BYU Law Review

Volume 2012 | Issue 1 Article 7

3-1-2012

(Un)Reasonable Expectation of Digital Privacy

Brandon T. Crowther

(Un)Reasonable Expectation of Digital Privacy

I. INTRODUCTION

The wide availability of the Internet has put the "world at our fingertips." However, it has also put *us* at the world's fingertips. A skilled user might be able to locate a great deal of information about a person through Facebook, MySpace, blogs, news articles, or any resumes that exist on the Internet. Companies, the government, and others can use tracking cookies and other widely available software to observe a user's shopping habits and visited websites. These tools also permit third parties to obtain unique identifying information such as a user's IP address, which is a unique number assigned to a computer or router when it accesses the Internet. Every click of the mouse, site visited, and page read creates a trail of digital cookie crumbs that can be analyzed and exploited by merchants, webmasters, and the government. In addition, all of this information presents a potential goldmine for law enforcement agencies to use in investigating crimes.

Ever since Samuel Warren and Louis Brandeis published their famous article *The Right to Privacy* in 1890,[1] the right to privacy has been continually discussed, debated, and modified by the courts. The common law right to privacy in the United States has few contours and protections, particularly when compared to European countries.[2] However, the constitutional right to privacy, embodied in the Fourth Amendment's protection from unreasonable search and seizure, has developed into a genuine protection from government intrusion.[3] The preliminary inquiry into whether a government search has occurred hinges on whether a person has a "reasonable

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

2. *See* Jacqueline D. Lipton, *Mapping Online Privacy*, 104 NW. U. L. REV. 477, 484 (2010) ("[T]he European Union has some of the strongest legal privacy protections in the world. By contrast, the United States has never been particularly focused on protecting individual privacy.").

3. U.S. CONST. amend. IV; *see* Katz v. United States, 389 U.S. 347, 350–51 (1967); *see also* Berger v. New York, 388 U.S. 41, 53 (1967) ("It is now well settled that 'the Fourth Amendment's right of privacy has been declared enforceable against the States through the Due Process Clause of the Fourteenth' Amendment." (quoting Mapp v. Ohio, 367 U.S. 643, 655 (1961))).

expectation of privacy" in the object or place searched.[4] To be found sufficiently reasonable, the expectation must be both subjectively and objectively reasonable.[5]

While this test has arguably worked in the contexts in which it was originally developed,[6] applying the reasonable expectation of privacy rationale in digital contexts has weakened privacy interests and will likely continue to do so. Simply put, since "the advent of the computer age, courts have struggled to balance privacy interests against law enforcement interests."[7] The result of this has been that "[a]s technology continues to advance . . . the area in which a person has a reasonable expectation of privacy [is] decreas[ing] until there is no place to go to seek a reasonable expectation of privacy."[8] Because of the relatively recent nature of the Internet and the subsequent wealth of information available for law enforcement purposes, the courts are far from conclusively defining the limits of law enforcement's ability to conduct permissible digital "searches."

This Comment argues that the current reasonable expectation of privacy test is unable to adequately ensure that digital privacy interests are protected from warrantless intrusions. Instead, a better test is needed to reclaim some of the digital privacy interests that have already been undermined. This Comment contributes to the existing body of literature by synthesizing and expanding on existing critiques of the reasonable expectation of privacy standard as applied in the digital context,[9] uniquely examining how the standard has played out in specific digital contexts, and proposing a broad combination of existing and new solutions to move digital privacy law in the right direction.

4. *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

5. *See id.* at 361; *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 257 (S.D.N.Y. 2005) ("[T]he expectation of privacy has objective and subjective components.").

6. For example, *Katz* involved the question of whether a listening device on the outside of a telephone booth violated the criminal defendant's right to privacy. *Katz*, 389 U.S. at 348.

7. United States v. Farlow, No. CR-09-38-B-W, 2009 WL 4728690, at *5 (D. Me. Dec. 3, 2009).

8. Jenny Parker Smith, Comment, *Threatsense Technology: Sniffing Technology and the Threat to Your Fourth Amendment Rights*, 43 TEX. TECH L. REV. 615, 628 (2011) (citing Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 50 (2005)).

9. *See, e.g.*, Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211 (2006) (focusing on the specific challenges of the third party doctrine and proposing a specific solution to that problem).

Part II explores the contours of the reasonable expectation of privacy standard and its general limitations, noting in particular the inherent conflict between the objective and subjective prongs of the current test. Part III examines four factors that have led the current reasonable expectation of privacy test to undermine digital privacy. These factors are (1) the increased gap between subjective and objective expectations in digital contexts, (2) contractual arrangements with Internet service providers, (3) storage of information on third-party servers, and (4) judges' technological inexperience. Part IV demonstrates where the reasonable expectation of privacy test has fallen short by looking at digital privacy law as it relates to personal computers and "private" e-mail. Part V argues that legislatures and courts can assure that digital privacy rights are adequately protected from warrantless government intrusions by reforming the subjective prong of the reasonable expectation of privacy standard, eliminating the third party doctrine in digital contexts, and creating a broad concept of "shared privacy."

