardless of whether they are considered “content” and regardless of how personal or intimate they might be.⁸¹

Finally, unlike the 1934 Communications Act, the ECPA has no exclusionary rule for electronic evidence obtained in violation of its provisions.⁸² If they are not deterred by the Act’s thus far minimally enforced criminal penalties⁸³ or the threat of civil liability,⁸⁴ law-enforcement officials could simply intercept or subpoena any kind of personal online data and use it in criminal trials. The lack of an exclusionary rule also makes it less likely that the many loopholes and ambiguities in the ECPA will ever be resolved, as the statute is hardly ever litigated in criminal cases.⁸⁵

Of course, Congress could step in to fix some or all of the deficiencies of the ECPA. Arguably, protecting personal Internet data via legislation has advantages over a judicially mandated Fourth Amendment solution. The potential error costs of legislation may be lower than those of constitutional decision making. Flawed statutes are relatively easy to amend, while erroneous Fourth Amendment decisions could require a constitutional

80. John B. Horrigan, *Cloud Computing Gains in Currency*, PEW RESEARCH CENTER (Sept. 12, 2008), <http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency>. Users of the Google Desktop program may even back up their hard drives on third-party servers unintentionally. See James X. Dempsey, *Digital Search & Seizure: Standards for Government Access to Communications and Associated Data*, in 2 TENTH ANNUAL INSTITUTE ON PRIVACY AND DATA SECURITY 2009, at 687, 707 (PLI Patents, Trademarks & Literary Prop., Course Handbook Series No. 19129, 2009).

81. See 18 U.S.C. § 2703(b).

82. Freiwald, *supra* note 26, ¶ 13; Kerr, *supra* note 33, at 806.

83. There are no reported cases of prosecution of law-enforcement officials for illegal acquisition of electronic communications data under the ECPA, and the Department of Justice may be reluctant to prosecute such officials. The Department of Justice also favors a very expansive interpretation of law enforcement officials’ ability to legally obtain electronic evidence. See COMPUTER CRIME & INTELLECTUAL PROP. SECTION, *supra* note 66, at 122–23, 145. Of course, the signaling function of the criminal penalties may be enough to deter flagrant violations, as law-enforcement officials are likely to be reluctant to engage in activities that are clearly crimes under the Act.

84. There have also been very few (and mostly unsuccessful) civil suits against government officials for ECPA violations involving electronic communications, suggesting that the prospect of being sued will have at best a small deterrent effect. See *Davis v. Gracey*, 111 F.3d 1472, 1484 (10th Cir. 1997) (holding that police officers’ good faith defense precluded liability for the seizure of e-mails on electronic bulletin board); *Bansal v. Russ*, 513 F. Supp. 2d 264, 276 (E.D. Pa. 2007) (holding that acquisition of plaintiff’s opened e-mails did not violate the ECPA); *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 816 F. Supp. 432, 443 (W.D. Tex. 1993) (finding liability for seizure of e-mails and other computer files). The provisions of the ECPA dealing with pen-register information do not provide for a right of civil action. See 18 U.S.C. §§ 3121–3127.

85. Freiwald, *supra* note 26, ¶ 34; Kerr, *supra* note 33, at 823–24.

amendment to overturn.⁸⁶ However, the Court has already decided that courts play an important role in determining reasonable expectations of privacy in new technologies, and this Article, like others addressing the Third Party Doctrine, takes that role largely as a given. The resilience of Fourth Amendment law might also be beneficial in that its privacy protections are less vulnerable to repeal in the wake of political shocks (such as terrorist attacks). Further, much of this Article's analysis could be applied to a proposed statute aimed at effectively protecting personal online data, and I offer suggestions for such legislation in Part V.

In any event, congressional action to amend the ECPA or provide new protections for personal online data appears unlikely for the foreseeable future.⁸⁷ It may be that Congress, as it has in the past, will wait for the Supreme Court to clearly define the scope of Fourth Amendment protection for new technologies before taking any legislative action.⁸⁸

As it stands, the ECPA alone is very unlikely to prevent the government from engaging in widespread surveillance if it is motivated to do so. Fourth Amendment protection (or much stronger legislation) will very likely be necessary to ensure effective privacy protection for personal data on the Internet.⁸⁹

B. THE THIRD PARTY DOCTRINE AND THE AUTOMATION RATIONALE

Prior to 1967, the law of the land was that the Fourth Amendment did not apply to intangible things, such as oral or telephone communications. As the Court held in *Olmstead*⁹⁰ in 1928, the Fourth Amendment applied

86. The Court itself might eventually recognize the error of its ways, but the force of stare decisis often causes questionable decisions to persist for decades. See Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 871 (2004).

87. Proposals to regulate certain kinds of data gathering used for targeted online advertising have come and gone since 2002, and recent proposals have not yet reached the committee level. David Kaplan, *Congress Takes Another Step on Behavioral Targeting Legislation*, CBS NEWS, Apr. 29, 2009, <http://www.cbsnews.com/stories/2009/04/24/paidcontent/main4966873.shtml>; Kate Kaye, *Web Privacy Bill Could Come by November*, CLICKZ (Oct. 1, 2009), <http://www.clickz.com/3635153>. Even if passed, the proposed legislation would likely only apply to uniform resource locaters ("URLs") and may not substantially decrease the number of URLs gathered. See Kaye, *supra* (noting that the legislation would likely mandate an opt-out regime for targeted advertising which many ISPs already have in place). Meanwhile, there appears to be no congressional interest in broader proposals to update the ECPA and increase the levels of protection received by content or noncontent information.

88. See Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 776 (2005).

89. Recall that the FBI's program of warrantless wiretapping did not fade until after the Supreme Court stripped away any doubt about its legality by declaring that it violated the Fourth Amendment in the late 1960s. See *Katz v. United States*, 389 U.S. 347, 353 (1967); CHARNS, *supra* note 3, at 91.

90. 277 U.S. 438, 466 (1928), *overruled by Katz*, 389 U.S. 347, and *Berger v. New York*, 388 U.S. 41 (1967).

only to people or property—the “persons, houses, papers, and effects” named in the text of the Amendment.⁹¹ Telephone wires extending beyond a citizen’s property were no more protected from government monitoring than the “highways along which they are stretched.”⁹² Conversations traveling along these wires were treated as exposed to the world.

A corollary of the *Olmstead* holding was that undercover agents or government informants could record face-to-face conversations for use in criminal trials, so long as they committed no trespass in obtaining the recordings. The Court affirmed this principle in a series of cases beginning in 1952.⁹³ Because the agents and informants could have personally appeared in court and testified about what they had heard,⁹⁴ there was no basis for excluding a recording that merely provided similar, extremely reliable evidence of the defendant’s statements.⁹⁵ These undercover-agent cases marked the beginnings of what became known as the Third Party Doctrine, which essentially provides that the Fourth Amendment does not protect any information willingly disclosed to a third party and obtained by the government from that party.⁹⁶

Then, in the 1967 case *Katz v. United States*,⁹⁷ the Court dramatically altered its conception of the scope of the Fourth Amendment. The Fourth Amendment’s scope would no longer depend on property interests and the law of trespass, but instead on citizens’ expectations of privacy.⁹⁸ *Katz* has been interpreted as establishing a two-part test: the Fourth Amendment applies whenever an individual has (1) an actual, subjective expectation of privacy, and (2) the expectation is one that society recognizes as objectively reasonable.⁹⁹ Thus, it can protect intangible as well as tangible things, including, as in *Katz*, an individual’s telephone conversations conducted from a public phone booth.¹⁰⁰

91. U.S. CONST. amend. IV.

92. *Olmstead*, 277 U.S. at 465.

93. *Hoffa v. United States*, 385 U.S. 293, 303 (1966); *Lewis v. United States*, 385 U.S. 206, 210 (1966); *Lopez v. United States*, 373 U.S. 427, 438–39 (1963); *On Lee v. United States*, 343 U.S. 747, 751–55 (1952).

94. The Court held that the use of deceit to gain access to the defendant’s property or to win the defendant’s trust did not constitute a trespass and therefore did not violate the Fourth Amendment. *Hoffa*, 385 U.S. at 302; *Lewis*, 385 U.S. at 210; *Lopez*, 373 U.S. at 438; *On Lee*, 343 U.S. at 752.

95. *Lopez*, 373 U.S. at 439; *On Lee*, 343 U.S. at 755.

96. See *United States v. Miller*, 425 U.S. 435, 443 (1976).

97. 389 U.S. 347 (1967).

98. *Id.* at 351–52.

99. *Id.* at 361 (Harlan, J., concurring).

100. *Id.* at 353 (majority opinion).

1. The Third Party Doctrine after *Katz*

It was briefly unclear, following *Katz*, whether undercover government agents or confidential informants could still record suspects' conversations and introduce them into evidence without violating the Fourth Amendment. The question was resolved in the 1971 case *United States v. White*,¹⁰¹ which made clear that the Third Party Doctrine had survived *Katz* wholly intact. The Court held that citizens inevitably assume the risk that persons with whom they converse may later reveal the conversation to the police, and therefore they essentially waive any Fourth Amendment expectation of privacy in the things they tell another person.¹⁰² As for the introduction of tape recordings into evidence, *White* again leaned heavily on the idea that there was no constitutional difference between a police officer testifying as to his conversations with a defendant and recording those conversations for introduction into evidence.¹⁰³

After *White*, the Third Party Doctrine clearly precluded Fourth Amendment protection for speech recorded in person by a government agent. Still, this principle had a relatively narrow application, and it was grounded in decades of familiar investigatory practices. The transformation of the Third Party Doctrine into a potential means of pervasive government surveillance of private affairs began in 1976, with *United States v. Miller*.¹⁰⁴ The Court in *Miller* ruled that the Third Party Doctrine applied to all personal documents and records that a citizen discloses to any other private party.¹⁰⁵ The case arose when the government issued subpoenas to banks used by Miller, requesting all records associated with his accounts, in the course of investigating him for running an illegal whiskey distillery.¹⁰⁶ The Court held that Miller had no reasonable expectation of privacy in records "conveyed to the banks and exposed to their employees in the ordinary course of business."¹⁰⁷ The majority concluded that this was little different from a person conveying information in a conversation with a third party.¹⁰⁸

101. 401 U.S. 745 (1971).

102. *Id.* at 752.

103. *Id.* at 751-53.

104. 425 U.S. 435 (1976). While *Couch v. United States*, 409 U.S. 322 (1973), had previously held that a person had no reasonable expectation of privacy in tax documents given to his accountant, that case primarily depended upon the fact that the defendant knew that his accountant was required to disclose much of the information to the IRS anyway, and that disclosure to the government was largely at the accountant's discretion. *Id.* at 335. Thus *Miller* was the first case to expand the reach of the Third Party Doctrine to personal records in general.

105. *See* 425 U.S. at 441-43.

106. *Id.* at 437.

107. *Id.* at 442.

108. *Id.* at 443.

Privacy scholars have objected to this rationale (as did Justice Brennan in his *Miller* dissent¹⁰⁹), arguing that a bank customer has a reasonable expectation that his bank will not disclose his personal records without authorization, and that the banks only did so in *Miller* when compelled by legal process.¹¹⁰ However, the force of this objection may be blunted by the fact that the Fourth Amendment does not prevent the compulsion of witnesses to testify.¹¹¹ Because the police could have subpoenaed the bank employees who dealt with Miller's accounts, it arguably requires only a small additional step to conclude that they can subpoena Miller's records, which provide similar (and more reliable) evidence of his transactions with the banks.

The Court applied *Miller* to records of electronic data in 1979's *Maryland v. Smith*.¹¹² Police officers asked the phone company to set up a "pen register"—a device that records all outgoing phone numbers dialed—on a suspect's telephone without first obtaining a warrant.¹¹³

The Court upheld the warrantless use of the pen register device, holding that the Fourth Amendment does not protect the numbers dialed by a telephone user.¹¹⁴ Applying *Katz's* two-part test, the Court concluded that a telephone user could have no subjective expectation of privacy in his phone numbers because users are surely aware that the phone company records the numbers of their long-distance phone calls.¹¹⁵ The numbers appear on customers' monthly bills,¹¹⁶ and the phone company also offers to identify persons making "annoying or obscene calls," or to "check for overbilling," making it clear that they can and do monitor dialed phone numbers.¹¹⁷ Further, even if Smith had a subjective expectation of privacy in the phone numbers, it was not an objectively reasonable one. Smith conveyed the numbers he dialed to a third party in the ordinary course of business, thus waiving any privacy interest in the numbers and assuming the risk that the third party would disclose them to the government.¹¹⁸ While the Court recognized that telephone-call routing was largely automated by the 1970s, it dismissed this point by hearkening back to the initial decades after the telephone's invention:

109. *Id.* at 449 (Brennan, J., dissenting)

110. See Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 829 (2005); Freiwald, *supra* note 26, ¶¶ 21–22.

111. *United States v. Dionisio*, 410 U.S. 1, 10 (1973); see Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 590 (2009).

112. 442 U.S. 735, 744 (1979).

113. *Id.* at 737.

114. *Id.* at 745–46.

115. *Id.* at 742.

116. *Id.*

117. *Id.* at 742–43.

118. *Id.* at 744.

The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.¹¹⁹

Though only briefly addressed, this point was crucial to *Smith's* holding. Rather than evaluating whether a human employee had actually observed *Smith's* dialed numbers, the Court simply decided the case as though the human operators still existed. As a result, the opinion strongly implies that citizens can have no reasonable expectation of privacy in any information that they expose to a third party's automated "equipment" in the ordinary course of business.¹²⁰

2. The Automation Rationale

This crucial but little noticed rationale of *Smith*, hereinafter referred to as the "automation rationale," stands for the proposition that there is no legally relevant difference between disclosure of one's personal information to a third party's automated systems and disclosure to a human being. Applied to the Internet, it has the potential to eliminate any possibility of Fourth Amendment protection for personal data and communications online. This is discussed in depth in Part III, but it is already visible in lower court cases dealing with police surveillance of the Internet. In *United States v. Forrester*,¹²¹ the Ninth Circuit applied *Smith's* automation rationale in holding that Internet users had no reasonable expectation of privacy in their e-mail to/from records or in the IP addresses¹²² of the websites they visit.¹²³ The court reasoned that e-mail and IP addresses, like telephone numbers, are voluntarily conveyed to "third party equipment," and therefore Internet

119. *Id.* at 744-45 (citation omitted).

120. *Id.* at 744 ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.")

121. 512 F.3d 500 (9th Cir. 2008).

122. "IP addresses" are sequences of numbers assigned to each computer's or other device's network interface(s) that are active on a network. *See, e.g., id.* at 510 n.5. They generally consist of four parts separated by periods, such as 199.239.137.200, the IP address of the *New York Times* website. *Id.*

123. *Id.* at 510. The court also held that the Fourth Amendment did not protect the total amount of data transmitted to and from the user's account, which likely includes data on files downloaded from each website visited. *Id.*; *see* Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2150 (2009).

users cannot have a reasonable expectation of privacy in such information.¹²⁴

Other courts have implicitly relied on the automation rationale in denying Fourth Amendment protection to personal online data.¹²⁵ For instance, in *United States v. Perrine*,¹²⁶ the Tenth Circuit failed to distinguish between disclosure of a user's information to an ISP's equipment and disclosure to its human employees. The court held that subscriber information associated with a user's IP address was not protected by the Fourth Amendment without determining whether any human employee actually observed it.¹²⁷ And in two recent cases, courts have relied heavily on the fact that e-mails are transmitted "to computers owned by a third party" and "physically stored on servers owned by an ISP" in determining that the Fourth Amendment does not apply even to the contents of e-mails.¹²⁸

The future of the automation rationale will become clearer as more courts are confronted with police requests for Internet data. Thus far, several courts have relied on the rationale either explicitly or implicitly to conclude that the Fourth Amendment does not apply to personal online information. No court has directly questioned the rationale's applicability to Internet data or communications.¹²⁹ The automation rationale of *Smith* appears to be destined to shape the future course of the law of Internet surveillance.

III. AUTOMATION ON THE INTERNET

So long as courts continue to apply *Smith v. Maryland's* automation rationale, any information disclosed to a third party's equipment is likely to be unprotected by the Fourth Amendment. This Part examines the extent to which personal information is exposed to third parties' automated equipment on the Internet. It then evaluates the probability that any such

124. *Forrester*, 512 F.3d at 510, 511.

125. See *United States v. Hambrick*, No. 99-4793, 2000 WL 1062039, at *3-4 (4th Cir. Aug. 3, 2000); *Freedman v. Am. Online, Inc.*, 412 F. Supp. 2d 174, 183 (D. Conn. 2005); *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000).

126. 518 F.3d 1196 (10th Cir. 2008).

127. *Id.* at 1205-06.

128. *In re United States*, 655 F. Supp. 2d 1210, 1213 (D. Or. 2009); see *Rehberg v. Paulk*, 598 F.3d 1268, 1282 (11th Cir. 2010) (holding that there is no Fourth Amendment protection for e-mail content, because e-mails are retained by third-party ISPs), *vacated*, 611 F.3d 828 (11th Cir. 2010).

129. A Sixth Circuit panel has ignored the automation rationale and declared that a defendant's e-mail content is protected by the Fourth Amendment on the basis that employees of the defendant's ISP did not access his e-mails in the ordinary course of business. *Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007). However, this decision was vacated on ripeness grounds by the en banc court, which expressed skepticism about the panel's analysis of the defendant's reasonable expectation of privacy in his e-mails. *Warshak v. United States*, 532 F.3d 521 (6th Cir. 2008) (en banc).

information will be exposed to a human being at any point during its automated storage and processing and concludes that the chances of human exposure are minimal. For all intents and purposes, personal information disclosed to automated Internet systems is limited to those systems and is not observed by another human being.