II. REASONABLE EXPECTATION OF PRIVACY STANDARD

The modern reasonable expectation of privacy standard for determining whether a Fourth Amendment "search" occurs can be traced back to Justice Harlan's concurrence in *Katz v. United States*[10] where he broadly "defined a search as a violation of a legitimate expectation of privacy."[11] Justice Harlan articulated the "twofold requirement" of the test as "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[12] The Court ultimately adopted Justice Harlan's test less than a year later in *Mancusi v. DeForte*,[13] and further clarified the test in *Smith v. Maryland* to make clear that the subjective prong means that "the individual has shown that 'he seeks to preserve [something] as private.'"[14] In subsequent cases, both of these prongs

10. 389 U.S. at 361.

11. Darren Kafka, Comment, *Propping Up the Illusion of Computer Privacy in* United States v. Burgess, 87 DENV. U. L. REV. 747, 757 (2010).

12. *Katz*, 389 U.S. at 361.

13. 392 U.S. 364, 368 (1968) (describing the test as "whether the [invaded] area was one in which there was a reasonable expectation of freedom from governmental intrusion"); Peter Winn, Katz *and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1, 7 (2009).

14. 442 U.S. 735, 740 (1979) (alteration in original) (quoting *Katz*, 389 U.S. at 351);

were further refined, but the resulting test is not without problems. The Supreme Court has acknowledged criticisms of the reasonable expectation of privacy test, and yet it has consistently upheld and applied it to further define the contours of the right to privacy.[15]

This Part outlines the contours of both the subjective and objective prongs of the reasonable expectation of privacy test, as well as the growth of the third party doctrine, which limits privacy protections for material shared with third parties. Each of these prongs has its own weaknesses, which should prompt caution when transplanting them into the modern digital context.

A. Subjective Expectation of Privacy

The subjective expectation of privacy is a very logical requirement in establishing a legitimate privacy interest. As a matter of policy, if a person does not have an actual expectation of privacy in a communication or a place, there is no reason why a right of privacy should be granted to that person. However, determining whether someone has a subjective expectation of privacy is a difficult inquiry.

Supreme Court guidance on this prong since *Katz* has been very limited because this standard is necessarily fact-intensive. The limited guidance offered by the Court is that the individual must show, by some external manifestation, that "he seeks to preserve [something] as private."[16] This clarification is basic, but it seeks to transform the subjective prong into one that can be objectively measured. For an individual to have an expectation of privacy, there must be some outward evidence that the individual, "*through his conduct* . . . sought to protect something as private."[17] For searches involving a tangible object, this inquiry "traditionally focuses on whether the subject suitcase, footlocker, or other container is physically locked."[18] With this clarification, in the majority of cases the subjective prong

see also William C. Rava, Comment, *Toward a Historical Understanding of Montana's Privacy Provision*, 61 ALB. L. REV. 1681, 1703 n.159 (1998).

15. *See* Kyllo v. United States, 533 U.S. 27, 34 (2001) ("The *Katz* test—whether the individual has an expectation of privacy that society is prepared to recognize as reasonable—has often been criticized as circular, and hence subjective and unpredictable.").

16. *Smith*, 442 U.S. at 740 (alteration in original) (internal quotation marks omitted).

17. Mary Graw Leary, *Reasonable Expectations of Privacy for Youth in a Digital Age*, 80 MISS. L.J. 1035, 1057 (2011).

18. United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007).

will not add much to the analysis and is essentially irrelevant.[19] In practice, there will be very few cases where an individual does not have a subjective expectation of privacy and yet, if she had, society would have been willing to recognize it as reasonable. More often, the converse would be true; a person would have a subjective expectation of privacy, but society would recognize that expectation as unreasonable.

Another major problem with this subjective prong is that its legitimacy relies upon accurately probing the mental state of an individual to see if she actually expects privacy. Absent a very unlikely admission by the individual that no privacy was expected, a judge is left to guess or infer a particular mental state from the person's actions. The Supreme Court established this in *Smith*, but the result is unsatisfactory as the individual still has a difficult burden to "show[] that 'he seeks to preserve [something] as private.'"[20] While there are certain clear-cut cases that lie on the extremes of this test, there is also a vast field of fact patterns in the middle that have no clear resolution. In other words, there are many situations in which it is very difficult to tell from the external manifestations of an individual whether she has a subjective expectation of privacy. Because of the difficulty of administering this prong and the little practical value it adds to the privacy inquiry, in the majority of situations it will be swallowed up by, or merged with, the second prong of the test—whether the expectation of privacy is one which society is prepared to recognize as reasonable.[21]

B. Society's Objective Expectations

Deciding what privacy expectations society is willing to accept as reasonable is also a difficult challenge. As with many reasonableness standards, courts are left to fill in the blanks with little guidance. In the forty years since *Katz*, courts have enunciated some vague guidelines to direct the objective expectation prong analysis, which unfortunately are not very useful outside of traditional privacy

19. *See* Morgan Cloud, *Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment*, 72 MISS. L.J. 5, 28 (2002) ("[T]he first prong is, for all practical purposes, functionally irrelevant.").

20. *Smith*, 442 U.S. at 740.

21. *See* Cloud, *supra* note 19, at 28. It is also interesting to note that in cases subsequent to *Katz*, Justice Harlan, the proponent of the original test, only referenced the objective component. Winn, *supra* note 13, at 11.

contexts. In 1978, the Supreme Court declared that "[l]egitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society."[22] This statement focuses on traditional privacy contexts, as it emphasizes security in a *place*. Perhaps the better articulation of this "objective" standard is that judges should look at "widely shared social expectations."[23] However, while this narrows the inquiry to what society in general expects, it gives no guidance as to how to determine what that shared expectation is.[24] And even with that standard, the Court noted that such social expectations are "naturally enough influenced by the law of property, but not controlled by its rules."[25] Tethering the reasonable expectation of privacy to the law of property may give useful guidance in some situations, particularly for conduct in the home, but it provides very little guidance for cyberspace where "place" becomes nebulous and real or personal property law may not give a clear answer to what society is willing to recognize as a reasonable expectation of privacy.