A. *INTERNET INFORMATION AND EXPOSURE TO AUTOMATED SYSTEMS*

Virtually every kind of personal online data is stored and processed by third-party automated equipment in order to route communications, detect spam and viruses, block computer hackers, or generate advertising revenue. E-mails and instant messages sent and received through a web-based e-mail service (services like Gmail, Yahoo!, Hotmail, and America Online, which account for over 200 million e-mail accounts in the United States¹³⁰), or through any service that stores e-mails on a remote server,¹³¹ are retained by the service provider until the user deletes them, and often even after deletion.¹³² Providers also store e-mail logs, recording e-mail to/from information, and the time each e-mail is sent and received.¹³³ The e-mails themselves are routed by equipment that processes their address information, and are scanned by the sending and receiving e-mail services for spam and viruses.¹³⁴ These services' spam filters generally "read" every e-mail and intercept those that contain text commonly associated with spam e-

130. Erick Schonfeld, *Gmail Nudges Past AOL Email in the U.S. To Take No. 3 Spot*, TECHCRUNCH (Aug. 14, 2009), <http://www.techcrunch.com/2009/08/14/gmail-nudges-past-aol-email-in-the-us-to-take-no-3-spot>.

131. The latter are referred to as Internet message access protocol ("IMAP") based e-mail services.

132. See, e.g., James X. Dempsey, *Digital Search & Seizure: Updating Privacy Protections To Keep Pace with Technology*, in SEVENTH ANNUAL INSTITUTE ON PRIVACY LAW: EVOLVING LAWS AND PRACTICES IN A SECURITY-DRIVEN WORLD, at 505, 523 (PLI Patents, Copyrights, Trademarks & Literary Prop., Course Handbook Series No. 8966, 2006) ("[S]ince ISPs retain data for varying lengths of time, and do not always delete email immediately upon request, customers may not be aware of whether their email is still stored and thus susceptible to disclosure."); Deirdre K. Mulligan et al., *Risks of Online Storage*, COMM. ACM, Aug. 2006, at 112, 112 ("Often, 'deleted' email will remain on backup storage unbeknownst to users."). Even e-mails sent through older services which transmit e-mails to and from a central server to the users' personal computers, referred to as post office protocol ("POP") based e-mail services, are copied in transit and generally stored on the server for at least a week. Achal Oza, Note, *Amend the ECPA: Fourth Amendment Protection Erodes as E-Mails Get Dusty*, 88 B.U. L. REV. 1043, 1052-53 & n.65 (2008); see PRESTON GRALLA, HOW THE INTERNET WORKS 87 (2001) (describing how e-mails are transmitted).

133. See, e.g., *Email Crimes*, FORENSIC SCI., http://library.thinkquest.org/04oct/00206/cos_email.htm (last visited Oct. 27, 2010).

134. *Warshak*, 490 F.3d at 474; Kerr, *supra* note 33, at 812-16; *More on Gmail and Privacy*, GMAIL, http://mail.google.com/mail/help/about_privacy.html (last updated Oct. 2010) ("Google scans the text of Gmail messages in order to filter spam and detect viruses, just as all major webmail services do.").

mails.¹³⁵ Virus scanners work much the same way, scanning through e-mails and attached files and matching them with recognized viruses.¹³⁶ Gmail, a rapidly growing web-based e-mail service already used by 37 million Americans, automatically scans its users' e-mails and places ads based on the content in the top margin of the e-mail message.¹³⁷ Yahoo! Mail, with 106 million users, scans e-mails for indexing and search purposes.¹³⁸ While the amount of text processed by e-mail services may vary,¹³⁹ e-mail messages are routinely stored and scanned by automated equipment for routing, spam and virus filtering, and advertising purposes.

ISPs also automatically collect and process enormous amounts of data about users' web-surfing habits. ISPs maintain logs of the IP addresses of each website a user visits as well as the volume of data transmitted to and from the user.¹⁴⁰ Some service providers even monitor and retain the address of each individual page a user visits.¹⁴¹ Many affiliated groups of websites collect the URLs¹⁴² of each page a user sees within their group.¹⁴³ These service providers and website networks then automatically use this information to target advertisements to the individual user, or sell the information to third-party advertisers for the same purpose.¹⁴⁴

Many other kinds of personal online data are exposed to the automated equipment of online service providers. Search terms input by a user into a search engine are inevitably processed by third-party equipment. Google,

135. See, e.g., David Mertz, *Spam Filtering Techniques: Six Approaches To Eliminating Unwanted E-Mail*, IBM (Sept. 1, 2002), <http://www.ibm.com/developerworks/linux/library/l-spamf.html>; Heinz Tschabitscher, *What You Need To Know About Bayesian Spam Filtering*, ABOUT.COM, http://email.about.com/cs/bayesianfilters/a/bayesian_filter.htm (last visited Oct. 27, 2010).

136. Geoff Kuenning, *How Does a Computer Virus Scan Work?*, SCI. AM., (Jan. 14, 2002), available at <http://www.scientificamerican.com/article.cfm?id=how-does-a-computer-virus>.

137. See Schonfeld, *supra* note 130; *More on Gmail and Privacy*, *supra* note 134.

138. Schonfeld, *supra* note 130; *Yahoo! Privacy Policy*, YAHOO.COM, <http://info.yahoo.com/privacy/us/yahoo/mail/details.html> (last visited Oct. 27, 2010).

139. The level of scanning may vary depending on the e-mail service's virus protection and spam settings. See, e.g., Tokson, *supra* note 123, at 2160 n.264; Mertz, *supra* note 135.

140. See, e.g., Terrence Berg, *Practical Issues in Searching and Seizing Computers*, 7 T.M. COOLEY J. PRAC. & CLINICAL L. 27, 37 (2004); Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 754-55 (2008).

141. See, e.g., Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1424-25, 1432-38; Nakashima, *supra* note 38.

142. A URL is the textual address of a specific website or file on the Internet, such as http://www.nytimes.com/2007/06/13/opinion/13wed3.html?_r=1, the address of a specific article on the *New York Times* website.

143. See, e.g., Omer Tene, *What Google Knows: Privacy and Search Engines*, 2008 UTAH L. REV. 1433, 1447-48; Nakashima, *supra* note 38; see also *In re Pharamtrak, Inc.*, 329 F.3d 9, 13-14 (1st Cir. 2003) (discussing how Pharamtrak provided pharmaceutical companies with software that allowed them to gather information about visitors to their websites).

144. See *In re DoubleClick Privacy Litig.*, 154 F. Supp. 2d 497, 503-04 (S.D.N.Y. 2001); Nakashima, *supra* note 38; Manjoo, *supra* note 38.

Yahoo!, and other search-engine companies retain search-term logs for years,¹⁴⁵ and while the data is usually anonymized after nine to eighteen months, such anonymization may be ineffective in some cases.¹⁴⁶ “Cloud computing” applications—that is, data processing or other computer programs available over the Internet that are run from a service provider’s remote servers—have grown in popularity in recent years.¹⁴⁷ By design, data generated by these programs is stored on third-party computers at all times. Cloud computing services do not scan or process stored documents themselves for advertising purposes; however, they may scan and index the documents so that users can search within their stored documents.¹⁴⁸ Also, most cloud documents are created on a third party’s equipment, and this alone may be enough to render them “exposed” to the automated systems of a third party, even if no other processing of the data occurs. Finally, service providers or websites that collect information from subscribers, such as name, home address, and credit card number, generally retain and process that information for registration or billing purposes. If exposure to third-party equipment is sufficient to deprive information of any Fourth Amendment protection, then, as many privacy scholars have suggested,¹⁴⁹ the Fourth Amendment will not apply to vast quantities of personal data and communications on the Internet.

B. *INTERNET INFORMATION AND EXPOSURE TO HUMAN BEINGS*

Online service providers store and process an incredible amount of personal Internet data. Yet in part because it is so voluminous, this mass of data is in many cases functionally anonymous, and the chance of it being directly observed by another human being (in the absence of direct government involvement) is extremely low. Accounts of Internet privacy that ignore this important characteristic of Internet use are likely to be flawed or, at best, incomplete.

E-mails, though scanned extensively by spam and virus filters and, in some cases, advertising software, are not read by online-service-provider employees in the ordinary course of business or even, it appears, outside of it. Many ISP privacy policies, which often permit ISPs to collect all kinds of

145. Thomas Claburn, *What Google Search Reveals About Us*, INFO. WEEK, Mar. 13, 2006, at 45; Brad Stone, *Microsoft Offers Privacy Options for Its Search Engine*, BITS N.Y. TIMES TECH. BLOG (July 23, 2007), <http://www.nytimes.com/2007/07/23/technology/23microsoftweb.html?ex=1342843200&en=bb60a818caf8add8&ei=5088&partner=rssnyt&emc=rss>.

146. John Palfrey, *The Public and the Private at the United States Border with Cyberspace*, 78 MISS. L.J. 241, 267 (2008); Tene, *supra* note 143, at 1445–49.

147. See, e.g., Michael Fitzgerald, *Cloud Computing: So You Don't Have To Stand Still*, N.Y. TIMES, May 25, 2008, at Bu4, available at 2008 WLNR 9877626.

148. See *What Kind of Scanning/Indexing of User Data Is Done?*, GOOGLE, <https://www.google.com/support/a/bin/answer.py?hl=en&answer=107810> (last visited Oct. 27, 2010).

149. See sources cited *supra* notes 26 and 33.

Internet data for marketing purposes, very clearly state that no human employee will ever see a user's e-mails.¹⁵⁰ Others simply omit e-mail information from the long lists of types of information they may collect and use.¹⁵¹ ISP employees appear to be adhering to these policies with remarkable fidelity, and privacy scholars characterize ISPs' track record on e-mails (and all other forms of personal online data) as "pristine."¹⁵² A detailed search turns up no news reports of employees reading user e-mails or disclosing them to others, nor lawsuits alleging employee violations of privacy.¹⁵³ This can most likely be chalked up to the adherence of employees to explicit privacy policies, the overwhelming volume of (boring) e-mails sent that make casual reading of interesting e-mails unfeasible, and market forces that would incentivize ISPs to harshly discipline any employee who violated user e-mail privacy.

A similar situation can be found in the growing field of cloud computing software. Google and many other leading cloud software providers¹⁵⁴ explicitly state that their processing of cloud computing documents is "automated and involve[s] no human interaction."¹⁵⁵ For any cloud computing service, allowing employees to view personal documents would presumably be devastating to the company's reputation, especially since business clients, who typically place a high value on document confidentiality, are expected to make up a large portion of the cloud computing market.

Aside from cloud computing documents, e-mails appear to be the only form of online data that ISPs do not reserve the right to collect, access, and profit from in their privacy policies.¹⁵⁶ Ironically, however, e-mail content is

150. See *More on Gmail and Privacy*, *supra* note 134 ("Google scans the text of Gmail messages in order to filter spam and detect viruses, just as all major webmail services do. . . . This is completely automated and involves no humans."); *Yahoo! Privacy Policy*, *supra* note 138.

151. See, e.g., *Lycos Network Privacy Policy*, LYCOS, <http://info.lycos.com/privacy.php> (last updated Dec. 17, 2007); *Microsoft Online Privacy Statement*, MICROSOFT, <http://privacy.microsoft.com/en-us/fullnotice.mspx> (last updated Aug. 2010); *Our Privacy Policy*, FASTMAIL, <http://www.fastmail.fm/pages/fastmail/docs/privacy.html> (last visited Oct. 27, 2010).

152. Ohm, *supra* note 141, at 1450-51.

153. See *infra* note 164.

154. See, e.g., *Privacy Policy*, Zoho, <http://www.zoho.com/privacy.html> (last updated Apr. 16, 2010) ("We assure you that the contents of your user account will not be disclosed to anyone and will not be accessible even to employees of Zoho [in this capacity]. We also do not process the contents of your user account for serving targeted advertisements.").

155. *What Kind of Scanning/Indexing of User Data Is Done?*, *supra* note 148.

156. See sources cited *supra* note 145; see, e.g., *Privacy Policy*, GOOGLE, <http://www.google.com/privacypolicy.html> (last updated Oct. 3, 2010) (stating that Google may access online information if it has a "good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to . . . satisfy any applicable law, regulation, legal process or enforceable government request" or to detect fraud, harm to Google, or security breaches). These limited rights of access are akin to those held by telephone companies, who may monitor telephone calls for law enforcement purposes, to detect fraud, or as "a necessary incident to the

probably the form of personal online information *most vulnerable* to employee exposure, precisely because it is the most intimate and interesting type of online data.¹⁵⁷ E-mails and e-mail conversations may be humorous, embarrassing, or amusing on their own terms¹⁵⁸ even if, as is likely, the employee does not personally know the sender or recipient. The same cannot be said for web-surfing information such as IP addresses or URLs.

A list of the IP or URL addresses a user has visited would simply be a list of random numbers or a string of mostly nonsense words. This web-surfing data is also generally anonymized and stored separately from any personal information about the user.¹⁵⁹ Even if an employee translated IP addresses or URLs into their associated websites, it would be difficult to derive much amusement from the anonymous Internet history of even the quirkiest web surfer. And finding that quirky user in the midst of millions of other dull users would be prohibitively difficult.¹⁶⁰ This is a deeply underappreciated reason for the pristine record of ISPs when it comes to human employee access to web-surfing information: there is very little motive for any human being to view this information out of curiosity or for personal enjoyment.

Nor do ISP employees in charge of maintaining an efficient network view such information in the ordinary course of network monitoring. Network monitoring entails repairing a computer network when an Internet router¹⁶¹ or server breaks down, and preventing network slowdowns caused by router and server problems, unanticipated traffic flows, or configuration problems.¹⁶² Network monitors ordinarily view data flows at the network

rendition of [its] service or to the protection of the rights or property of the provider of that service.” 18 U.S.C. § 2511(2)(a) (2006); *United States v. Pervaz*, 118 F.3d 1, 5–6 (1st Cir. 1997).

157. Cloud computing documents might also be vulnerable to employee viewing if they were, for instance, a famous person’s novel or a celebrity’s diary rather than everyday business documents.

158. Humorous or embarrassing e-mails, often sent from work accounts, have been forwarded around the Internet by recipients, and often end up on blogs to be viewed by the public at large. *See, e.g., Email Scandals*, ABOVE THE LAW, http://abovethelaw.com/email_scandals (last visited Oct. 27, 2010).

159. *See infra* note 167.

160. Search terms records or search-engine URLs might be more readable on their own terms than standard URL or IP data, although they are also anonymized and would be difficult (though not impossible) for employees to link to individual users. *See, e.g., Tene, supra* note 143, at 1446–49. It would also be extremely difficult to predict *ex ante* which anonymous string of search terms in a database of millions would be amusing or interesting, and thus worth reading.

161. An Internet router, generally speaking, is a device designed to route and forward packets of information between computers connected over a network.

162. *See, e.g., HEWLETT-PACKARD, A PRACTITIONER’S GUIDE TO MORE EFFICIENT NETWORK MANAGEMENT* 3 (2009); Mike Angell, *Network Management May Rely More Often on Specialty Software*, INVESTOR’S BUS. DAILY, Dec. 31, 2001, at A5.

level; they are concerned with overall performance¹⁶³ and are unlikely to observe the individual actions of a single user unless that user is a hacker in the process of attacking the network.¹⁶⁴ In other words, a network monitor at a large ISP like Comcast would have little time or motivation to observe the activities of a single Internet user out of the thirteen million or so on the Comcast network,¹⁶⁵ unless that user were threatening the network itself. And human observation of individual users has become, if anything, even more unlikely in recent years, as network monitoring and threat-response processes have themselves increasingly become automated.¹⁶⁶

Further, as mentioned above, the comprehensive data collected from Internet users about their web-surfing histories or search term records is processed in large and anonymous blocks of data, unconnected to any personally identifiable information about the user.¹⁶⁷ There is no indication that ISP employees personally observe individuals' subscriber information in the ordinary course of providing online services for their hundreds of millions of users.¹⁶⁸ Further, for the ISPs that collect subscriber information,

163. See, e.g., Ohm, *supra* note 141, at 1470; *vWire: Managing Virtual Infrastructure*, vWIRE (2009), http://dev.vwire.com/_docs/VWDS13_vWire_datasheet.pdf.

164. See, e.g., Ohm, *supra* note 141, at 1466–67, 1470; *Network Attacks Review*, TOPBITS.COM, <http://www.tech-faq.com/responding-to-network-attacks-and-security-incidents.html> (last visited Oct. 27, 2010); Paul Robichaux, *Noticing and Responding to Network-Borne Attacks*, MICROSOFT TECHNET, <http://technet.microsoft.com/en-us/library/cc723457.aspx> (last visited Oct. 27, 2010).

The author contacted several leading ISPs and those that responded confirmed that human employee involvement is limited to situations involving suspected abusive or fraudulent network activity. Kate Dean, Executive Director of the United States Internet Service Provider Association, also provided helpful information and similarly stated that employee access was limited to extraordinary situations. E-mail from Kate Dean, Exec. Dir., U.S. Internet Serv. Provider Ass'n, to Matthew Tokson, Bigelow Fellow, The Univ. of Chi. Law Sch. (Aug. 16, 2010, 21:16 CST) (on file with author).