Because the Court has failed to nail down a clear objective standard to measure society's expectations, particularly within the digital context, judging what society is willing to recognize as reasonable has become a very flexible standard. This flexibility might be seen as a virtue that allows certain societal interests in security, such as airline security, to trump an individual's desire for privacy.[26] However, it is also concerning that an individual's interest in privacy hinges "on whether 'society'—i.e., some unspecified group of other individuals—approves of such protection."[27] This is even more concerning when it becomes one step removed and a judge is deciding what society is willing to recognize as reasonable.

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

23. Georgia v. Randolph, 547 U.S. 103, 129 (2006).

24. This approach to applying the Fourth Amendment was heavily criticized by the dissent in *Randolph*. The dissent pointed out that society's expectations change dramatically based on small changes in fact patterns and that "[s]uch shifting expectations are not a promising foundation on which to ground a constitutional rule." *Id*. at 130 (Roberts, J., dissenting).

25. *Id*. at 111 (majority opinion).

26. Amy L. Peikoff, *Pragmatism and Privacy*, 5 N.Y.U. J.L. & LIBERTY 638, 639 (2010).

27. *Id*. at 640. A potential solution to this problem is discussed *infra* Part V.A.

Another general problem with this prong is that it develops the law using a case-by-case approach.[28] Although this can be a virtue in some situations, in privacy law the result has been a vague standard accompanied by inconsistent applications, which hinders the underlying privacy interest.[29] The protections of privacy have been further limited because, after being created by the Warren Court (which viewed the Fourth Amendment more expansively), the reasonable expectation of privacy test was subsequently interpreted and defined by the Burger and Rehnquist Courts, which tended "to be less protective in the criminal procedure arena generally."[30] And because this test is particularly vague, it is even more subject to judicial whim than it would otherwise be. Finally, and most troubling, because judges have some insulation from the "real world," it should come as no surprise that judges may falsely declare that society is not willing to recognize an expectation of privacy as reasonable, when the exact opposite may be true.[31] This is confirmed by the latest empirical research on expectations of privacy, which suggests "that lay perceptions in fact differ from Supreme Court doctrine—at times substantially."[32]

C. Third Party Doctrine

Related to the reasonable expectation of privacy, the Court in *Katz* also elaborated the third party doctrine,[33] which states that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[34]

28. Russell L. Weaver, *The Fourth Amendment, Privacy and Advancing Technology*, 80 MISS. L.J. 1131, 1154–55 (2011); *see also* City of Ontario v. Quon, 130 S. Ct. 2619, 2628 (2010) ("[T]he question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis.").

29. *See* Weaver, *supra* note 28, at 1154–55.

30. *Id*. at 1156.

31. One commentator has pointed out that ultimately the objective prong of this test "turn[s] on the subjective views of a majority of the Justices about what privacy expectations are objectively 'reasonable.'" Cloud, *supra* note 19, at 28.

32. Jeremy A. Blumenthal, Meera Adya & Jacqueline Mogle, *The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy,"* 11 U. PA. J. CONST. L. 331, 341 (2009).

33. This doctrine has also been termed the "voluntary disclosure doctrine," "knowing exposure," or the "assumption of risk principle." Brenner, *supra* note 8, at 39; Christian M. Halliburton, *How Privacy Killed* Katz*: A Tale of Cognitive Freedom and the Property of Personhood as Fourth Amendment Norm*, 42 AKRON L. REV. 803, 842 (2009); Junichi P. Semitsu, *From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance*, 31 PACE L. REV. 291, 298 (2011).

34. Katz v. United States, 389 U.S. 347, 351 (1967); *see also* Semitsu, *supra* note 33, at

At its basic level, this doctrine "recognizes that the government does not unlawfully invade a person's privacy when it uses information a defendant disclosed in conversation with a government informant, undercover agent, or other witness, regardless of whether that conversation took place in a 'private' context."[35] The Supreme Court has further clarified that a person does not maintain a reasonable expectation of privacy in records that are held in third-party storage.[36]

In at least some instances, the third party doctrine serves as a substantial limitation on an individual's reasonable expectation of privacy. In many cases, it can completely undermine what would appear to be a private situation, as in a discussion with a close friend. The Supreme Court has said that "when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information."[37]

The third party doctrine makes the most sense in the contexts it originally derived from. In *United States v. Miller*, the government was able to obtain a customer's bank records from the bank that retained them,[38] and in *Smith v. Maryland*, the government was able to obtain from a phone company the numbers dialed from the defendant's phone.[39] In both of these cases, the defendant voluntarily and knowingly shared specific, limited information with the service provider to enable them to provide the service. The holdings of these cases "center on the fact that the information at issue was divulged as part of the regularly transacted business between the user and the third party, and was kept as a record of such transaction."[40] Even without the third party doctrine, it would be difficult to argue that the defendant had a subjective expectation

298 (explaining the effect of the "Third Party Doctrine").