165. See *Customer Stories: Comcast*, VERTICA, http://www.vertica.com/customers/customer_stories (last visited Nov. 7, 2010) (describing Comcast's use of an automated web-surfing analysis service).

166. See, e.g., TIM GRIESER, IDC, ENABLING DATACENTER AUTOMATION WITH VIRTUALIZED INFRASTRUCTURE 1–2 (2008), available at http://www.vmware.com/files/pdf/analysts/IDC-White-Paper_MGMT.pdf; HEWLETT-PACKARD, *supra* note 162, at 2–3; Press Release, Hewlett Packard, HP Enhances Automation Software To Reduce Cost of Managing Virtualization Technology (Apr. 8, 2009), <http://www.hp.com/hpinfo/newsroom/press/2009/090408a.html>.

167. See, e.g., *In re DoubleClick Privacy Litig.*, 154 F. Supp. 2d 497, 503 (S.D.N.Y. 2001) (describing how targeted advertising is carried out by assigning Internet users a random identification number); *State v. Reid*, 945 A.2d 26, 29 (N.J. 2008) (“[M]ost users continue to enjoy relatively complete IP address anonymity when surfing the Web.”); Tene, *supra* note 143, at 1446–49; Peter Whoriskey, *Every Click You Make: Internet Providers Quietly Test Expanded Tracking of Web Use To Target Advertising*, WASH. POST, Apr. 4, 2008, at D1 (noting that random numbers assigned by ISP “deep packet inspection” that record individual URLs cannot be traced to individual users).

168. Billing processes are frequently automated as well, as automatic processing of customer credit cards is a common form of billing among ISPs and web-based merchants.

connecting this information to a given individual's web-surfing data can be arduous.¹⁶⁹ When law enforcement requires an ISP to identify a single user, the employees often prefer to turn over blocks of data gathered from thousands of customers rather than search through the data for the single customer that the police have targeted.¹⁷⁰ Extensive research turned up no reports of employees linking subscriber information to web-surfing data for personal or recreational purposes, such as spying on the web-surfing habits of an acquaintance who happens to use the ISP where the employee works, and such behavior is obviously not among the acceptable listed uses for personally identifiable information in ISPs' privacy policies.¹⁷¹

Finally, even if ISP employees were highly motivated to spy on users, observing the personal data of a significant number of users would likely be impossible simply due to time constraints. Approximately 248 million Americans use the Internet,¹⁷² writing e-mails, conducting Internet searches, visiting websites, posting comments, and sometimes chatting with other Internet users for hours. To observe with even the barest minimum of comprehension the activity of a typical Internet user would be a very time consuming enterprise. Perhaps a highly trained, highly dedicated employee who worked around the clock would be able to observe the daily Internet activities of, say, forty or fifty Internet users. Even so, it would take millions of such employees to monitor even a fraction of American Internet users. None of this is to say that employee access to personal online data in the absence of law-enforcement coercion is impossible, or that instances of invasive access will never occur.¹⁷³ Rather, the crucial point is that such access is unusual and highly unlikely from the perspective of an individual

169. Orin S. Kerr, Essay, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 294 & n.58 (2005); see Whoriskey, *supra* note 167.

170. Kerr, *supra* note 169, at 294 n.58.

171. See, e.g., 2009 Comcast Customer Privacy Notice, COMCAST, <http://www.comcast.com/customerprivacy/> (revised and effective Jan. 1, 2009); 2009 Customer Information: Your Privacy Rights as a Cox Customer, COX, <http://www.cox.com/policy/annualprivacynotice.asp> (last updated Dec. 10, 2008); Privacy: FAQ, DOUBLECLICK BY GOOGLE, <http://www.doubleclick.com/privacy/faq.aspx> (last visited Oct. 27, 2010); Will Personally Identifiable Information Google Collects Land in Government's Hands?, GOOGLE WIFI HELP, <https://wifi.google.com/support/bin/answer.py?hl=en&answer=30850> (last visited Oct. 27, 2010).

172. See *supra* note 34 and accompanying text.

173. One report exists of a Google employee stalking several teenagers he had befriended by reading their Google Chat transcripts; the employee was fired in July 2010 after his actions were reported to Google. See Adrien Chen, *GCreep: Google Engineer Stalked Teens, Spied on Chats (Updated)*, VALLEYWAG (Sep. 14, 2010, 3:26 PM), <http://gawker.com/5637234/gcreep-google-engineer-stalked-teens-spied-on-chats?skyline=true&s=i>. There have also been unsubstantiated reports of privacy violations by employees of Facebook. See Owen Thomas, *Why Facebook Employees Are Profiling Users*, VALLEYWAG (Oct. 29, 2007, 7:44 PM), <http://valleywag.gawker.com/316469/why-facebook-employees-are-profiling-users>. Of course, most information associated with Facebook is already exposed to many other people and would very likely be outside the scope of Fourth Amendment protection under the Third Party Doctrine.

user. Internet users have no reason to expect that human employees will ever observe their online data. ISPs likely have powerful incentives to prevent their employees from observing or disclosing users' personal information.¹⁷⁴ Isolated instances of employee access would presumably not diminish users' expectations of privacy in online data; after all, isolated instances of employee monitoring of customers' telephone calls has not diminished customers' expectations of privacy in telephone conversations.¹⁷⁵ And employee access will become even less likely as network-monitoring tasks are themselves increasingly automated.¹⁷⁶ In other words, ISP employees do not access individuals' personal online data in the ordinary course of business, or even, in most cases, outside of it.

Nonetheless, third-party ISPs store enormous quantities of users' personal Internet data, and virtually all of it is processed by their automated systems. Courts applying the Third Party Doctrine precedents to the Internet will have to address the question of what this means for Internet users' reasonable expectations of privacy in their online data. Part IV analyzes the privacy implications of disclosing information to third-party automated systems alone.

IV. THE INTERNET USER, AUTOMATION, AND PRIVACY

The Third Party Doctrine is in many ways akin to a doctrine of waiver. It is premised on the idea that voluntarily disclosing one's personal information to a third party renders it no longer wholly secret.¹⁷⁷ The government can obtain such information from the third party without implicating the Fourth Amendment because the individual has already in some sense lost her privacy in it by sharing it with another person.¹⁷⁸

But what if there is no person? The central question for the application of the Third Party Doctrine on the Internet is whether a third party's automated systems will be treated as the functional "counterpart"¹⁷⁹ of an actual human observer. Courts and theorists will have to determine, in other

174. See *infra* Part IV.B.

175. There are several reported cases involving telephone-company employees who have listened in on conversations (generally on suspicion of billing fraud) and reported what they heard to law-enforcement officials. See, e.g., *United States v. Pervaz*, 118 F.3d 1 (1st Cir. 1997); *United States v. Ross*, 713 F.2d 389 (8th Cir. 1983); *United States v. Savage*, 564 F.2d 728 (5th Cir. 1977); *United States v. Auler*, 539 F.2d 642 (7th Cir. 1976); *United States v. McLaren*, 957 F. Supp. 215 (M.D. Fla. 1997).

176. See *supra* note 166 and accompanying text.

177. SOLOVE, *supra* note 33, at 64, 201; see *supra* text accompanying notes 108 and 120; cf. Kerr, *supra* note 111, at 588 (advocating that the court adopt a consent-based, rather than waiver-based, Third Party Doctrine).

178. See, e.g., *United States v. Miller*, 425 U.S. 435, 442-43 (1976); see also SOLOVE, *supra* note 33, at 201 (discussing how information loses its privacy status when the information is exposed to others).

179. See *Smith v. Maryland*, 442 U.S. 735, 744 (1979).

words, whether an Internet user can waive or otherwise lose her privacy in information simply by disclosing it to a third party's automated systems.

Ultimately, as in *Smith v. Maryland*, courts will seek to determine whether Internet users have a reasonable expectation of privacy in such information under *Katz v. United States*. Fully explicating the meanings of the *Katz* test would require an article (or series of articles) on its own. Many such articles have been written without reaching a definitive conclusion. But some common themes have emerged.

Katz's two-part test looks to whether an individual has (1) an actual, subjective expectation of privacy that (2) society recognizes as objectively reasonable.¹⁸⁰ Interpreted literally, this would seem to suggest that Fourth Amendment privacy exists whenever detection is unlikely. But, as the Supreme Court has pointed out, the test is not a purely empirical measure of the probability of observation.¹⁸¹ Thus,

A burglar plying his trade in a summer cabin during the off season may have a thoroughly justified subjective expectation of privacy, but it is not one which the law recognizes as "legitimate." His presence . . . is "wrongful"; his expectation is not "one that society is prepared to recognize as 'reasonable.'"¹⁸²

Instead, the *Katz* test has incorporated a blend of probabilistic analyses, intuitive assessments of social norms and attitudes about whether an expectation of privacy is legitimate,¹⁸³ and normative balancing of the policy interests (personal privacy versus law-enforcement effectiveness) at stake.¹⁸⁴ Whether courts should lean more heavily on assessments of existing social understandings of privacy or on normative considerations is unclear, and the answers offered by legal scholars are likely to vary from case to case. There is also disagreement about how to assess existing social expectations of privacy. Some scholars advocate the use of empirical data about social attitudes; other scholars, and many courts, support simply intuiting

180. See *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

181. *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978).

182. *Id.* (citations omitted).

183. Courts have frequently looked to social norms, practices, and attitudes in applying the objective prong of the *Katz* test. See 1 WAYNE R. LAFAYE, SEARCH AND SEIZURE § 2.1(d), at 439-45 (4th ed. 2004) (collecting sources that discuss how the Court looks to societal attitudes and norms in assessing whether an individual has an objectively reasonable expectation of privacy); see also *Georgia v. Randolph*, 547 U.S. 103, 111-14 (2006) ("The constant element in assessing Fourth Amendment reasonableness . . . is the great significance given to widely shared social expectations. . ."); *Minnesota v. Olson*, 495 U.S. 91, 98-100 (1990) (basing Fourth Amendment scope on "social custom" and societal understandings); *Rakas*, 439 U.S. at 144 n.12 (stating that Fourth Amendment privacy is largely based upon "understandings that are recognized and permitted by society").

184. See *Hudson v. Palmer*, 468 U.S. 517, 525 n.7 (1984); Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 403 (1974); Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 519-22 (2007).

expectations of privacy from personal experiences or deriving them from other areas of law, such as property law.¹⁸⁵

This Article does not advocate for any particular conception of the *Katz* test. Instead, it attempts to offer evidence relevant to the various approaches courts and scholars have used in determining where a reasonable expectation of privacy exists. Thus, Part III addressed the probability of exposure of Internet information to automated systems and human beings. Part IV.A offers a theoretical and intuitive argument that Fourth Amendment privacy is not lost or waived upon mere exposure to automated systems, and argues that our conception of a loss of privacy is bound up with the presence of a human observer. Part IV.B offers empirical evidence that suggests that Internet users share this intuition, and that society as a whole considers information exposed only to automated systems to remain private. Part V will address normative and policy considerations relevant to the question of whether courts should give credence to these social norms and attitudes.

A. A THEORETICAL ANALYSIS OF DISCLOSURE TO AUTOMATED SYSTEMS

An Internet user opens her web browser and visits five websites. Her ISP's software logs the web addresses she visits and stores that information on the ISP's remote server, located on its property. The software processes her web-surfing-history information and uses it to automatically target advertisements to the user. No employee or other person ever observes this information, and some time later the data is discarded unseen. Is her web-address information still "private?" Or has she lost what we think of as privacy in this information?

1. Privacy Theories and the Human Observer

Privacy theorists have largely not addressed the possibility of personal-data collection without eventual exposure to a human observer, probably because, until recently, private entities had little reason to collect personal data unless a human was likely to observe it at some point. It is beyond the scope of this Article to advance a particular theory of privacy, or to give a comprehensive account of what should be considered a "privacy harm." Rather, this Subpart makes a limited theoretical claim about what does *not* constitute a loss of privacy. It argues that information disclosed only to an

185. For instance, Christopher Slobogin and Stephen Henderson have advocated a more explicitly empirical approach to the reasonable expectation of privacy test, SLOBOGIN, *supra* note 26, at 179–96; Henderson, *supra* note 26, at 1000, while Orin Kerr and Lior Strahilevitz have defended a more intuitive approach, Kerr, *supra* note 111, at 543–47; Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 936–38 (2005). Strahilevitz argues, primarily in the context of privacy torts, against a reliance on survey data in assessing expectations of privacy. Strahilevitz, *supra* at 936–38.

automated system remains “private” as that word is commonly used and as it is used in Fourth Amendment law.

Certainly the early conceptions of privacy in the legal literature are based upon the idea of exposure of private facts to other human beings. The first privacy scholars largely focused on harms caused by journalists invading someone’s solitude, or publishing private facts for the public to see.¹⁸⁶ Of course, this may not tell us much, since most means of electronic surveillance did not even exist at the time Samuel Warren and Louis Brandeis wrote their seminal *Harvard Law Review* article on privacy as a legal concept. But deeper theories of privacy developed after the advent of electronic surveillance suggest that the idea of the human observer, with his capacity for curiosity, judgment, and salacious enjoyment of our private affairs, is central to our conception of privacy harm.

In some cases, the focus on human observers is explicit. Many privacy theorists conceive of privacy primarily as a concern for limited accessibility to other people.¹⁸⁷ These theorists have defined privacy harms by reference to the disclosure of personal information to human observers and to uniquely human aspects of observation, like listening, staring at, or otherwise gaining physical access or proximity to the observed.¹⁸⁸ The specific harms that these theorists seek to avoid via limited access, including censure, ridicule, and punishment,¹⁸⁹ also depend on human involvement.

186. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196–97, 205 (1890).

187. See, e.g., SISSELA BOK, *SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION* (1983); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 423 (1980) (claiming our interest in privacy is related to our accessibility to others, including “the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others’ attention”); Hyman Gross, *The Concept of Privacy*, 42 N.Y.U. L. REV. 34 (1967); Sidney M. Jourard, *Some Psychological Aspects of Privacy*, 31 LAW & CONTEMP. PROBS. 307, 307 (1966) (suggesting privacy is like an act of concealment where people “wish to withhold from others certain knowledge as to [their] past and present experience and action and [their] intentions for the future”); Edward Shils, *Privacy: Its Constitution and Vicissitudes*, 31 LAW & CONTEMP. PROBS. 281, 281 (1966) (arguing privacy is a “zero-relationship” between two persons or groups because “it is constituted by the absence of interaction or communication or perception”).

Grouping privacy scholarship into categories is inherently an oversimplification; many of the scholars discussed here touch upon several conceptions of privacy in their work. Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002), provides an excellent overview and critique of the various conceptions of privacy, and I use many of Solove’s categories as a starting point in my analysis of conceptions of privacy harm. See DANIEL J. SOLOVE ET. AL., *INFORMATION PRIVACY LAW* 39–74 (2d ed. 2006).

188. BOK, *supra* note 187, at 10–11; Gavison, *supra* note 187, at 432–33; Gross, *supra* note 187, at 36; Jourard, *supra* note 187, at 311–12 (grounding the concept of privacy in other people’s comprehension of the observed individual); Shils, *supra* note 187, at 281 (defining privacy as limited accessibility “vis-à-vis” other persons and analyzing it as a relationship between persons or groups).

189. Gavison, *supra* note 187, at 448; Jourard, *supra* note 187, at 308.

Other privacy scholars view privacy through the lens of intimacy, intimate information, and personal relationships. This conception of privacy arises from a concern with the pernicious effects on intimacy of a judgmental human observer, likely to misunderstand or even to exploit what he sees.¹⁹⁰ By definition, intimate information is that which no other person should observe without permission, that which should be kept from “humanity as a whole.”¹⁹¹ Intimacy is especially compromised by physical intrusion and persistent visual or auditory observation, as well as the voyeuristic pleasure or curiosity of the observer.¹⁹² Further, privacy harms can result from misjudgments about the observed, someone about whom the observer may know only a single misrepresentative piece of information.¹⁹³ This kind of judgment, or misjudgment, is a familiar social problem. It is also uniquely human. As discussed below, an automated system might unfairly sort an individual into a statistical category, causing a human operator to misjudge her. But the machine alone is incapable of passing judgment, just as it is incapable of misunderstanding (or even trying to understand) the personality of a human being.

A related strand of privacy scholarship focuses on the social harms that stem from lack of privacy, and emphasizes the importance of privacy in fostering development of the self, free from social influence or coercion.¹⁹⁴ This freedom from society and its norms is essential to personal autonomy and the discovery of one’s true preferences; it is a precondition for any functioning liberal democracy.¹⁹⁵ Society and conformity to social norms are, of course, inherently human concepts. Machines can, at most, aid members of society in enforcing norms; they have (thus far) no

190. See JULIE C. INNESS, *PRIVACY, INTIMACY, AND ISOLATION* 57–58, 61–63 (1992) (discussing physical intrusion, persistent staring, and listening as privacy harms to intimacy); Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 268, 273 (1977); Robert S. Gerstein, *Intimacy and Privacy*, in *PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY* 265, 267–69 (Ferdinand D. Schoeman ed., 1984); James Rachels, *Why Privacy Is Important*, in *PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY*, *supra*, at 290, 292, 296.

191. INNESS, *supra* note 190, at 61.

192. *Id.* at 63; Gerety, *supra* note 190, at 271–72; Gerstein, *supra* note 190, at 269–70; Rachels, *supra* note 190, at 297.