35. Marc J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not a Level Playing Field*, 97 J. CRIM. L. & CRIMINOLOGY 569, 574 (2007).

36. *Id*. at 575; *see also* Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976).

37. United States v. Jacobsen, 466 U.S. 109, 117 (1984); *see also* Brenner, *supra* note 8, at 39 (elaborating on the rationale stated in *Jacobsen*).

38. *Miller*, 425 U.S. at 436.

39. *Smith*, 442 U.S. at 737.

40. Zwillinger & Genetski, *supra* note 35, at 575.

of privacy in that information, or that society would be willing to recognize that expectation as reasonable. However, as detailed below, this doctrine breaks down in digital contexts.[41]

III. DIGITAL COMPLICATIONS

Arguably, the reasonable expectation of privacy standard works in traditional Fourth Amendment settings such as searches of vehicles, homes, and instances involving customer information, where it has already been defined and applied. However, the digital age has amplified the standard's quirks and limitations in ways that Justice Harlan could not have fathomed when he announced the standard over forty years ago. As Justice Scalia put it: "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[42] This advancement of technology has created problems that challenge consistent application of the reasonable expectation of privacy standard and threaten digital privacy.[43]

Four central problems have arisen with the advent of digital technology. These are (1) the increased gap between what level of privacy individuals expect in digital information and what society (i.e. a court) is willing to recognize as reasonable, (2) terms of service agreements that undermine significant privacy interests, (3) the enormous expansion of situations that implicate the third party doctrine, and (4) a judiciary that lacks the technical expertise to effectively define digital privacy.

A. The Digital "Expectations" Chasm

With the rise of the latest digital technologies, there is an increasing gap between what a court is willing to recognize as private and what an individual subjectively expects as private, as detailed above. The basic problem is that the inner workings of the Internet and other digital technologies produce a much larger data trail than most people expect, and portions of that data trail are available to more people and companies than most would expect.[44] And because

41. *See infra* Part III.C.

42. Kyllo v. United States, 533 U.S. 27, 33–34 (2001).

43. Some proposals to address these problems are offered. *See infra* Part V.

44. *See, e.g.*, Athima Chansanchai, *Many Sharing More on Facebook Than They Know*, DIGITAL LIFE ON TODAY (Apr. 11, 2011, 12:06 PM), http://tinyurl.com/3l35tz3 (summarizing a study from Columbia University, which found that almost 94% of respondents

judges base society's expectations on the nature of the underlying technology,[45] the gap persists and increases as technology progresses. Simply put, judges use a stricter standard to measure privacy expectations than individuals do, which leads to faulty conclusions that society does not expect privacy in most digital contexts.

Web 2.0[46] has brought new challenges for the reasonable expectation of privacy standard. The increase of "voices online" and the quantity of "recording devices" has incidentally resulted in more information being gathered from users.[47] But incidentally sharing more information with various sources should not necessarily decrease the amount of privacy that users of these technologies deserve and expect. Certainly, those who post material on a public blog recognize that they are giving up privacy for that information, but should the same hold true for cell phone users whose movements are incidentally tracked as the phone locates the closest tower to facilitate service?[48] This wealth of digital information is breaking down the boundaries between public and private information, and as one commentator concluded, "any privacy laws premised on now-dated conceptions of a 'reasonable expectation of privacy' are becoming more difficult to apply."[49] What this means for

had revealed information on Facebook that they did not intend to).

45. *See, e.g.*, *Kyllo*, 533 U.S. at 33–34.

46. Web 2.0 "refers . . . to the 'participatory nature of how a website's content is created and delivered'" and encompasses modern social networks and wikis where most of the content is user-generated. Griffin v. State, 19 A.3d 415, 420 n.8 (Md. 2011) (citing Seth P. Berman, Lam D. Nguyen & Julie S. Chrzan, *Web 2.0: What's Evidence Between "Friends"?*, BOS. B. J., 5, 5 (Jan.–Feb. 2009)).

47. Lipton, *supra* note 2, at 481–82. The Internet has greatly increased the total quantity of recorded conversations as information is continually stored on various websites (particularly social network sites) and in a user's cache/cookies.

48. *See* James X. Dempsey, *Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology*, 935 PRAC. L. INST./PAT 543, 548 (2008) ("Among other things, cell phones can serve as location tracking devices. Automobiles also increasingly have geo-location features."). Recently, a German politician obtained his records from his cellphone company showing that "[i]n a six-month period, . . . [his service provider] had recorded and saved his longitude and latitude coordinates more than 35,000 times." Noam Cohen, *It's Tracking Your Every Move and You May Not Even Know*, N.Y. TIMES, Mar. 26, 2011, at A1, *available at* http://www.nytimes.com/2011/03/26/business/media/26privacy.html?_r=2. The potential problems with tracking have become even more serious as it has been revealed that Apple's iPhone intentionally tracks user movements and stores the data on the device itself. *See* Charles Arthur, *iPhone Keeps Record of Everywhere You Go*, GUARDIAN.CO.UK (Apr. 20, 2011, 2:06 PM), http://www.guardian.co.uk/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears.

49. Lipton, *supra* note 2, at 482.

users of technology is that while their subjective expectation of privacy in digitally shared information may remain strong, the fact that the information is generated and shared regularly suggests that courts are less willing to recognize such an expectation as reasonable and, consequently, that law enforcement can freely gather and use such information without obtaining a warrant.

B. Undermining Digital Privacy by Agreement

Because the objective prong of the *Katz* test is heavily fact-based, it can be dramatically changed by contract.[50] Few would argue that one should not be able to sign a contract that gives up a privacy right. In fact, this is a common occurrence in employment contracts,[51] cell-phone contracts,[52] and contracts for credit cards.[53] In each of these cases, the individual signing the contract grants the right to the other party to have access to that person's data, whether it be to search the person's work e-mail, record information about the person's phone usage, or track the person's spending. The premise behind these types of contracts does not generally offend a person's sense of fairness, because the privacy is knowingly and expressly given up, and often for the purpose of enabling the other party to better provide a desired service. However, the lines of fairness can be blurred, and in some cases dissolved, when similar contracts are "entered into" online.

Virtually every website and online service provider has a set of terms associated with the site or service. These terms are often called "End User License Agreements," "Terms and Conditions," "Terms of Service," or simply "Terms," and purport to bind the user to an agreement. These terms can come in the form of a clickwrap

50. *Cf.* City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010) ("[E]mployer policies . . . shape the reasonable expectations of their employees . . . .").

51. *See, e.g.*, United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (company policy allowed monitoring of "all file transfers, all websites visited, and all e-mail messages").

52. *See, e.g.*, VERIZON CUSTOMER AGREEMENT, http://www.verizonwireless.com (click "Customer Agreement" at bottom of site) (last visited Jan. 20, 2012) ("We collect personal information about you. We gather some information through our relationship with you, such as information about the quantity, technical configuration, type, destination and amount of your use of our telecommunications services.").

53. *See, e.g.*, TERMS AND CONDITIONS OF BANKAMERICARD VISA, http://tinyurl.com/7sc7wnb (last visited Jan. 20, 2012) ("You consent to our sharing of information about you and your account with the organization, if any, endorsing this credit card program. You authorize us to share with others, to the extent permitted by law, such information and our credit experience with you.").

agreement (clicking "I Accept" or its equivalent), a browsewrap agreement (where a notice at the bottom of the page binds the user to the terms and acceptance is presumed by continuing to use the site), and potentially even cookiewrap agreements (where acceptance of an agreement is stored in a cookie and used on subsequent visits to a site).[54] These online agreements are becoming so commonplace that it would be nearly impossible for an individual to read all of the agreements that he "accepts," and studies suggest that extremely few people ever read any.[55]

Despite being ignored by users, these forms of online contracts are gaining judicial approval, thereby undermining the traditional doctrine of assent.[56] What this means for the traditional reasonable expectation of digital privacy analysis is that an expectation that contradicts the terms of an online agreement is likely not one that a court is willing to recognize is accepted by society as reasonable, even if individuals do not realize that they are contracting away privacy rights. For example, Google's "Terms of Service" provide that "Google reserves the right (but shall have no obligation) to pre-screen, review, flag, filter, modify, refuse or remove any or all Content from any Service."[57] After "agreeing" to Google's terms of service, it is hard to argue that you have any expectation of privacy from Google, who can then freely share information with law enforcement. Facebook's terms are even more direct. Facebook's privacy policy provides that it "may share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so."[58]

As terms in these agreements become more onerous and move towards uniformly removing a person's privacy, society's expectations will naturally change. A user agreement by one online service provider may be an anomaly that does not affect what society will recognize as reasonable, but an industry standard likely will.

54. *See* Nancy S. Kim, *Clicking and Cringing*, 86 OR. L. REV. 797, 799 (2007); Max Stul Oppenheimer, *Consent Revisited*, 12 J. INTERNET L. 3, 3 (2010).

55. Kim, *supra* note 54, at 800.

56. Cheryl B. Preston & Brandon T. Crowther, *Infancy Doctrine Inquiries*, 52 SANTA CLARA L. REV. 47 (2012).

57. GOOGLE TERMS OF SERVICE 8.3, http://www.google.com/accounts/TOS (last visited Jan. 20, 2012).

58. FACEBOOK DATA USE POLICY, http://www.facebook.com/full_data_use_policy (last visited Jan. 20, 2012).

After all, who can say that they reasonably expect privacy in an area where online service providers universally disclaim that such a privacy interest exists and most users appear to agree to such terms?

C. Exponential Third-Party Growth

The third party doctrine, elaborated above, has the potential to destroy almost all digital privacy. When applied to the Internet context, the principle has very few limits. For example, under a literal application of the doctrine, any user posting material on a social networking site would lose any reasonable expectation of privacy, regardless of the user's privacy settings,[59] simply because the user knowingly exposes the content to Facebook staff, a third party to the communication.[60] In fact, virtually all online activity would fail to meet the reasonable expectation of privacy standard because most websites and online services create a record of "regularly transacted business," such as visits to the site, content shared, purchases, and other associated data.[61] As one commentator put it, "[we] have no expectation of privacy in information . . . shared with [online] entities or information they have gathered about [us]."[62] Law enforcement can thus direct the activities of these online service providers and obtain requisite information "without a warrant based on suspicion or simple curiosity."[63]

The Supreme Court has not yet decided how the third party doctrine applies in the context of the Internet,[64] but other courts have generally upheld the application of the doctrine. For example, in *United States v. Forrester*, the Ninth Circuit held that "e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to

59. Facebook allows a user to control who can see posted content by adjusting individual privacy settings that range from sharing with "Friends Only" to sharing with the public generally. FACEBOOK, http://tinyurl.com/83b9gds (last visited Jan. 20, 2012).