193. JEFFREY ROSEN, *THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA* 8–9 (2000); Gerety, *supra* note 190, at 287; Gerstein, *supra* note 190, at 268, 270; see Lawrence Lessig, *Privacy and Attention Span*, 89 GEO. L.J. 2063, 2065 (2001).

194. See, e.g., Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 738–40 (1999); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423–28 (2000); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1647–58 (1999).

195. Allen, *supra* note 194, at 740; Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, in *NOMOS XIII: PRIVACY* 1, 7 (J. Ronald Pennock & John W. Chapman eds., 1971); Cohen, *supra* note 194, at 1423–26; Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381 (1996) (providing a law and economics account of the social value of privacy and the coercive force of constant social exposure); Schwartz, *supra* note 194, at 1648–58.

consciousness and thus no society or social norms of their own. Although technologies such as security cameras can induce citizens to modify their behavior in accordance with social norms, such technologies depend on the implied likelihood of human observation for their socially coercive power.¹⁹⁶ If human beings do not view individual web address logs,¹⁹⁷ users need not feel pressure to conform to social norms when surfing the Internet—and available evidence suggests that they feel no such pressure.¹⁹⁸

Another set of privacy theorists remains, however. Many scholars conceive of privacy primarily as a function of control over one's personal information. We might expect these scholars to conceive of privacy in such a way that disclosure of private information to automated systems would be no different than disclosure to human beings. After all, both involve the collection of one's personal data and thus a loss of absolute control over it. Yet even these theorists' concerns about data collection are largely based upon the potential next step: a human actor deciding what to do with our information. It is ultimately this ceding of control to another's judgment that constitutes the loss of privacy. Charles Fried, who defines privacy as "the *control* we have over information about ourselves,"¹⁹⁹ conceives of the harm of data collection in terms of the "vast opportunities for malice and misunderstanding on the part of authorized personnel" with access to our information.²⁰⁰ Alan Westin discusses privacy in terms of control over information, but also in the context of "the relation of the individual to social participation."²⁰¹ Privacy provides space for "minor noncompliance with social norms" and "allows individuals to deviate temporarily from social etiquette," both of which are essential for the development of personal autonomy and for emotional release.²⁰² Like the intimacy theorists, he fears privacy harms caused by the "curiosity of others"—the observers who may choose to judge the observed and to influence her to conform.²⁰³ Richard Parker is perhaps most explicit about the centrality of human beings to the concept of privacy harms, asserting that privacy is a concept that derives from the dignity and intimacy of the human body itself. He defines privacy as "control over when and by whom the (physical) parts of us (as identifiable

196. See, e.g., Thomas J. L. van Rompay, Dorette J. Vonk & Marieke L. Fransen, *The Eye of the Camera: Effects of Security Cameras on Prosocial Behavior*, 41 ENV'T & BEHAV. 60, 62, 64, 69 (2009) (attributing the effects of surveillance cameras to the "implied presence of others").

197. See *supra* Part III.B.

198. See *infra* Part IV.B.

199. Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968).

200. *Id.* at 490.

201. ALAN F. WESTIN, *PRIVACY AND FREEDOM* 7 (1967)

202. *Id.* at 34–35.

203. *Id.* at 7, 54–56.

persons) can be seen or heard (in person or by use of photographs, recordings, TV, etc.), touched, smelled, or tasted by others.”²⁰⁴

Focusing attention on data-collection and control rights is sensible, especially if the (accurate) presumption is that data collection increases the risk that government agents or other persons might obtain our personal information. But ultimately, the privacy harms identified by the “control” theorists are similar to those described by other scholars: the chilling effects of having one’s behavior observed by others, the possibility of being misunderstood or judged by a capricious human observer, or the overexposure to social influence and coercion that impedes autonomy.

2. The Human Observer in Fourth Amendment Law

Further, this human-centered conception of privacy is arguably reflected in many of the Supreme Court’s Fourth Amendment cases after *Katz*. In cases involving new technologies, the Court’s holdings support the idea that no Fourth Amendment “search” occurs until electronic information is exposed to a human being.²⁰⁵ For instance, in *United States v. Karo*,²⁰⁶ the Court held that the mere placement of a homing beacon among Karo’s belongings did not invade his privacy because the electronic information it transmitted was not monitored by law-enforcement agents.²⁰⁷ As the Court stated, “It is the *exploitation* of technological advances” by police officers that violates the Fourth Amendment, “not their mere existence.”²⁰⁸ When the agents later monitored the beacon inside Karo’s home, only then did they conduct a warrantless search under the Fourth Amendment.²⁰⁹ Similarly, in *Kyllo v. United States*,²¹⁰ the Court held that the use of a thermal imaging device that allowed investigators to see infrared heat waves emanating from a house was a Fourth Amendment search. The Court acknowledged that the Fourth Amendment did not protect heat waves outside of the house, but concluded that the government’s use of a thermal scanner was a search because it allowed government agents to infer activity inside the defendant’s home.²¹¹ Again, without human involvement, mere

204. Richard B. Parker, *A Definition of Privacy*, 27 RUTGERS L. REV. 275, 283–84 (1974).

205. See Orin S. Kerr, *Searches and Seizure in a Digital World*, 119 HARV. L. REV. 531, 553–54 (2005).

206. 468 U.S. 705 (1984).

207. *Id.* at 712.

208. *Id.* (emphasis added).

209. *Id.* (“The mere transfer to Karo of a can containing an unmonitored beeper infringed no privacy interest. . . . To be sure, it created a *potential* for an invasion of privacy, but we have never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment.”)

210. 533 U.S. 27 (2001).

211. *Id.* at 35; see Tokson, *supra* note 123, at 2145–47.

gathering of information by a machine would not have been a Fourth Amendment search.²¹²

The Court's reasoning in *Karo* and *Kyllo* tracks this Article's proposed distinction closely: while data exposed to automated equipment is capable of human monitoring, it remains private unless it is eventually exposed to a human observer. Indeed the logic of *Karo* and *Kyllo* seems to contradict that of the automation rationale, offering a firm doctrinal basis for rejecting it, as I discuss in Part V.

This Part seeks, for the first time, to make explicit what is implicit in the various accounts of privacy discussed above: our concept of a loss of privacy is inextricably bound up in the idea of a human observer. It contends that the automated collection of personal data without eventual exposure to a human observer does not constitute a loss of privacy in theory or law.

3. The Centrality of Human Observation

If no other conscious being senses us or our information, we do not think of ourselves as having lost our privacy. The common element of the violations of privacy discussed above is the exposure of ourselves or our information to another person, an observer capable of judging us and imposing social sanctions,²¹³ of salacious curiosity towards our intimate relationships,²¹⁴ or of misunderstanding who we truly are.²¹⁵ Even if we are unaware of being watched, the human observer gains power over us and deprives us of some measure of our dignity, as the intimate details of our lives become subject to his whim and discretion.²¹⁶

By contrast, machines alone cannot condemn, or "see," or enjoy our personal information. Today's automated equipment performs all sorts of complex tasks—in some cases the same tasks that humans used to perform, like connecting telephone calls. It is easy to anthropomorphize these

212. See Kerr, *supra* note 205, at 553–54.

213. WESTIN, *supra* note 201, at 34; Allen, *supra* note 194, at 738–40; Cohen, *supra* note 194, at 1423–28; Gavison, *supra* note 187, at 448; Jourard, *supra* note 187, at 308; Schwartz, *supra* note 194, at 1647–58; see Murphy, *supra* note 195, at 2381.

214. INNESS, *supra* note 190, at 57–58, 61–63; WESTIN, *supra* note 201, at 55–56; Fried, *supra* note 199, at 482; Gerety, *supra* note 190, at 233, 268, 273; Gerstein, *supra* note 190, at 265, 267–69; Rachels, *supra* note 190, at 290, 292, 296.

215. ROSEN, *supra* note 193, at 8–9; Gerety, *supra* note 190, at 287; Gerstein, *supra* note 190, at 268, 270; Lessig, *supra* note 193, at 2065.

216. See WESTIN, *supra* note 201, at 33; Benn, *supra* note 195, at 7 (discussing the effects of scrutiny by an outside observer). A useful way to conceptualize the privacy harms caused by an unknown human observer is to think of a peeping Tom. Imagine that a woman undresses in her bedroom and then takes a shower while a peeping Tom is perched outside in a tree, peering at her through binoculars. A policeman on patrol walks by the house and sees Tom, shakes the tree until he falls out, and arrests him without alerting the still-showering woman. Tom cannot convincingly say to the policeman, "I am innocent. I have not violated anyone's privacy because the woman never knew I was there!" Rather, as the policeman would likely reply, Tom has severely violated the woman's privacy; she is simply not aware of the violation.

capable machines, to think of the computers that analyze personal data and send targeted advertisements as the equivalent of a human salesman tailoring his sales pitch to his audience. But without some modicum of human observation, disclosure of our information to automated systems alone is ultimately no different from “disclosure” to any other inanimate object that stores our personal data. Automated computers alone do not “observe” us any more than a digital bathroom scale observes our weight, or the walls of a storage locker observe our personal belongings, or our word-processing document observes what we type. These devices cannot see us, think about us, judge us, ridicule us, or be curious about us—they cannot perceive us at all. They cannot, then, truly violate our privacy.

To be sure, the collection of data by automated Internet systems may create what we might think of as a harm simply by placing large amounts of our personal information on a third party’s property. But the harm is, by its nature, a probabilistic one—an increase in the *risk* of exposure of our personal data to others.²¹⁷ It does not in itself constitute the elimination of privacy. In fact, automated systems are increasingly the means by which we *maintain* privacy in a world where virtually every transaction involves the collection of personal information.²¹⁸

Still, other objections to the above claims might be raised. Depending on how we define “privacy harm,” harms involving deterrence of activity (“chilling-effect” harms) could occur without human observation. One suffers, for instance, a chilling effect when faced with a security camera that is sometimes monitored by human observers, even if no human happens to be monitoring the camera when one passes by. And typically this chilling effect itself is considered a harm related to privacy. Daniel Solove’s influential taxonomy of privacy harms includes several other types of harms related to privacy that do not involve direct observation of any kind, but rather an increased risk of eventual observation.²¹⁹ These harms include data insecurity, exclusion from one’s data, the unauthorized secondary use of already-disclosed data, and “increased accessibility.”²²⁰ My claim is not that such chilling-effect or increased-risk harms are unworthy of statutory attention or recognition in tort law. Rather, these types of harms should be distinguished from our binary, is-it-private-or-not conception of a “loss of privacy” (and its legal counterpart, the “all-or-nothing”²²¹ Fourth Amendment). Creating a chilling effect or otherwise deterring people from engaging in private activities can certainly be considered a harm related to

217. See Solove, *supra* note 14, at 488.

218. Machines frequently allow us to keep our information away from actual observers. For instance, automated systems anonymize the names of movies that hotel guests order so that the desk clerk cannot judge them by their viewing habits. See Murphy, *supra* note 195, at 2398.

219. See Solove, *supra* note 14, at 488.

220. See *id.* at 505–41.

221. See, e.g., Amsterdam, *supra* note 184, at 388.

privacy and worthy of legal redress. But being chilled or subject to risk of eventual exposure to human observers cannot itself constitute a *loss* or *violation* of privacy as we use those terms, or as they are used in Fourth Amendment law.

Consider the absurdity of equating these kinds of “privacy harms” with the loss of one’s privacy under the Fourth Amendment. For example, John composes an e-mail on his desktop e-mail program. Concerned about the potential scanning of e-mails by spam filters or advertising software, or human employees, he is “chilled” and decides not to send the e-mail. John has suffered what many scholars would justifiably call a privacy harm, but has he lost his privacy in the drafted and unsent e-mail? Can the government now hack into his computer and obtain the e-mail without a warrant? Again, because no being other than John has observed (or even been made aware of) the e-mail, the best answer is that the e-mail remains private. We could perform a similar thought experiment with the risk-based harms and with many other privacy-related harms scholars have identified in recent years.²²²

One additional category of privacy-related harms may be of particular concern. As several critical surveillance theorists have asserted, people can experience harm when their personal information is used to sort them (automatically or otherwise) into categories, especially on the basis of race, gender, or demographic and socioeconomic status.²²³ Legal scholars have identified similar harms stemming from the unwanted processing of disclosed information, and the inability of data subjects to view or make corrections to their records.²²⁴ All of these harms could be classified as harms relating to privacy, but none of them constitutes a loss of privacy in the absence of disclosure to a human being. To contend that privacy is lost whenever information is used by man or machine to “sort” people, or to grant or deny them access to resources, would be to modify our current conceptions of privacy to the point of unrecognizability. We are constantly using information to classify people, and we often use these classifications to treat people differently, sometimes beneficially and sometimes problematically. If privacy were to require an end to all information-based

222. See generally Solove, *supra* note 14 (providing a taxonomy to understanding privacy violations).

223. See OSCAR H. GANDY, JR., *THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION* 2, 15–18 (1993); David Lyon, *Surveillance as Social Sorting: Computer Codes and Mobile Bodies*, in *SURVEILLANCE AS SOCIAL SORTING: PRIVACY, RISK AND DIGITAL DISCRIMINATION* 13, 20–22 (David Lyon ed., 2003). The claim that increased data gathering generally leads to more pernicious discrimination has been criticized by Lior Strahilevitz, who has pointed out that in many contexts richer information can reduce the tendency to rely on crude proxies such as race or gender. See Lior Jacob Strahilevitz, *Reputation Nation: Law in an Era of Ubiquitous Personal Information*, 102 NW. U. L. REV. 1667, 1702 (2008).

224. M. Ryan Calo, Essay, *The Boundaries of Privacy Harm*, 86 IND. L.J. (forthcoming 2011) (manuscript at 27), available at <http://ssrn.com/abstract=1641487>; Solove, *supra* note 14, at 518–22.

social sorting, it would require “unthinkable” social change far beyond what even the critical theorists propose.²²⁵ As leading surveillance theorist David Lyon makes clear, the problem the critical theorists target is neither a lack of privacy nor social sorting per se, but rather *discriminatory* sorting occurring in both private and public spheres.²²⁶ The crux of the harm identified here is not the accessing of information, which is often publically available,²²⁷ but rather what is done with the already-exposed information. Again, this is arguably a harm related to privacy. But it is not, as this Article contends, a harm relevant to the concept of a loss of privacy—the concept that drives Fourth Amendment law.

This Subpart has presented a novel theoretical analysis of privacy violations and privacy harms. If its central claim is correct, then the currently dominant conception of Internet privacy—that it is lost as soon as information is disclosed to a third-party automated system—should be modified. Yet arguably just as important for Fourth Amendment purposes as the theory itself is the evidence supporting it—evidence that Internet users consider information exposed only to automated Internet systems to be private.²²⁸

B. INTERNET USER ATTITUDES AND BEHAVIOR

Imagine that, as some courts have suggested,²²⁹ the exposure of information to third-party automated equipment is the equivalent of

225. Lyon, *supra* note 223, at 13. Even Karl Marx, the proto-critical theorist, famously advocated allocating work to “each according to his ability” and distributing goods “to each according to his needs.” KARL MARX, *CRITIQUE OF THE GOTHA PROGRAM* 27 (Wildside Press 2008).

226. See Lyon, *supra* note 223, at 18–19, 26–27 (disavowing additional privacy as a solution to the deeper problem of discriminatory social sorting).

The idea that sorting or data-processing technologies can be directly equated with their human creators is similarly incompatible with our conceptions of privacy. Humans designed the telephone and coded word-processing software, yet we consider the information we expose to these technologies to be private. Deadbolt locks on the doors of houses help to sort people into categories—those who can legitimately enter and occupy a house and those who cannot. This sorting largely depends upon individuals’ economic resources and property rights. Yet one who uses a house lock (or is excluded by it) does not lose his privacy, as we use that term. In other words, to point out that human beings designed and coded automated Internet systems, and that such systems may help to sort people according to their personal characteristics, raises interesting questions about technology and social structure but does not tell us much about privacy.

227. See Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1263–67 (2008).

228. See discussion *infra* Part IV.B.

229. See *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008); *In re United States*, 665 F. Supp. 2d 1210, 1224 (D. Or. 2009); see also *Rehberg v. Paulk*, 598 F.3d 1268, 1282 (11th Cir. 2010) (holding that voluntary disclosures to third party equipment eliminate a citizen’s expectation of privacy), *vacated*, 611 F.3d 828 (11th Cir. 2010); *United States v.*

exposure to human employees. Polling data on Internet users' attitudes towards data collection on the Internet would be surprising, to say the least—large percentages of Internet users appear to be unconcerned with the exposure of their personal online data. For instance, in a recent poll only 54% of Internet users reported being “uncomfortable with third parties collecting information about their online behavior.”²³⁰ Of course, this may be a function of the fact that Internet users have a poor understanding of data collection practices on the Internet. Although they are generally aware that websites may collect their web-surfing data,²³¹ they have little understanding of how extensive the data collection is or how their information is used for advertising purposes.²³² However, polls that tell Internet users that their online activity will be collected and used to tailor advertisements to them report similar levels of comfort with the practice, with only 59%,²³³ 53%,²³⁴ and 51%²³⁵ of users reporting themselves “uncomfortable” in recent polls.²³⁶

Further, these numbers may drastically overstate the level of real concern among Internet users. Even the roughly half of Internet users who claim to be uncomfortable with data collection and targeted advertisements do not appear to be taking substantial steps to protect their private data online.²³⁷ Several polls have reported “discrepancies between respondents’

Perrine, 518 F.3d 1196, 1205–06 (10th Cir. 2008) (same); *United States v. Hambrick*, No. 99-4793, 2000 WL 1062039, at *3–4 (4th Cir. Aug. 3, 2000) (same).