60. Semitsu, *supra* note 33, at 296.

61. *See* Zwillinger & Genetski, *supra* note 35, at 575.

62. Brenner, *supra* note 8, at 56–57.

63. *Id*. at 57, 61–62.

64. Nathan Petrashek, Comment, *The Fourth Amendment and the Brave New World of Online Social Networking*, 93 MARQ. L. REV. 1495, 1520 (2010) (citing Robert Ditzion, Note, *Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers*, 41 AM. CRIM. L. REV. 1321, 1334 (2004)).

and used by Internet service providers."[65] It is unclear whether courts will extend the third party doctrine to content stored on third-party servers beyond Internet identifiers shared with Internet service providers.[66] However, a literal application of the third party doctrine suggests that courts will likely extend the doctrine to such kinds of content.

D. Judicial Technological Inexperience

It is no secret that younger generations are the masters of the latest technology, and that many older judges struggle to understand the highly technical aspects of this technology.[67] With such a disadvantage, it is not impossible to reach correct results, but it is certainly more difficult.[68] How is a judge who has never used Facebook supposed to understand to what extent society is willing to recognize each type of communication made on the site as private? Or how can a judge with no technological background grasp the intricacies of an IP address that allows substantial tracking of individuals online, and at the same time gauge how much privacy society feels it is giving up by going online? Drawing distinct lines with such limited information will lead to inconsistency and a confusing standard.[69]

65. 512 F.3d 500, 503 (9th Cir. 2007); *see also* United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) ("Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation."); Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) ("We conclude that plaintiffs in these cases lack a Fourth Amendment privacy interest in their subscriber information because they communicated it to the systems operators."). *But see* State v. Reid, 914 A.2d 310, 317 (N.J. Super. Ct. App. Div. 2007) ("[D]efendant had a reasonable expectation of privacy in her ISP account information.").

66. *See* Semitsu, *supra* note 33, at 338–42. This concept is explored further in the e-mail context in Part IV.B.

67. *See* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, 545 U.S. 913, 958 (2005) (Breyer, J., concurring) (referring to "the limitations facing judges where matters of technology are concerned").

68. *See* Warshak v. United States, 532 F.3d 521, 527 (6th Cir. 2008) (en banc) ("'[T]he task of generating balanced and nuanced rules' in this area 'requires a comprehensive understanding of technological facts.'" (quoting Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 875 (2004))).

69. *See* City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.").

As a result, courts appear increasingly willing to sacrifice digital privacy to crack down on cybercrimes,[70] but they walk a dangerous road. In most cases, courts do not possess "an informed understanding of the technical facts they need to appreciate the technology they are attempting to regulate."[71] Because of this, judges must often "rely on the crutch of questionable metaphors to aid their comprehension."[72] But how much is a wireless network really like a cordless phone?[73] Or a computer like a suitcase or briefcase?[74] These metaphors may allow judges to reach some correct conclusions, but they have the potential to quickly break down and cause the law to do the same, allowing for more illegitimate government intrusions into an individual's privacy than would otherwise be warranted.[75] Where judges are more comfortable with the facts, they will naturally reason through the issues better and reach more sound conclusions. Where the reasonable expectation of privacy standard is extremely fact-intensive, judges' technological inexperience and misunderstandings threaten to further undermine digital privacy interests.

IV. SPECIFIC DIGITAL PRIVACY SHORTCOMINGS

Articles on Fourth Amendment digital privacy tend to focus on either privacy from government surveillance technology[76] or privacy

70. *See, e.g.*, *id*. (allowing a government employer to obtain transcripts of employee's text messages on a company pager); Rehberg v. Paulk, 611 F.3d 828 (11th Cir. 2010), *cert. granted*, 131 S. Ct. 1678 (2011).

71. Kerr, *supra* note 68, at 879.

72. *Id*. at 875–76.

73. *See* United States v. Ahrndt, No. 08-468-KI, 2010 WL 373994, at *3 (D. Or. Jan. 28, 2010).

74. *See* United States v. Burgess, 576 F.3d 1078, 1088 (10th Cir. 2009).

75. *See* United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999) ("[A]nalogies to closed containers or file cabinets may lead courts to 'oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage.'" (quoting Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 104 (1994))); *see also* United States v. Bach, 310 F.3d 1063, 1066–67 (8th Cir. 2002) (holding that a police officer had to be present where a search was conducted of an e-mail provider's server without realizing that police would not be any help and would not know how to prevent Fourth Amendment violations in that context); Kerr, *supra* note 68, at 878–79 (explaining that the problems caused in *Bach* were the result of a lack of technical knowledge and arguing that the majority of technically complex cases happen under similar circumstances).

76. *E.g.*, Sonia K. Katyal, *The New Surveillance*, 54 CASE W. RES. L. REV. 297 (2003); Lindsey Gil, Note, *Bad Intent or Just a Bad Day? Fourth Amendment Implications Raised by*

on social networks.[77] However, the reasonable expectation of privacy standard applies well beyond these two areas to other categories that deserve individualized analysis. Looking at the current case law discussing privacy in personal computers and personal e-mail demonstrates what Professor Kerr has previously observed: "the answer to the question of how much privacy protection the Fourth Amendment guarantees to Internet communications appears to be 'not much.' And certainly not enough."[78] The following examples demonstrate where the traditional reasonable expectation of privacy standard has failed in digital contexts and where the courts have yet to clearly define boundaries.

A. Personal Computing

The important inquiry for determining Fourth Amendment limits in the personal computing context is what an objectively reasonable expectation of privacy is for circumstances involving data stored on a personal computer. Courts have held that "as a general matter an individual has an objectively reasonable expectation of privacy in his personal computer."[79] However, this reasonable expectation "can be diminished by one's conduct with the computer."[80] For example, courts have held that file-sharing destroys a legitimate expectation of privacy in data stored on a personal computer.[81] The destruction of that privacy interest might be so thorough that "a court would uphold a federal agent's suspicionless and warrantless search of any computer folder that is accessible by a file-sharing program."[82] The relevant question then is how far the

Technological Advances in Security Screening, 16 B.U. J. SCI. & TECH. L. 231 (2010); Stephen Hoffman, Comment, *Biometrics, Retinal Scanning, and the Right to Privacy in the 21st Century*, 22 SYRACUSE SCI. & TECH. L. REP. 38 (2010); Smith, *supra* note 8, at 615.

77. *E.g.*, Patricia Sanchez Abril, *A (My)space of One's Own: On Privacy and Online Social Networks*, 6 NW. J. TECH. & INTELL. PROP. 73 (2008); Brian Kane, *Balancing Anonymity, Popularity, & Micro-Celebrity: The Crossroads of Social Networking & Privacy*, 20 ALB. L.J. SCI & TECH. 327 (2010); Semitsu, *supra* note 33; Petrashek, *supra* note 64, at 1520.

78. Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 814 (2003).

79. United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008).

80. United States v. Ahrndt, No. 08-468-KI, 2010 WL 373994, at *12–15 (D. Or. Jan. 28, 2010); *see also Ganoe*, 538 F.3d at 1127 (holding that defendant's expectation of privacy did not survive his "decision to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program").

81. *See, e.g.*, United States v. Stults, 575 F.3d 834 (8th Cir. 2009).

82. Kafka, *supra* note 11, at 757. This could potentially include the full contents of the

privacy interest in information stored on a computer extends where there is less than a file-sharing arrangement.

For example, an individual has an absolute privacy interest in a computer that is in her home,[83] password protected,[84] and not connected to any networks.[85] Beyond that, courts have recognized that "the mere act of accessing a network does not in itself extinguish privacy expectations."[86] However, once a computer accesses the Internet, its owner can expect to lose a great degree of privacy in his computer. For example, merely transmitting your information to an Internet service provider ("ISP") such as Comcast, Time Warner, or even a cellphone company, opens your information, including your IP address, to government access.[87] Furthermore, courts have deemed "Internet identifiers" to be beyond an individual's privacy interests because they are disclosed to third-party websites.[88] The troubling aspect of this line of reasoning is that many users never even know that they are disclosing these identifiers. Certainly, most users have not undertaken any intentional action to disclose these identifiers other than merely accessing these websites, which can hardly be deemed consent to sacrificing one's privacy.

Beyond individuals' passive disclosure of information on the Internet, law enforcement officers have been given great latitude to affirmatively gather information on individuals through online tools

computer's hard drive.

83. *See* United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers."); Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) ("Home owners would of course have a reasonable expectation of privacy in their homes and in their belongings—including computers—inside the home.").

84. Some courts have recognized that password protection and encryption entitle the user to a greater level of privacy protection. Kafka, *supra* note 11, at 758; *see also* United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007) (analogizing password protection to a lock on a footlocker or suitcase); Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001) (holding that consent to search a computer did not extend to co-tenant's password protected files).

85. Interestingly enough, this situation protects deleted files, although under traditional privacy law, there is no privacy interest in abandoned material. Kafka, *supra* note 11, at 757–58; *see also* United States v. Upham, 168 F.3d 532, 537 n.3 (1st Cir. 1999) ("We reject the government's suggestion that, by deleting the images, Upham 'abandoned' them and surrendered his right of privacy.").

86. United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007).

87. United States v. Perrine, 518 F.3d 1196, 1204–05 (10th Cir. 2008) (collecting cases where transmitting information to a service provider opened that information to the government).

88. White v. Baker, 696 F. Supp. 2d 1289, 1303 n.9 (N.D. Ga. 2010).

without obtaining a search warrant.[89] This has proven extremely useful where the law allows as little information as an IP address to sufficiently pinpoint the location of a user through subpoenaing an ISP.[90] These strategies have proven especially effective in tracking down and prosecuting child pornographers and other online offenders.[91] However, this extra measure of safety has come at the price of digital privacy. The closest nondigital analogy to this government action is the gathering of phone records from relevant service providers because both involve giving ongoing information to an outside company to use its service. However, the quantity of information that can be gathered digitally is much greater than what was traditionally available to law enforcement through phone records. If these differences were noted and treated as such, perhaps the courts could have crafted the law to provide greater privacy protection for activities that take place on private computers, even when users access the Internet.