230. *Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy*, CONSUMERSUNION.ORG (Sept. 25, 2008), http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html.

231. *Id.*; Joseph Turow, Deirdre K. Mulligan & Chris Jay Hoofnagle, *Research Report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace*, 2 (Oct. 2007), http://groups.ischool.berkeley.edu/samuelsonclinic/files/annenberg_samuelson_advertising.pdf.

232. Sixty-one percent of Internet users believe that their online data is “not shared without their permission.” *Consumer Reports Poll*, *supra* note 230. Another poll found that 55% of Internet users believe that the existence of a privacy policy alone means that the site cannot sell collected information to other companies. Turow, Mulligan & Hoofnagle, *supra* note 231, at 2.

233. Press Release, David Krane, Vice President, Harris Interactive, Majority Uncomfortable with Websites Customizing Content Based Visitors Personal Profiles, at 1 (Apr. 10, 2008), <http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Majority-Uncomfortable-with-Websites-Customizing-C-2008-04.pdf>.

234. *Consumer Reports Poll*, *supra* note 230.

235. Press Release, Behavioral Targeting: Not That Bad?! TRUSTe Survey Shows Decline in Concern for Behavioral Targeting (Mar. 4, 2009), http://www.truste.com/about_TRUSTe/press-room/news_truste_behavioral_targeting_survey.html.

236. When one poll asked about if tailored ISPs were to give better notice of their practices and offer some choice about the types of tailored advertisements shown, only 45% remained uncomfortable and 55% reported themselves comfortable with targeted advertising. Press Release, Krane, *supra* note 233, at 2.

237. Note that one may be more “uncomfortable” than “comfortable” about a practice like automated online data gathering without actually being worried about it. Also, many Internet users find Internet ads annoying, *see* Anne Kandra & Andrew Brandt, *The Great American Privacy Makeover*, PC WORLD, Nov. 2003, at 146, *available at* <http://www.pcworld.com/article/112468/>

concerns about online dangers and their practices.”²³⁸ Despite high numbers of users reporting themselves concerned about their online data, only about 8% of users routinely take steps to protect their privacy.²³⁹ Only 28% of all Internet users usually check whether a website has a privacy policy at all.²⁴⁰ Privacy-protective services have generally failed to attract users in the marketplace.²⁴¹ Users also appear to be unwilling to spend the time and effort necessary to gain expertise about online privacy—in one poll, 64% of users reported that they never search for instructions on how to protect their online information, and 5% reported doing so only once.²⁴² In fact, the information cost of acquiring knowledge about the best means to protect online privacy is probably the most substantial cost facing privacy-concerned Internet users.²⁴³ Yet, even computer experts do not appear to take substantial steps to hide their information—one study showed that advanced Internet users, and even the editors of *PC World* magazine, do not do much more than the average user to protect their online privacy.²⁴⁴

Does all of this mean that a large proportion of Internet users are indifferent to the privacy of their online data? This Article argues that it does not. Rather, while users perceive disclosure of their personal information to humans as a serious privacy harm, they do not consider disclosure to automated systems alone to be a significant harm.²⁴⁵ The

great_american_privacy_makeover.html, and they may rate themselves as “uncomfortable” with receiving any ads at all.

238. *Id.*

239. Miguel Helft, *Ask.com Puts a Bet on Privacy*, N.Y. TIMES, Dec. 11, 2007, at C1.

240. *Survey Information: Americans Care Deeply About Their Privacy*, CTR. FOR DEMOCRACY & TECH. (Oct. 22, 2009), <http://www.cdt.org/privacy/guide/surveyinfo.php> (reporting the results of a December 2006 poll).

241. For instance, Ask.com recently marketed a free anonymized search engine feature, and its market share has actually dropped (probably due to the emergence of Bing, a search engine that does collect search-term data) since it started offering the feature. *Compare* Helft, *supra* note 239 (stating that Ask.com had a 4.7% share of the search market in 2007), with *Nielsen Reports December U.S. Search Rankings*, NIELSENWIRE (Jan. 13, 2010), http://blog.nielsen.com/nielsenwire/online_mobile/nielsen-reports-december-u-s-search-rankings (stating that Ask.com now has a 1.7% share of the search market in December 2009).

242. JOSEPH TUROW, ANNENBERG PUB. POLICY CTR. OF UNIV. OF PA., AMERICANS AND ONLINE PRIVACY: THE SYSTEM IS BROKEN 25 (2003), available at http://www.annenbergpublicpolicycenter.org/Downloads/Information_And_Society/20030701_America_and_Online_Privacy/20030701_online_privacy_report.pdf.

243. Much of the software that one might use to protect one’s identity online is available for free, *see, e.g.*, ANONYMOUSE, <http://anonymouse.org> (last visited Oct. 27, 2010); TOR, <http://www.torproject.org> (last visited Oct. 27, 2010), yet it appears to be little-used outside of nations like China and Iran.

244. Kandra & Brandt, *supra* note 237, at 146.

245. It is worth noting that it can be difficult to discern from some of the evidence discussed whether or not Internet users would object to *any* exposure of their information to human beings, or whether they only care about such exposure when the information can be linked to their name and address. The limited survey data available on this question suggests that users are at least somewhat concerned about human observation of even their anonymous

evidence is largely circumstantial, but taken as a whole, it builds a compelling case. For instance, one recent survey of Internet users from the Annenberg School for Communication at the University of Pennsylvania is an outlier among privacy polls. It reports that 68% of respondents “definitely” would not allow and 19% “probably” would not allow advertisers to gather their web-surfing data.²⁴⁶ The finding that 87% of users were not comfortable with targeted advertising is far higher than the 51%–59% reported in other polls taken during the last two years.²⁴⁷ There is nothing obvious in the phrasing of the questions to suggest that the Annenberg poll described targeted advertising in any materially different way than the other polls—they mentioned that user data would be processed anonymously and that the advertisements would be delivered “in exchange for free content.”²⁴⁸ However, the poll’s description of targeted advertising differed in one subtle respect. It suggested that human marketers and advertisers actually track users’ online behavior, following them around the Internet and seeing what they see. Thus, marketers “often use technologies to follow the websites you visit and the content you look at in order to better customize ads,” and “advertisers . . . follow you online” to gather your web-surfing data.²⁴⁹ This anthropomorphic phrasing appears to have a substantial impact—only 10% of users responding to this question would “probably” allow such anonymous tracking, and only 2% would “definitely” allow it,²⁵⁰ in contrast to the 41%–49% of users who would do so in the other polls.

1. Internet User Survey

This Subpart reports the results of a survey of seventy-one law students who regularly use the Internet. The survey was conducted to assess attitudes about the invasiveness of various potential privacy harms. It was modeled

data. *See infra* note 246 and accompanying text. Ultimately this is not an important distinction for the purposes of this article. Users may reasonably conclude that their privacy is not at all compromised by disclosure of their data to human beings when that data cannot be linked to them personally—they may not consider themselves “observed” in such circumstances. In any event, anonymized web-surfing data is not generally viewed by human employees in practice. *See supra* Part III.B. The relevant point is that users do not appear to be concerned by the disclosure of their personally identifiable data to automated systems, while they appear to be very concerned by disclosure of such data to other human beings. The online information used in criminal investigations that many courts have found to be unprotected by the Fourth Amendment is, of course, not anonymous—it has been linked to the specific user. It is user concern about this kind of disclosure that is the focus of this Subpart.

246. Joseph Turow et al., Annenberg Sch. for Commc’n, *Americans Reject Tailored Advertising and Three Activities That Enable It*, 16 (2009), <http://www.ftc.gov/bcp/workshops/privacy-roundtables/Turow.pdf>.

247. *See supra* notes 233–35.

248. Turow et al., *supra* note 246, at 14; Press Release, Krane, *supra* note 233.

249. Turow et al., *supra* note 246, at 14 (internal quotation marks omitted).

250. *Id.* at 16.

after Christopher Slobogin and Joseph Schumacher's useful study of the perceived invasiveness of different types of police actions.²⁵¹ Respondents were presented with several hypothetical scenarios (arranged randomly²⁵²), and asked to rate the scenarios on a scale of 1 to 10, with 1 representing an action not at all invasive of privacy, 5–6 moderately invasive of privacy, and 10 maximally invasive of privacy. Results are reported in Table 1.

251. See Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727 (1993).

252. Four versions of the survey were created, each with a random ordering of scenarios, and distributed in equal numbers.

TABLE 1

Privacy Scenarios	Invasiveness Rating 1–10
Receiving a spam e-mail	2.7
A hacker obtains your bank records	9.7
A hacker obtains your e-mail address information over past 6 months	9.0
A person eavesdrops on several of your cell-phone calls	9.5
Spam filter automatically blocks an e-mail from known spammers	2.0
Spam filter software scans the text of your e-mails looking for words commonly used in spam	3.4
E-mail software scans e-mails and places contextual ads above them (e.g., Gmail)	5.5
ISP employee reads several e-mails, tells no one	8.7
ISP employee reads e-mails, forwards some to friends	9.8
ISP computers collect web-surfing data and send targeted ads	6.1
ISP employee collects web-surfing data and sends targeted ads	8.4
ISP sells to advertiser, advertiser's computers collect web-surfing data and send targeted ads	6.9
ISP sells to advertiser, advertiser's employee collects web-surfing data and sends targeted ads	8.6
Difference between advertiser's employee and automated processing of web-surfing data	1.7 ^{***}
Difference between ISP employee and automated processing of web-surfing data	2.3 ^{***}
Difference between employee and automated scanning of e-mail content	5.3 ^{***}

*** Denotes that the difference is significant at a 1% level (99% confidence).

This survey offers further evidence that Internet users distinguish between exposure to human beings and exposure to automated systems. Respondents gave high invasiveness ratings to baseline scenarios such as a

hacker obtaining their bank records (9.7), a person eavesdropping on their cell-phone calls (9.5), and a hacker viewing their e-mail to/from addresses (9.0). The highest rating was given to a scenario in which an ISP employee read user e-mails, and forwarded some of the e-mails to coworkers and friends (9.8). A modified scenario in which the employee did not forward or otherwise disclose the e-mails rated an 8.7, suggesting that most of the perceived invasiveness of the e-mail-reading scenario stems from the act of a human being reading the e-mails, rather than any potential further consequences or the chance of public exposure.²⁵³ By contrast, the reading of e-mail content by automated spam detection software rated only a 3.4, suggesting that the respondents distinguished sharply between disclosure of their e-mails to automated systems and disclosure to human beings. This rating is higher but still comparable to the ratings received by the lowest-rated baseline scenarios: receiving an e-mail from a “spammer” (2.7) and anti-spam software automatically blocking a spam e-mail without scanning (2.0).

Respondents’ distinction between automated and nonautomated targeting of advertising was less dramatic, but still substantial. Respondents rated the observation of their web-surfing data and the transmission of targeted ads by human employees at 8.4, while they rated the automated processing and transmission of targeted ads at 6.1. While a sizable and statistically significant (at the 1% level) difference, the disparity in ratings is noticeably less than the disparity between automated and human observation of e-mail content. There are several potential explanations for this result, all of which may be operating to some degree. The first is the simplest—some respondents may not have understood that no human employees were involved in the automated ad targeting process. The question provided that data was collected and processed by automated computers, but it did not specify that the data would never be observed by human employees. A forcefully worded statement such as “no human being ever sees the information” was omitted from the scenario to avoid the risk of biasing the results in favor of a low rating. Some respondents may have made a similar mistake to the one many judges have made, and simply assumed that the collection of web-surfing data by a third party’s equipment meant that human employees would eventually access the information.

A second, related explanation may be that the rating reflected the perceived risk of eventual exposure to human employees or of full public exposure. Again, the scenario did not provide that the information was discarded unseen or that no human being would ever observe the information, and the possibility of this occurrence (perhaps made salient by

253. See *supra* note 158 (discussing the public disclosure of amusing e-mails).

the numerous other scenarios involving exposure of personal information to human beings²⁵⁴) may be reflected in the 6.1 rating.²⁵⁵

A third explanation, which the survey does not rule out, is that users perceive the storage of their personal information by a third party's automated systems or the use of such information to target advertisements as itself intrusive of privacy.²⁵⁶ It is possible that the storage of already-processed information, without more, causes an actual invasion of privacy (rather than simply an increase in the risk of eventual exposure to human beings), but this would be highly counterintuitive. A more plausible explanation would be that users perceive some intrusion on their privacy simply from receiving ads, regardless of additional monitoring.²⁵⁷ Even if this is the case, it may tell us less about privacy than it appears to. An analogy might be drawn to polls where respondents have indicated that receiving a telephone call from a telemarketer is invasive of privacy, regardless of whether the telemarketer receives any personal information from the call recipient.²⁵⁸ It is at least possible that these people are conflating the inconvenience of receiving an unwanted phone call with the invasiveness of a loss of personal privacy.

Again, these explanations are not mutually exclusive, and it seems likely that all of them play some role. In any event, this survey's results show that respondents differentiate between disclosure of their information to an automated system and disclosure to a human employee. In the case of web-based ads, the difference is strongly statistically significant. In the (simpler) case of e-mail content, the difference is nothing short of dramatic.

254. The students surveyed had also recently completed a writing assignment that involved privacy tort issues and the Internet, so they may have been especially sensitive to the risks of Internet information disclosure.

255. A modified version of the scenarios which involved the sale of data or rights to access data to third-party advertisers returned higher ratings and a somewhat smaller difference between human and automated processing, with human employee access rated at 8.6 and automated processing rated at 6.9. (The difference between the two ratings, while smaller, remains statistically significant at the 1% level.) The higher rating for third-party automated scanning may reflect the perceived increased risk of exposure when personalized data is shared with other parties.

256. Another possibility is that the respondents feel that their web-surfing histories are more private than the contents of their e-mails, but this is very unlikely, especially since respondents rated the reading by an employee of their e-mails without further disclosure or use at 8.7, higher than the observation and use by an employee of their web-surfing histories, which received an 8.4 rating.

257. This effect would also explain why users gave a rating higher than 1 to merely receiving spam e-mails from a spammer. It may also explain why a scenario describing an e-mail service like Gmail, which scans e-mails and places context-relevant ads above one's e-mails and e-mail inbox, received a 5.5 rating.

258. See *Public Opinion on Privacy*, ELEC. PRIVACY INFO. CTR., <http://epic.org/privacy/survey/> (last visited Oct. 27, 2010) (reporting the results of a July 2000 poll by *USA Weekend*).

2. Other Evidence

Of course, polls are imperfect tools for measuring attitudes about online privacy. There are other sources of evidence that Internet users distinguish between human and computerized observation. For instance, it is well known that the Gmail service scans the content of users' e-mails and uses that content to deliver relevant advertisements. The policy is spelled out explicitly in Gmail's privacy policy, and the content-relevant ads appear right at the top of users' e-mails.²⁵⁹ Presumably at least some of Gmail's 37 million monthly users value the privacy of their e-mails. Most likely, these users agree with Google that "[w]hen e-mail messages are fully protected from unwanted disclosure, the automatic scanning of e-mail does not amount to a violation of privacy," because the scanning is "completely automated and involves no humans."²⁶⁰ Yahoo! Mail, with 106 million unique monthly users, conducts similar scans for searching and indexing purposes.²⁶¹ Yahoo! makes the same assertion that automated scanning does not violate privacy, and emphasizes that no human ever reads users' e-mails.²⁶² The implication is that Gmail and Yahoo! Mail's millions of users will tolerate pervasive disclosure to automated equipment but will not tolerate any exposure to human beings.

In one instance, aspects of users' online behavior were disclosed to other people, and the users reacted with outrage. Facebook, the popular social-networking website, briefly ran a program called Beacon that automatically collected web-surfing information from third-party websites and then used that information to send messages to people's Facebook "friends" about sites they had visited, in the hopes of getting the friends to visit as well. Users could opt out of the program, but the messages were sent if they did not explicitly do so. The program immediately met with protests and complaints from Facebook users who felt their privacy had been invaded.²⁶³ A month after introducing it, Facebook responded to the backlash (which by then included a campaign against the program led by activist group MoveOn.org) by making Beacon an opt-in program, meaning that users had to affirmatively sign up for it before the program collected any data or sent any messages.²⁶⁴ It shut down the program for good in 2009, as part of a \$9.5 million settlement of a class-action lawsuit brought by

259. *More on Gmail and Privacy, supra* note 134.

260. *Id.*

261. Schonfeld, *supra* note 130; *Yahoo! Privacy Policy, supra* note 138.

262. *Yahoo! Privacy Policy, supra* note 138 ("No person reads your email, nor is any personal information collected or stored in [the scanning] process. Your email is just as private with or without this feature enabled.")

263. *See, e.g.,* Farhad Manjoo, *Facebook Finally Lets Users Turn Off Privacy-Invasive Ads*, SALON.COM (Dec. 6, 2007), http://www.salon.com/tech/machinist/blog/2007/12/06/facebook_beacon/index.html.

264. *Id.*

Facebook users.²⁶⁵ Again, if users considered their web-surfing data no longer private after disclosing it to automated-data collection systems, it is unlikely that so many of them would have reacted with such anger to Facebook's ad program, which differed from other online ad programs only in that it revealed users' web-surfing activities to other human beings.²⁶⁶

One can also infer that Internet users generally consider their Internet use private despite the relatively well-known fact that websites may collect their online data from the wide range of intimate activities that they engage in online.²⁶⁷ From online voting, to viewing pornography, to visiting substance-abuse or medical condition support group websites,²⁶⁸ users engage in activities online that are generally considered extremely private or intimate. It is unlikely that many users would engage in these activities if they felt that ISPs or websites collecting basic web-surfing data from them in automatic and anonymized fashion were akin to human beings viewing their web-surfing activity.

In sum, the available evidence indicates that Internet users do not consider disclosure of their online information to automated equipment to be a privacy harm in and of itself, but that they consider disclosure of their information to other human beings to be a substantial harm. At least it appears by their actions that users are generally indifferent to the former and actively hostile to the latter. It is likely that the main reason for users' apathy is that they simply perceive that having their online data automatically gathered produces no consequences beyond generating targeted ads, which they may not even notice. To be sure, these users incur an increased risk of their data being viewed or even disclosed by ISP employees, but the risk is minimal in virtually all cases.²⁶⁹ In other words, users' indifference is not only understandable, it is probably rational. Taking steps to avoid web-surfing tracking and targeted ads would be a time consuming process, and users would incur fairly high information costs, which would arguably outweigh the benefits of avoiding the small risk of an eventual privacy harm.²⁷⁰ Further, if enough users avoided targeted

265. Jon Brodtkin, *Facebook Halts Beacon, Gives \$9.5M To Settle Lawsuit*, PC WORLD (Dec. 8, 2009), http://www.pcworld.com/article/184029/facebook_halts_beacon_gives_95m_to_settle_lawsuit.html.

266. Of course, disclosure of a user's online activities to her friends and associates might be more upsetting than disclosure to a snooping Facebook employee who is a stranger to the user.

267. See *supra* note 231 and accompanying text.

268. See *supra* notes 40–43 and accompanying text.

269. See *supra* note 152 and accompanying text.

270. Bargaining with individual ISPs over specific privacy policy provisions would likely be far more costly—scholars have estimated the total time cost to Americans of merely reading all applicable privacy policies at over \$700 billion (roughly \$3534 per Internet user). Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 564–65 (2009) (estimating the cost to Americans of reading all of their applicable privacy policies at around \$781 billion); see also CTR. FOR THE DIGITAL FUTURE, *supra*

advertising, websites might be forced to charge users for access to their content.

Users strongly prefer to have free access to web content and receive web ads rather than pay for content without ads.²⁷¹ This Subpart thus proposes a new model of Internet-user behavior in privacy markets. Internet users largely do not eschew privacy-protective technologies and practices because of privacy-market failures, collective-action problems, bounded rationality, and the like.²⁷² The primary reason they do not undertake time-consuming efforts to avoid automated data collection is that they do not perceive it as a privacy harm, or at least consider it a small enough harm that the benefits of avoiding it do not outweigh the costs.

V. DOCTRINAL AND THEORETICAL APPLICATIONS

The arguments of the previous Part may be relatively intuitive (or they may not²⁷³), but their doctrinal and theoretical implications are potentially enormous. This Part examines these implications for both courts and scholars addressing the question of Fourth Amendment protection for online data. Using the analysis developed in Parts III and IV, it describes how a court might address the Fourth Amendment issue in the absence of confusion about disclosure to human employees. It analyzes potential grounds for distinguishing *Smith v. Maryland*, and concludes that *Smith* can easily be distinguished and limited to its unique facts. It defends this corrected approach from potential criticisms and compares it to alternative schemes for applying the Fourth Amendment to personal online data. It then examines further theoretical implications of the model of consumer behavior proposed in Part IV.

A. THE CHOICE

In recent years, more and more courts have had to decide whether the Fourth Amendment applies to online data.²⁷⁴ Litigation of this issue will only increase as Internet use, Internet-based crimes, and the government's

note 22, at 29 (noting that 80% of Americans use the Internet); *U.S. Population Clock*, *supra* note 34 (estimating U.S. population at over 310 million people).

271. CTR. FOR THE DIGITAL FUTURE, *supra* note 22, at 120 (noting that only 16% of Internet users would prefer to pay for content without ads, compared to 51% who would prefer free content supported by ads); Press Release, Knowledge Networks, New Knowledge Networks Study Shows Streamers, Downloaders Reject For-Pay Model: One in Four Is "More Inclined" To Buy from Sponsoring Brands (Mar. 18, 2009), http://www.knowledgenetworks.com/news/releases/2009/031809_forpay.html (finding that 80% of Internet users prefer to view advertisements in exchange for free video content rather than pay for content).

272. See discussion *infra* Part V.C.3.

273. See, e.g., *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (holding that Internet users have no reasonable expectation of privacy in Internet information disclosed to "third party equipment").

274. See, e.g., cases cited *supra* note 44.

use of Internet data as evidence become more prevalent.²⁷⁵ Courts facing this issue must decide, explicitly or implicitly, whether the disclosure of online data to automated systems divests the data of any Fourth Amendment protection. Courts will have to choose between two legal paradigms for such disclosure. The first paradigm is that of disclosure to human beings. Courts could decide that disclosure to automated systems on the Internet is no different than disclosure to a government informant, and that therefore any information disclosed to and processed by computers cannot be protected by the Fourth Amendment.

The second paradigm is that of the “rental property” cases, which generally hold that citizens retain an expectation of privacy in things stored on another’s property, so long as the owner of the property has only limited rights of access to the stored items.²⁷⁶ The Supreme Court has held that a landlord cannot consent to a police search of a renter’s apartment, despite the landlord’s ownership of the premises and the fact that a landlord has the right to access the property for some purposes.²⁷⁷ Likewise, renters have a reasonable expectation of privacy in items stored in a third party’s storage locker, regardless of rights of access.²⁷⁸ Similar rules apply to packages handed over to a third-party common carrier,²⁷⁹ and to items stored in a shop or in another person’s home.²⁸⁰ Thus, numerous cases have held that

275. See Tokson, *supra* note 123, at 2109–10.

276. See *Georgia v. Randolph*, 547 U.S. 103, 112 (2006); Bellia, *supra* note 66, at 1405.

277. *Chapman v. United States*, 365 U.S. 610, 616–18 (1961). Arguably, another reason for this ruling may be the necessity of affording some Fourth Amendment protection to renters—otherwise akin to homeowners, who traditionally receive strong Fourth Amendment protections—despite the fact that their landlords may at times observe their apartments. This “homeowner equivalency” rationale appears to be the driving force behind the cases that hold that hotel guests retain Fourth Amendment protection in their rooms, despite the fact that the hotel’s “maids, janitors, or repairmen” regularly access them. *Stoner v. California*, 376 U.S. 483, 489 (1964); see *United States v. Jeffers*, 342 U.S. 48 (1951); *Lustig v. United States*, 338 U.S. 74 (1949). An alternative explanation would be that these employees may have only very limited rights to access the room without the guest’s permission (e.g., they will not disturb the room of a guest who hangs the appropriate sign), thereby preserving the guest’s privacy right in the room itself. In any event, landlords do not routinely access their renters’ apartments, and their rights of access in law are quite limited, see *Chapman*, 365 U.S. at 616, a situation roughly analogous to ISP or telephone company access to customer communications, see *supra* note 156 and accompanying text. Courts have also applied the rationale of *Chapman* beyond the residential context. See *infra* notes 278–80 and accompanying text.

278. *United States v. Karo*, 468 U.S. 705, 721 n.6 (1984); *United States v. Johns*, 851 F.2d 1131, 1136 (9th Cir. 1988); see *United States v. Reyes*, 908 F.2d 281, 286 (8th Cir. 1990); *United States v. Rahme*, 813 F.2d 31, 34 (2d Cir. 1987); see also *United States v. Barry*, 853 F.2d 1479, 1481–83 (8th Cir. 1988) (holding that defendant had a reasonable expectation of privacy in suitcase that airport was holding for safekeeping).

279. See *United States v. Jacobsen*, 466 U.S. 109, 114 (1984); *United States v. Souza*, 223 F.3d 1197, 1201–02 (10th Cir. 2000); Bellia, *supra* note 66, at 1407.

280. *United States v. Fultz*, 146 F.3d 1102, 1105 (9th Cir. 1998) (holding that homeowner could not consent to police search of defendant’s box stored on his property); *United States v.*

merely storing things with a third party, even one with some rights of access, is not sufficient to eliminate Fourth Amendment protection in the things stored. Courts deciding whether the Fourth Amendment protects online information could choose to adopt this paradigm and determine that the Third Party Doctrine is inapplicable to all online information not disclosed to human employees, even if ISPs reserve rights of access in certain situations.

1. The Current Confusion

Unfortunately, courts have largely avoided reaching this issue altogether. As discussed in Part II, the Ninth Circuit in *United States v. Forrester* simply adopted *Smith's* automation rationale and applied it to Internet data.²⁸¹ Other courts have conflated disclosure to automated systems with disclosure to human employees without referring to *Smith*.²⁸² Many of these courts have based their rulings on unsupported, and likely incorrect, factual or legal claims. In *United States v. Hambrick*,²⁸³ the Fourth Circuit stated that a defendant “knowingly revealed” the subscriber information associated with his IP address to an ISP’s “employees,” without examining whether any employees ever accessed such information.²⁸⁴ In *Freedman v. America Online, Inc.*,²⁸⁵ the district court employed a remarkable bit of circular reasoning to determine that online data was disclosed to human employees, holding that subscriber information associated with Freedman’s IP address “was exposed to AOL employees in the normal course of business, as evidenced by AOL’s compliance with Defendants’ request for Plaintiff’s subscriber information.”²⁸⁶ Apparently, the fact that employees could access information when compelled by the police was sufficient to destroy any reasonable expectation of privacy in the information itself. By this logic, citizens could not have an expectation of privacy in their telephone calls, which phone-company employees can easily access and record when compelled by legal process.²⁸⁷

In a recent case involving the Fourth Amendment and stored e-mails, the district court stated that users of Google’s Gmail service have no

Most, 876 F.2d 191, 197–98 (D.C. Cir. 1989) (holding that police could not pat down bag left with store clerk, regardless of the fact that the clerk could have permissibly touched the bag).

281. 512 F.3d 500, 504 (9th Cir. 2008).

282. See *supra* notes 125–28 and accompanying text.

283. No. 99-4793, 2000 WL 1062039, at *3–4 (4th Cir. Aug. 3, 2000).

284. *Id.*

285. 412 F. Supp. 2d 174 (D. Conn. 2005).

286. *Id.* at 183; see also *United States v. Sherr*, 400 F. Supp. 2d 843, 848 (D. Md. 2005) (finding no expectation of privacy in subscriber information given to AOL because AOL customer agreement stated that AOL would turn over such information to the government if compelled by legal process).

287. See, e.g., *United States v. Kerrigan*, 514 F.2d 35, 38 (9th Cir. 1975); *United States v. Mares-Martinez*, 240 F. Supp. 2d 803, 815 (N.D. Ill. 2002).

expectation of privacy in the contents of their e-mails.²⁸⁸ The court based its ruling on its conflation of automated systems with human employees, claiming without any support that the defendants “voluntarily . . . exposed to the ISP’s employees *in the ordinary course of business* the contents of their e-mails.”²⁸⁹ If this were true, one suspects the employees would not be in

288. *In re United States*, 665 F. Supp. 2d 1210 (D. Or. 2009); *see also* *Rehberg v. Paulk*, 598 F.3d 1268, 1281 (11th Cir. 2010) (holding that the Fourth Amendment does not apply to e-mail content obtainable from third party ISPs), *vacated*, 611 F.3d 828 (11th Cir. 2010).

289. *In re United States*, 665 F. Supp. 2d at 2224 (emphasis added). The district court also relied upon Google’s general privacy policy, which stated that Google will disclose subscribers’ information when it has a “good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to . . . satisfy any applicable law, regulation, legal process or enforceable government request.” *Id.* (quoting *Privacy Policy*, *supra* note 156) (internal quotation marks omitted). Other courts have pointed to the importance of similar access rights in privacy policies, albeit in cases with limited precedential value. *See* *Warshak v. United States*, 532 F.3d 521, 527–28 (6th Cir. 2008) (en banc) (vacating the case on ripeness grounds); *United States v. Maxwell*, 45 M.J. 406, 417 (C.A.A.F. 1996). There are several arguments against basing Fourth Amendment protection on the access provisions of privacy policies rather than actual practices on the Internet. The privacy policies provide for only limited access rights, and the rental property line of cases suggest that such rights do not eliminate Fourth Amendment protection in the absence of regular access. *See* text accompanying notes 276–80. The privacy policy cases also run afoul of *Smith’s* refusal to make expectations of privacy depend on individual telephone company policies—it concluded that to do so would make an unadministerable “crazy quilt” of the law. *Smith v. Maryland*, 442 U.S. 735, 745 (1979). The Internet’s quilt would be even crazier. Some ISPs have no privacy policy at all while the rest have individualized and often lengthy policies, which they generally update or change every year or so. If the Fourth Amendment depends upon the language of such policies rather than the actual practices of ISPs, Fourth Amendment litigation over Internet privacy may be endless. Further, basing Fourth Amendment protection solely on the language of privacy policies would be inconsistent with several Fourth Amendment cases dealing with the surveillance of employees in the workplace. In cases like *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir. 2008), *rev’d sub nom. City of Ontario v. Quon*, 130 S. Ct. 2619 (2010), and *United States v. Long*, 64 M.J. 57 (C.A.A.F. 2006), courts have looked beyond the mere language of Internet policies that provide for total access to employee online data and examined whether employers have actually accessed such data. Relying only on policy language in the context of home use would lead to the strange result that Internet communications sent from the workplace and subject to invasive monitoring policies would receive more Fourth Amendment protection than communications sent from the home and not subject to routine monitoring. Finally, the provisions in the privacy policies at issue in *In re United States* and *Warshak* are very similar to provisions of the ECPA that allow telephone providers to record telephone calls and disclose them to law-enforcement officials where appropriate. 18 U.S.C. § 2511(2)(a)(i) (2006) (“It shall not be unlawful under this chapter for . . . an officer, employee, or agent of a provider of wire or electronic communication service . . . to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service.”); *id.* § 2511(2)(a)(ii) (providing for telephone company compliance with law-enforcement requests). In fact telephone companies appear to record or listen to customers’ phone calls and report what they overhear to law enforcement officials more frequently than ISP employees independently monitor Internet activity and report it to law enforcement. *See, e.g., United States v. Pervaz*, 118 F.3d 1 (1st Cir. 1997); *United States v. Ross*, 713 F.2d 389 (8th Cir. 1983); *United States v. Savage*, 564 F.2d 728 (5th Cir. 1977); *United States v. Auler*, 539 F.2d 642 (7th Cir. 1976); *United States v. McLaren*, 957 F. Supp. 215 (M.D.

business for very long. Further, Google explicitly promises that no human being will read users' e-mails, and by all accounts keeps this promise.²⁹⁰ The courts that have held that Internet users' online information is not protected by the Fourth Amendment have done so either on the basis of an unexamined application of *Smith's* automation rationale to the Internet context, or by simply conflating disclosure to automated systems with disclosure to humans.

2. The "Rental Property" Paradigm

In order to reach the issue of how to treat online information exposed only to automated systems, courts will have to avoid making the erroneous factual claim that human employees regularly access such information. Assuming they do, this Subpart proposes that courts adopt the "rental property" paradigm and rely on the rental cases to analyze disclosure of online information to automated machines. In both situations, humans generally have only limited-access rights and, in practice, do not regularly access the stored items or data. By contrast, in the leading Third Party Doctrine case *United States v. Miller*, bank employees regularly accessed customer records in the course of their everyday business.²⁹¹ A crucial basis for the Third Party Doctrine cases was the idea that human informants or employees could be subpoenaed to testify about what they had heard or seen without implicating the Fourth Amendment, and therefore, the Fourth Amendment could not bar the admission of tapes or records that merely offered a more reliable version of their testimony.²⁹² Yet in the Internet context there will likely be no employee that could possibly testify about a user's online information, because no employee will have seen it (in the absence of government compulsion).²⁹³

As discussed in Part IV.B, available evidence suggests that Internet users conceive of automated servers on the Internet more like rental property²⁹⁴ than like human beings. The point is intuitive. Individuals engage in

Fla. 1997). Regardless, telephone users continue to have a reasonable expectation of privacy in their telephone calls under *Katz*. See, e.g., *Kyllo v. United States*, 533 U.S. 27, 32–33 (2001). Thus there is little reason why privacy policies providing only limited access to electronic communications or other data should by themselves eliminate an expectation of privacy in online data.

290. See *supra* notes 150–52 and accompanying text.

291. 425 U.S. 435, 442 (1976).

292. See *supra* notes 94–96, 103, 111 and accompanying text.

293. Human employees who surveil an individual at the government's behest are considered government agents, and the surveillance would violate the Fourth Amendment. See, e.g., *Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971).

294. ISPs also profit from the use of collected user data and targeted advertising; in exchange for this advertising revenue, they provide online services to users. This exchange of services for revenue is not materially different from a rental arrangement where a renter exchanges money for the rental of a room or storage locker.

intimate activity in hotel rooms or even rental cars, and store personal belongings in storage bins and lockers, because while they or their belongings are exposed to a third party's equipment, they are not actually observed by any third party. They view pornography, send personal e-mails, and even vote on the Internet, for the same reason. They do not think of themselves as viewing pornography in front of an ISP employee, or letting the employee stand in the voting booth with them, or allowing her to read a personal e-mail before they send it.

Further, failing to treat Internet data as private would create a troubling contradiction in the law. As discussed earlier, Supreme Court cases like *United States v. Karo* and *Kyllo v. United States* suggest that no Fourth Amendment search occurs until private information is exposed to a human being.²⁹⁵ Applying *Smith's* automation rationale to the Internet would require holding that information disclosed only to automated equipment is exposed and thus no longer private for Fourth Amendment purposes. But the logic of the first idea undermines the second—if exposure to the government (a “search”) does not occur without human observation, then exposure to a third party does not occur without it either.

Under the legal paradigm of the rental-property cases, the Third Party Doctrine would presumably be inapplicable to all online information not disclosed to human employees, and such information would thus receive Fourth Amendment protection under *Katz v. United States*. Of course, in theory, a court could determine that the Third Party Doctrine does not apply but still determine under a fresh application of the *Katz* test that society is not prepared to recognize a privacy interest in certain types of Internet information regardless of the fact that no human being sees them.²⁹⁶ This Article does not suggest that protecting all Internet information with a warrant requirement is the only conceivable legal regime for the Internet. It does claim, however, that as it stands today, there are no grounds in existing Fourth Amendment law or privacy theory for equating disclosure to machines with disclosure to government informants or to human employees.

But what of *Smith* and its correlation of automated telephone equipment with the human operators of old? For several reasons, *Smith* can be easily distinguished and limited to its unique facts. Many scholars have advocated that *Smith* be overturned because it uses the Third Party Doctrine.²⁹⁷ Others have (justifiably) criticized it as a poorly reasoned and

295. See *supra* Part IV.A.2.

296. See *infra* Part V.B.

297. See *supra* note 26 and accompanying text.

poorly written opinion.²⁹⁸ The analysis of this Article suggests a different reason why *Smith* may have been wrongly, or at least sloppily, decided. *Smith* arguably makes the same mistake as the recent Internet cases in that the Court assumes that human employees of telephone companies regularly access telephone number information. For instance, most of the examples it gives of regular employee access to telephone numbers, such as “to check for a defective dial, or to check for overbilling,”²⁹⁹ involve employees checking billing statements upon a customer’s request. Beyond these rare and fully consented instances, it is not clear whether modern-day phone-company employees access their customers’ phone numbers at all.³⁰⁰ This is not to say that *Smith* must be overturned, or that it is likely that the Court will overturn it on the basis that its analysis of exposure to human employees was faulty. But the dubious reasoning of *Smith* provides a further reason for the Court to limit its holding to its facts if there are grounds for doing so. And there are several potential grounds for limiting *Smith* and for distinguishing it from disclosure of information on the Internet.³⁰¹

The most compelling of these is that *Smith* depends upon the unique context of telephone operation, which unlike data transmission on the Internet, was performed by human employees for decades before it was automated.³⁰² Societal expectations of privacy in telephone numbers were initially formed when callers told human operators the names or numbers of

298. See, e.g., Bellia, *supra* note 66, at 1402; Cate, *supra* note 27, at 455; Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 157 (2002).

299. *Smith v. Maryland*, 442 U.S. 735, 742 (1979). *Smith* also claims that phone companies “regularly” monitor numbers “to determine whether a home phone is being used to conduct a business.” *Id.* at 742 (quoting Note, *The Legal Constraints upon the Use of the Pen Register as a Law Enforcement Tool*, 60 CORNELL L. REV. 1028, 1029 (1975)) (internal quotation marks omitted). This is a particularly specious example of human access; it refers to a single case where a phone company monitored dialed phone numbers after a customer had ordered a personal and a business line, but then suspiciously cancelled the business line after being told it would be metered. See *id.*; see also *Schmulker v. Ohio-Bell Tel. Co.*, 116 N.E.2d 819 (Ohio 1953) (upholding telephone companies’ use of pen registers to ensure that home phones were not being used to conduct business).

300. The Court emphasizes that telephone companies may view dialed numbers without customer permission in order to “detect[] fraud.” *Smith*, 442 U.S. at 742. But telephone companies also listen to actual telephone conversations for the same purpose, a practice explicitly permitted by the ECPA, 18 U.S.C. § 2511(2)(a)(i)–(ii) (2006), and yet customers retain a Fourth Amendment right in their conversations, see *supra* note 289.

Unlike conversations, telephone numbers did appear on customer’s monthly bills, which in 1979 may have been handled by employees and mailed by hand. Unfortunately the Court never examines the extent to which employees saw the numbers on customers’ bills. Finally, telephone company employees generally have little reason to want to look at telephone numbers, since the names and numbers themselves, like strings of IP addresses or URLs, have little independent interest or meaning.

301. See *infra* note 306.

302. See ANTON A. HUURDEMAN, *THE WORLDWIDE HISTORY OF TELECOMMUNICATIONS* 232 (2003). The last manual telephone exchange was finally retired in 1978. *Id.* at 232 n.3.

the people they wished to call.³⁰³ Operators, often young women who lived in the same town where they worked, may have known the people whose calls they connected.³⁰⁴ The Justices of the *Smith* majority, who grew up with this method of telephone switching, essentially offered a privacy analysis of the old, human-based system and then stated that they were “not inclined” to reach a different result “because the telephone company had decided to automate.”³⁰⁵ Thus, *Smith* indicates, without actually addressing the question, that societal expectations of privacy in telephone numbers had not changed despite the replacement of this system with an automated switching system. This may be correct. Regardless, the reasoning cannot apply to the Internet context, where transmission, collection, and scanning of data have been automated from the beginning. *Smith*’s automation rationale can be distinguished on the basis that it depends entirely on the unique history of the telephone and the fact that human operators once performed the tasks that automated equipment now performs.³⁰⁶

B. THE FUTURE OF KATZ ON THE INTERNET

1. The Content/Noncontent Alternative

Although most privacy scholars addressing the Third Party Doctrine have focused on arguing for its abandonment,³⁰⁷ a few have proposed alternative schemes for applying the Fourth Amendment in the Internet context.³⁰⁸ Most prominent among these is the proposal that the law should

303. *See id.* at 188.

304. A telephone operator’s social status resembled that of a domestic servant. IRVING FANG, A HISTORY OF MASS COMMUNICATION: SIX INFORMATION REVOLUTIONS 87 (1997).

305. *Smith*, 442 U.S. at 744–45.

306. A court could offer several other reasons for distinguishing *Smith*. *Smith*’s best point about disclosure to human employees is the appearance of their long-distance phone calls on their monthly bill. There is at least a small possibility of employees reading over the phone numbers a customer dials in the course of printing or mailing her monthly bills. Of course, Internet users do not receive a bill from their network provider listing all of the websites they visited or people they e-mailed. For e-mails, a court might distinguish *Smith* on the basis that while telephone customers were surely aware that the telephone company recorded their long distance calls, many e-mail users are likely unaware that spam and virus filters actually read their e-mail content and thus do not “voluntarily disclose” their e-mails to scanning equipment. *See id.* at 744. Finally, a court might take *Smith*’s assertions of regular employee access to telephone numbers to check for defective dials or overbilling at face value and determine that no equivalent human access occurs in the Internet context. In short, if *Smith* is not to be overturned on the basis of its automation rationale, it can nonetheless easily be distinguished from cases dealing with Internet information and limited to its unique facts.

307. *See supra* notes 25–26.

308. Stephen Henderson has proposed a nine-factor test for determining whether the Fourth Amendment applies to personal information Internet data. It is essentially a normative balancing test, explicitly weighing law enforcement and privacy interests for each individual disclosure of data. *See Henderson, supra* note 26, at 988–89. Christopher Slobogin has advocated a multi-tiered regime of levels of suspicion required to obtain different kinds of

track the old distinction between content and envelope information originally developed for mail delivered by the U.S. Postal Service.³⁰⁹ The proposal is both attractive on policy grounds and based in existing case law, as several courts dealing with Internet information have already drawn on the analogy between e-mails and paper mail.³¹⁰ Proponents of this alternative argue that the Fourth Amendment should protect content information on the Internet, such as the body of e-mails, while noncontent information, such as e-mail to/from addresses or IP addresses of websites, should receive no protection.³¹¹

Advocates of this alternative (or other, less conventional alternatives) might object to this Article's proposals on the ground that they are too strictly empirical. These advocates might say that, legal and theoretical arguments aside, a proposal to treat Internet information as private because no human being sees it is flawed because it lacks any normative balancing of law-enforcement interests with privacy interests. Supporters of a strict content/noncontent distinction might further argue that the Court has already performed such a normative balancing in the 1877 decision of *Ex parte Jackson*,³¹² which famously determined that envelope information is not protected by the Fourth Amendment. Today's Court is therefore compelled to adhere to this decision and to import it as closely as possible to the Internet context.

But such a criticism would be based on a misunderstanding of this Article's proposals. The *Katz* test can indeed be normative—the objective prong of the test is generally the controlling factor, and the objective inquiry

Internet data based on a survey that measured how intrusive people consider different kinds of searches of their personal property or information. SLOBOGIN, *supra* note 26, at 179–96. For a critique of these approaches, see KERR, *supra* note 111, at 586, and Orin S. Kerr, *Do We Need a New Fourth Amendment?*, 107 MICH. L. REV. 951 (2009) (reviewing CHRISTOPHER SLOBOGIN, *PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT* (2007)).

309. Orin S. Kerr, *Applying the Fourth Amendment to Internet Communications: A General Approach*, 62 STAN. L. REV. 1005 (2010) [hereinafter Kerr, *Applying the Fourth Amendment*]; see Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide To Amending It*, 72 GEO. WASH. L. REV. 1208, 1227–28 & n.142 (2004) [hereinafter Kerr, *A User's Guide*]; Rich Haglund, Note, *Applying Pen Register and Trap and Trace Devices to Internet Communications: As Technology Changes, Is Congress or the Supreme Court Best-Suited To Protect Fourth Amendment Expectations of Privacy?*, VAND. J. ENT. L. & PRAC., Spring 2003, at 137, 141–42. See *Ex parte Jackson*, 96 U.S. 727, 733 (1877) (stating that letters sent by mail were protected by the Fourth Amendment, while information on their envelopes or packages was not); *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008) (“The government’s surveillance of e-mail addresses also may be technologically sophisticated, but it is conceptually indistinguishable from government surveillance of physical mail.”).

310. See *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 905 (9th Cir. 2008), *rev'd sub nom.* *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010); *Forrester*, 512 F.3d at 511; see also *Smith*, 442 U.S. at 741 (distinguishing *Katz* in part on the basis that it dealt with content information).

311. See *supra* note 309.

312. 96 U.S. 727.

into what “*society* is prepared to recognize as ‘reasonable’”³¹³ often contains a strong normative element.³¹⁴ But while the Third Party Doctrine cases dealing with Internet information may be driven by implicit normative considerations, the conclusions of most of the cases depend on a purely factual assertion—that the human employees of an ISP regularly see customers’ personal information, which is *therefore* not protected by the Fourth Amendment.³¹⁵ This Article proposes doing away with this inaccurate assertion. As for *Forrester*, its holding is based on the erroneous legal supposition that disclosure to machines is the equivalent of disclosure to human employees.³¹⁶ This Article attacks this supposition as well and concludes that information disclosed to ISP equipment is not exposed under the Third Party Doctrine. However, once a court determines that the Third Party Doctrine does not apply, it is nonetheless free to continue to apply a normative version of the *Katz* test. It will simply be doing so without cutting off the *Katz* inquiry prematurely based on an erroneous factual or legal assumption.

At that point, the court may still use any of the proposed alternative methods to determine whether to protect, for instance, noncontent Internet information. It could explicitly weigh the interests of law enforcement against individuals’ privacy interests on a case-by-case basis.³¹⁷ It may even conclude that there can never be a reasonable expectation of privacy in any noncontent information.³¹⁸ But it must do so explicitly, without masking its normative balancing behind a flawed conception of disclosure to automated systems.

2. *Katz* Without the Automation Rationale and the Dangers of Analogy

As discussed above, courts may legitimately decide to deprive all noncontent Internet data of Fourth Amendment protection. However, they would face a substantial doctrinal obstacle in doing so. As discussed in Part IV, noncontent Internet information is not exposed to human observation

313. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

314. See *Hudson v. Palmer*, 468 U.S. 517, 525 n.7 (1984); Kerr, *supra* note 184, at 519–22 (arguing that a normative, policy-based model of Fourth Amendment protection features “heavily . . . in a few cases, moderately in some cases, and not at all in other cases”).

The Supreme Court has stated that if the government were to erode actual expectations of privacy by announcing a normatively unacceptable policy, a court should nonetheless find that the Fourth Amendment applies. *Smith*, 442 U.S. at 741 n.5; see also *Amsterdam*, *supra* note 184, at 403 (discussing the normative nature of the *Katz* test).

315. See *United States v. Perrine*, 518 F.3d 1196, 1205–06 (10th Cir. 2008); *United States v. Hambrick*, No. 99-4793, 2000 WL 1062039, at *3–4 (4th Cir. Aug. 3, 2000); *In re United States*, 665 F. Supp. 2d 1210, 1224 (D. Or. 2009); *Freedman v. Am. Online, Inc.*, 412 F. Supp. 2d 174, 183 (D. Conn. 2005); *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000).

316. See *supra* Part IV.

317. See *Henderson*, *supra* note 26, at 1025.

318. See Kerr, *Applying the Fourth Amendment*, *supra* note 309.

in practice, and Internet users appear to consider such information to be private. It would be unusual (although not unprecedented) for a court to determine that information that is functionally private and that society generally treats as private is nonetheless not protected by the Fourth Amendment because the court believes that law enforcement ought to have access to the information regardless.³¹⁹

Jackson certainly drew no such conclusion. Rather, *Jackson* was based upon information exposure in practice.³²⁰ Indeed, proposals to import the content/noncontent distinction from traditional mail to the Internet provide a striking example of the dangers of analogy in applying existing law to new technologies. Postal employees regularly see the information on envelopes but do not see the contents of the envelopes. The decision in *Jackson* to protect letters but not their envelopes was a practical decision based upon actual employee behavior; yet today it is used to justify *deviating* from actual employee practices on the Internet.³²¹ Further, although paper letters and e-mail may seem to be “conceptually indistinguishable”³²² and therefore ripe for analogy, subtle differences between Internet and paper communications can become enormously significant in the surveillance context, arguably dwarfing the similarities.

Human postal employees, who often live in the same town as the sender, see the sender’s envelopes, but ISP employees do not look at a sender’s e-mail to/from information. Thus, a person living in a small town might be more reluctant to mail a letter to, say, the Impotence Association or Alcoholics Anonymous than to send those organizations an e-mail. A postal worker in 1896 at best might have recalled the address information of one or two suspicious packages sent or received by an individual. Even if told by police to monitor all packages and letters with a certain address, the postal worker only could have monitored the suspect’s mail going forward, and even that would be ineffective unless the sender included a return address on the outer envelope. Today, law-enforcement officials can obtain the addresses of every e-mail a user has sent or received for years, and the sender inevitably reveals his address to his service provider when he sends an e-mail. The typical e-mail user also likely sends far more messages per day than the typical letter writer sent in 1896. And with greater access to a greater volume of noncontent data come additional opportunities to obtain intimate information about the sender. For instance, researchers at the Massachusetts Institute of Technology were able to determine a Facebook

319. *Illinois v. Caballes*, 543 U.S. 405 (2005), and *Rakas v. Illinois*, 439 U.S. 128 (1978), are arguably examples of the Supreme Court finding no expectation of privacy even in areas (the trunk and glove compartment of a car) that society generally regards as private.

320. See 96 U.S. 727, 733 (1877).

321. *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008); Kerr, *Applying the Fourth Amendment*, *supra* note 309, at 1020–23.

322. *Forrester*, 512 F.3d at 511.

user's sexual orientation just by analyzing his list of contacts;³²³ a similar analysis could likely be performed on an Internet user's e-mail contacts.³²⁴ Finally, a recent study suggests that people consider law-enforcement officials obtaining their noncontent Internet information to be particularly invasive of their privacy.³²⁵ Participants rated police acquisition of web-surfing records as more intrusive than a physical pat-down, and acquisition of e-mail to/from information as more intrusive than a physical search of one's car.³²⁶ Presumably the viewing of traditional mail envelope information would be considered far less intrusive.

All of these differences suggest the benefits of courts undertaking a fresh *Katz* analysis for noncontent Internet data rather than simply drawing an analogy to a paper mail case from over 100 years in the past. Applying older sources of law to new technological contexts is unlikely to be as smooth or simple as it first appears. This Subpart's analysis calls into question the line of scholarship that proposes that analogies to traditional doctrinal contexts are always sufficient to address legal questions surrounding new technologies.³²⁷ Drawing the legal line at protecting content and exposing noncontent might very well be the best approach. Alternatively, courts might take an intermediate approach and require "reasonable suspicion" for the government to access noncontent information.³²⁸ But before reaching any conclusion, the Court should evaluate the balance of law-enforcement and privacy interests anew, without confusion over disclosure to automated systems, or uncritical adherence to existing law governing other technologies.

3. Burdening Law Enforcement

Another related potential objection to applying the Fourth Amendment to all forms of online information is that requiring a warrant to obtain noncontent Internet information would unduly burden the police. It could

323. Matthew Moore, *Gay Men 'Can Be Identified by Their Facebook Friends'*, TELEGRAPH (Sept. 21, 2009), <http://www.telegraph.co.uk/technology/facebook/6213590/Gay-men-can-be-identified-by-their-Facebook-friends.html>.

324. Computer scientists using "re-identification algorithms" have also been able to identify the owners of anonymous Internet accounts based in part on social-network analysis. Steve Lohr, *How Privacy Vanishes Online*, N.Y. TIMES, Mar. 16, 2010, <http://www.nytimes.com/2010/03/17/technology/17privacy.html>.

325. SLOBOGIN, *supra* note 26, at 184.

326. *Id.*

327. See Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207; see also Kerr, *Applying the Fourth Amendment*, *supra* note 309, at 1015 (arguing that analogies to the pre-Internet world should dictate how the Fourth Amendment is applied on the Internet); Kerr, *supra* note 111, at 574-79 (explaining how the third party doctrine can be justified via analogies to a world without third party communications).

328. See SLOBOGIN, *supra* note 26, at 185-86; see also *Terry v. Ohio*, 392 U.S. 1, 27 (1968) (establishing the "reasonable suspicion" standard for investigative stops by police).

prevent them from gathering the initial evidence required to show probable cause, and thus preclude effective investigations altogether.³²⁹ This is a substantial concern. If experience proves that depriving law enforcement officials of the ability to obtain noncontent Internet data without a warrant significantly impedes their ability to investigate crime, then courts may have good reason to determine that noncontent data is unprotected by the Fourth Amendment despite its lack of exposure to humans. But there is evidence to suggest that this concern is overstated. Many police officers already lack easy access to noncontent information such as telephone numbers. Eleven states have rejected the Third Party Doctrine in some form on state constitutional grounds, and their courts have typically ruled that the police cannot obtain dialed phone numbers without a warrant.³³⁰ Further, police may often be able to gather sufficient evidence for probable cause before obtaining noncontent Internet information. Take the subscriber-information cases, for instance. In *Hambrick*, the police requested the subscriber information of an Internet user who they knew had tried to entice an undercover agent posing as a fourteen-year-old boy into living with him.³³¹ In *United States v. Perrine*, police saw the child pornography their suspect had sent to another user before requesting his subscriber information.³³² It is highly likely that police had probable cause with respect to these users and could have obtained a warrant for the personal information if one had been required. By contrast, in *Freedman*, local police officials obtained the subscriber information of a user who had anonymously sent a purportedly threatening e-mail to supporters of a primary candidate who opposed his favored candidate.³³³ The e-mail was tame at best, no charges were ever filed, and the officers likely lacked probable cause to believe that the user had committed a crime.³³⁴ Arguably, applying the Fourth Amendment to noncontent information would not prevent police from obtaining the information in the course of most valid investigations, but would deter fishing expeditions or politically motivated investigations. Given the government's track record with electronic surveillance, deterring politically motivated data-gathering might even be worth the cost of slightly diminished law-enforcement effectiveness.

329. Kerr, *A User's Guide*, *supra* note 309, at 1228 n.142; see *In re Subpoena Duces Tecum*, 228 F.3d 341, 348–49 (4th Cir. 2000).

330. Stephen E. Henderson, *Learning from All Fifty States: How To Apply the Fourth Amendment and Its State Analogs To Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 396–99 nn.118–28 (2005).

331. *United States v. Hambrick*, No. 99-4793, 2000 WL 1062039, at *1 (4th Cir. Aug. 3, 2000).

332. *United States v. Perrine*, 518 F.3d 1196, 1199 (10th Cir. 2008).

333. *Freedman v. Am. Online Inc.*, 412 F. Supp. 2d 174, 180 (D. Conn. 2005).

334. The e-mail stated only that “The End is Near,” probably referring to the impending loss of the opposing candidate. See *id.*

4. Statutory Alternatives

Although the prospects for a broad revision of the ECPA appear dim at present, Congress could act to increase statutory protections for Internet data either before or after the Court issues a Fourth Amendment ruling. What would such legislation look like? Some fixes are relatively obvious and widely supported among privacy scholars.³³⁵ This Article's analysis and its model of Internet-user behavior offer additional considerations and guidelines for a more sensible statutory regime.

For instance, as some scholars have advocated,³³⁶ new legislation should do away with the distinction between e-mails and other content data stored for 180 days or less and content stored for over 180 days, as well as the distinction between opened and unopened e-mails in storage. Both distinctions are based on the now obsolete idea that e-mails stored online for more than 180 days or opened e-mails stored online for any length of time were abandoned by the recipient, who essentially waived his privacy interest in them by failing to import them to his home computer.³³⁷ As discussed above, Internet users do not waive their privacy interests in content data stored online with a third party and disclosed to its automated systems; rather, available evidence suggests that they consider such stored information to remain wholly private.³³⁸

As for noncontent Internet data, this Article has suggested that the Court should weigh law-enforcement interests in obtaining noncontent information against the privacy interests of Internet users, whose noncontent information is virtually always free from human observation. It has also argued that noncontent data on the Internet has the power to reveal far more about individuals and their activities than the envelope information of an earlier era. Congress should engage in a similar balancing of interests with these considerations in mind if it undertakes to amend the ECPA. It could plausibly determine that such information should be protected by a warrant requirement, or that anything but easy access to

335. Many scholars have advocated new legislation that would offer the same level of protection to personal data stored with a "remote computing service" (which today includes cloud computing and photographic storage services) as it does to electronic communications. Bellia, *supra* note 66, at 1436; Mulligan, *supra* note 33, at 1593-96. They have also argued that the ECPA should be amended to include an exclusionary rule. Bellia, *supra* note 66, at 1436; Kerr, *supra* note 33, at 837-40. New legislation might also do away with the restrictive definition of "electronic storage" in the Act and extend its protections to services that are used like public services but are not available to the general public, such as university-run e-mail and Internet services. *See supra* notes 66-67 and accompanying text.

336. Bellia, *supra* note 66, at 1436; *see* Mulligan, *supra* note 33, at 1582-92.

337. Bellia, *supra* note 66, at 1422.

338. *See supra* Part IV. Doing away with these distinctions would mean that e-mails and other content data would be protected by a warrant requirement. *See* 18 U.S.C. § 2703(a) (2006).

noncontent information would burden law enforcement to such a degree that the current subpoena requirement should be kept in place.

It could also choose an intermediate path. Christopher Slobogin has proposed that courts should hold that the Fourth Amendment applies to noncontent Internet information, but that law-enforcement officials can obtain it with a court order issued upon a demonstration of reasonable suspicion, rather than a warrant based upon probable cause.³³⁹ Although this compromise is appealing, courts may be reluctant to create such a novel court-order requirement. However, it could be easily implemented by statute. Congress could amend section 201(d) of the ECPA to require reasonable suspicion for noncontent court orders, rather than the laxer “relevant and material” standard currently in place.³⁴⁰

C. THEORETICAL AND OTHER IMPLICATIONS

1. Future Issues in Law and Automation

The problems of factual and legal confusion surrounding disclosure to automated systems are by no means limited to the Internet or telephone contexts. On the contrary, they are likely to arise with increasing frequency in the next few decades as new automated technologies capable of gathering information about their human users proliferate. Many of these technologies are already being tested, and a few are in the early stages of commercial use.

Implantable or wearable computer chips that link their users to databases of medical and other personal information are already in limited use.³⁴¹ These chips can constantly track a user’s location.³⁴² More sophisticated versions of these chips might allow service providers to record data about virtually every kind of activity the user engages in, from shopping to cooking to sleeping.³⁴³ Medical robots and robots developed for housework are already being tested, and in some cases, marketed. This next generation of “social robots” will record the reactions of their owners and process the collected data in order to adapt to their owners’ personalities and provide better medical care or services.³⁴⁴ Even more pervasive behavioral tracking may someday be conducted by “aware homes,” which can adapt to owners’ needs or preferences by continuously gathering

339. SLOBOGIN, *supra* note 26, at 185–86.

340. 18 U.S.C. § 2703(d).

341. See Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2060–64 (2004).

342. *Id.* at 2062–64.

343. *Id.*

344. See, e.g., Jerome Groopman, *Robots That Care*, NEW YORKER, Nov. 2, 2009, at 66, 66 (discussing the development of robotics in technological therapy).

information on their daily habits.³⁴⁵ Several prototype versions of aware homes already exist, including one in Atlanta, Georgia, that offers guided tours.³⁴⁶ The adaptive features developed for use in aware homes will likely be integrated into offices, stores, cafés, and other environments.³⁴⁷

All of these technologies are automated, and all of them collect personal information about their users, ranging from location data to information on the thousands of daily activities that occur in the privacy of the home. Their potential for surveillance of personal activities dwarfs even that of Internet technology.³⁴⁸ Yet the legal rules that apply to the information disclosed to these automated technologies will very likely be formed in cases involving the Internet. At present, these cases largely evince no recognition of any distinction between disclosure to machines and disclosure to humans, and only a tenuous grasp of how automated technologies function in practice.³⁴⁹ The most important decision, however, will be made by the Supreme Court. The first Court case addressing privacy expectations in Internet data is likely to determine not only the future of privacy on the Internet, but in an ever-increasing variety of technological contexts as well. It is beyond the scope of this Article to analyze the unique issues that each new technology is likely to raise. The importance of the central issue is nonetheless clear: The time has come to recognize the differences between human observers and automated systems in theory and in law.

2. Targeted Advertising

Like courts, legal scholars have often conflated disclosure of information to automated systems with disclosure to human employees.³⁵⁰ Conceiving of automated-data collection in human terms, in terms of “the actors controlling the servers”³⁵¹ and the “ISPs [that] can view our online activity across the Internet landscape, seeing everything we do,”³⁵² may obscure important differences in the invasiveness of various information-gathering practices. For advocates of legislation that would bar or limit

345. Brenner & Clarke, *supra* note 26, at 222; AWARE HOME RESEARCH INITIATIVE, <http://awarehome.imtc.gatech.edu/> (last visited Oct. 27, 2010); *Ambient Intelligence: Changing Lives for the Better*, PHILIPS, <http://www.research.philips.com/technologies/projects/ami/background.html> (last visited Oct. 27, 2010).

346. See, e.g., AWARE HOME RESEARCH INITIATIVE, *supra* note 345.

347. See Brenner & Clarke, *supra* note 26, at 213 n.6, 222.

348. See *id.* at 222.

349. See cases cited *supra* note 315.

350. See, e.g., Brenner & Clarke, *supra* note 26 at 212, 224; Mulligan, *supra* note 33, at 1563; Ohm, *supra* note 141, at 1438; Palfrey, *supra* note 146, at 267–69, 289–90.

351. Palfrey, *supra* note 146, at 269.

352. Ohm, *supra* note 141, at 1438.

targeted advertising,³⁵³ it will ultimately be more useful to have a clear picture of how Internet data collection works. All-or-nothing arguments about the disclosure of personal information to automated systems will likely fail, as preventing all such disclosure probably would be prohibitively costly. Both legislatures and courts are more likely to allow private entities to engage in pervasive data collection than to totally prohibit all forms of automated data collection, potentially crippling the online advertising industry and imposing large costs on politically influential corporations, including Google, Microsoft, and Comcast. A graduated approach that focuses on the riskiest forms of online data collection (such as those involving difficult-to-anonymize data³⁵⁴) is far more likely to prevail and lead to effective consumer protections. And in general, legislative proposals based on a realistic account of ISP practices are likely to be more convincing than those that always equate ISP servers with human eyes.

None of this is to say that data collection by automated systems is beneficial or without risk, or that calls for legislation banning or curtailing targeted advertising are misguided. Not only does automated data collection and the sale of collected data to third parties greatly increase the risk of government surveillance (especially if courts continue to apply the automation rationale), but it increases the risk, however small, of exposure to ISP employees or the public at large. The argument of this Article is that the disclosure of personal information to automated systems alone is not itself a violation of privacy. It does not contend that it is a benign or welfare-enhancing practice, or that Congress should not act to protect consumers from unwanted and often invisible data collection and personalized advertising.

3. Privacy Markets

Many prominent privacy scholars have studied the “privacy market,” and the ability or inability of Internet users to effectively manage, or even sell, their privacy rights as a commodity.³⁵⁵ These authors have convincingly argued that the potential for an efficient privacy market is limited. They note that there is little “privacy price discrimination” available for Internet consumers—that is, consumers generally do not have the option in the current market to pay their ISPs more in order to have enhanced privacy

353. See Louise Story, *A Push To Limit the Tracking of Web Surfers' Clicks*, N.Y. TIMES, Mar. 20, 2008, at C3.

354. Search terms are especially difficult to anonymize, and even standing alone might enable a hacker or malicious marketer to identify the user. See *supra* note 146 and accompanying text.

355. Anita L. Allen, Commentary, *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861, 870–71 (2000); Cohen, *supra* note 194, at 1391–402; James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 62–66 (2003); Schwartz, *supra* note 341, at 2076–82.

protections online.³⁵⁶ These authors have identified several possible reasons for this apparent market failure. Information asymmetries likely exist between Internet users and ISPs. As discussed in Part IV.B, most users are aware that data is collected about their web-surfing habits but are not fully aware of the extent to which their personal information is used by their ISPs, or of the contents or the relevance of ISP privacy policies.³⁵⁷ Internet users may also face a collective-action problem when it comes to Internet privacy markets. Even if some savvy and privacy-concerned consumers exist, there may not be enough of them to incentivize ISPs to offer privacy-protecting products or contract terms for an additional fee.³⁵⁸

Although these factors likely contribute to the absence of a robust privacy market, this Article's analysis suggests that the primary reason for the absence of privacy price discrimination is simply absence of demand on the part of rational consumers for privacy-protective products with any significant cost. The evidence suggests that Internet users are largely not concerned about disclosure of their private information to automated systems. At the same time, users strongly prefer to have free access to web content, and appear to be willing to allow ISPs to collect their data in largely anonymized form in exchange for the free use of Internet services.³⁵⁹ In the absence of any perceived privacy harm, and especially considering the low risk of eventual human observation or disclosure to humans of their personal information, few consumers are likely to consider the costs of disclosure to automated systems as high enough to incentivize them to pay even a small additional fee for privacy-protective services. In fact, even free protective services have failed to attract consumers.³⁶⁰

The privacy market scholars should grapple with this alternative explanation as they attempt to account for the absence of privacy price discrimination in online markets. Of course, consumers likely value the risk of eventual exposure of their private online data at some measurable level, and the studies of privacy-market failure offer convincing reasons why this consumer preference has been largely invisible in Internet markets. It may also be that ISPs should actually be paying users for the opportunity to gather their web-surfing information and sell it to advertisers. The work of the privacy market scholars may explain why users have not been able to recapture any surplus that ISPs may obtain from selling their personal information.

356. See Schwartz, *supra* note 341, at 2077.

357. See Cohen, *supra* note 194, 1396–97; Nehf, *supra* note 355, at 62; Schwartz, *supra* note 341, at 2078–80; *supra* notes 231–32 and accompanying text.

358. Cohen, *supra* note 194, at 1397; Schwartz, *supra* note 341, at 2079.

359. CTR. FOR THE DIGITAL FUTURE, *supra* note 22, at 120 (reporting that only 16% of Internet users would prefer to pay for content without ads, compared to 51% who would prefer free content supported by ads).

360. See *supra* note 241.

VI. CONCLUSION

Properly conceptualizing the disclosure of personal information to automated systems is crucial to the continued development of privacy law and privacy theory. It has the potential to clarify the scope of Fourth Amendment protection for Internet information, and indeed for all future information technologies. It can help to account for Internet users' seeming indifference to the collection of their online data and to explain the successes and failures of existing "privacy markets." It also points to serious defects in current conceptions of how to apply older bodies of law to new and evolving technologies. Finally, it exposes an overlooked flaw in *Maryland v. Smith*, the most important precedent for the application of the Fourth Amendment to new communications technologies.

The Supreme Court has not yet addressed whether any form of personal Internet data is protected by the Fourth Amendment. But, given the increasing number of lower court cases struggling with this issue in recent years,³⁶¹ the Court is likely to do so in the relatively near future. When it does face this difficult question, the answer it gives may determine the course of informational privacy for decades, just as *Olmstead v. United States* and *Katz v. United States* did in the previous century. Yet it is uncertain, at best, that the Court will answer correctly—it has certainly failed to adapt the Fourth Amendment to new technologies before.³⁶²

The Court may do as many lower courts have done and simply assume that Internet information is regularly exposed to human employees. This would be a tragic mistake, one that would deprive personal online data of effective legal protection, not on the basis of a well-reasoned balancing of law-enforcement and privacy interests, but solely due to a misunderstanding of how the Internet functions. Even if it avoids this misstep, the Court will still have to choose whether disclosure of information to automated systems alone is sufficient to eliminate any Fourth Amendment interest in Internet data. It would be easy to do as *Smith* did and simply equate these automated machines with human beings. Yet both privacy theory and empirical evidence of individuals' behaviors indicate that violations of privacy require some involvement by a human observer. This Article has proposed that the Court follow the lead of Internet users themselves and choose to treat information disclosed only to automated systems as private, as no different from personal items stored in a locker, or kept in a rented apartment. Indeed, to choose otherwise would be to expose vast quantities of personal, even intimate, online data to potential government surveillance, guarded only by an ineffective statute and ultimately protected only by the good will of the officials with the power to access it.

361. See *supra* notes 229 and 315.

362. See *supra* text accompanying notes 1–13, 90–92.