B. "Private" E-mail

One of the most troubling areas where the reasonable expectation of privacy analysis falls short is the protection of personal e-mail. Courts have been clear that a company may intercept and read its employees' e-mails, particularly when authorized by a company policy.[92] This makes sense because the e-mail system is

89. *See* United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008) (using peer-to-peer software); United States v. Courtney, No. 4:07CR261 JLH, 2008 U.S. Dist. LEXIS 109344, at *5–6 (E.D. Ark. Sept. 22, 2008) (employing chat rooms, Internet searches, and social networking sites); United States v. Carter, 549 F. Supp. 2d 1257, 1259 (D. Nev. 2008) (posting links to a dummy website on a child pornography website to record the IP addresses of users).

90. *See* United States v. Stults, 575 F.3d 834, 838 (8th Cir. 2009).

91. *See, e.g.*, United States v. Haffner, No. CR-337-J-34-TEM, 2010 WL 5296920, at *2 (M.D. Fla. Aug. 31, 2010); United States v. Ahrndt, No. 08-468-KI, 2010 WL 373994, at *2 (D. Or. Jan. 28, 2010); United States v. Christie, 570 F. Supp. 2d 657, 690 (D.N.J. 2008).

92. *See, e.g.*, United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (no legitimate expectation of privacy in Internet use where company policy allows monitoring of "all file transfers, all websites visited, and all e-mail messages"); Thygeson v. U.S. Bancorp, 2004 WL 2066746, at *21 (D. Or. Sept. 15, 2004) (no reasonable expectation of privacy where company policy bans personal use of office computers and allows monitoring); Kelleher v. City of Reading, 2002 WL 1067442, at *8 (E.D. Pa. May 29, 2002) (no reasonable expectation of privacy in e-mail because of city policy); Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (no expectation of privacy in company e-mail notwithstanding assurances by management that e-mail would not be intercepted); *see also* City of Ontario v. Quon, 130 S.

provided by the company and the employees have generally consented to that as a condition of employment. But where would the government get a similar right to intercept and read e-mails without that conduct constituting a search? To best understand how e-mail should be treated under traditional privacy law, it is useful to look at its "real-world" counterpart.

The established privacy rule for standard mail is that it is entitled to Fourth Amendment protection while in the custody of the U.S. Postal Service.[93] The Fourth Amendment specifically mentions "[t]he right of the people to be secure in their persons, houses, *papers*, *and effects*,"[94] and the Supreme Court has declared that a letter is a "paper or effect" that deserves protection.[95] What this means is that, absent a warrant, the government only has access to the outward form of the mail and its weight, but not its contents.[96] However, this protection only applies where the mail is "sealed" and thus would not protect, for example, an unpackaged magazine or newspaper.[97]

E-mail is roughly analogous to regular first-class mail as even its name ("electronic mail") suggests. The primary differences are that 1) e-mail is sent through third-party Internet service providers rather than through a government entity, similar to mail sent through third-party carriers like UPS and FedEx, and 2) the message is coded into digital information for transmission and permanent storage. These differences are so small that it is difficult to argue that e-mail should have any less protection than regular mail. One commentator even makes the case that perhaps e-mail deserves *greater* Fourth Amendment protection than regular mail.[98] As mentioned above, the

Ct. 2619, 2630 (2010) ("[E]mployer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated.").

93. Ryan A. Ray, *The Warrantless Interception of E-mail: Fourth Amendment Search or Free Rein for the Police?*, 36 RUTGERS COMPUTER & TECH. L.J. 178, 200 (2010).

94. U.S. CONST. amend. IV (emphasis added).

95. Ray, *supra* note 93, at 200; *see also* Olmstead v. United States, 277 U.S. 438, 460 (1928).

96. *See Ex parte* Jackson, 96 U.S. 727, 733 (1877).

97. Ray, *supra* note 93, at 202; *see also* United States v. Van Leeuwen, 397 U.S. 249, 251 (1970) (distinguishing "first-class mail such as letters and sealed packages" from "newspapers, magazines, pamphlets, and other printed matter").

98. Ray, *supra* note 93, at 205–06. The author argues that the reasonable expectation of privacy in e-mail has been increased by the Wiretap Act, which prohibits "the interception of e-mail by law enforcement and Internet Service Provider ("ISP") employees," and by policies

to/from addresses of e-mails are not protected, just as the identity of the recipient of regular mail is not protected.[99] However, it remains unclear from the case law whether individuals have a reasonable expectation of privacy in the content of their private e-mail messages stored on third-party servers.

The earliest case suggesting that an individual might have a reasonable expectation of privacy in e-mail content was *Warshak v. United States* in 2007.[100] In *Warshak*, a panel on the Sixth Circuit upheld a preliminary injunction against government monitoring of Warshak's e-mail through his e-mail service provider.[101] The court analogized the content of e-mail to the content of telephone calls[102] and held that "individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP. The content of e-mail is something that the user 'seeks to preserve as private,' and therefore 'may be constitutionally protected.'"[103] The court had no problem upholding the privacy interest, although the e-mail provider routinely scanned the contents of messages for pornography and viruses.[104] The court also noted that if the user agreement had "call[ed] for regular auditing, inspection, or monitoring of e-mails," the expectation of privacy could have been different.[105] Ultimately, however, the Sixth Circuit's panel opinion was later vacated when the court, en banc, determined that "Warshak's constitutional claim [was] not ripe for judicial resolution."[106] The Sixth Circuit did, however, reaffirm that an individual's expectation of privacy in e-mail content "shifts from internet-service agreement to internet-service agreement."[107] This is particularly troublesome today where major e-mail providers undermine privacy through their usually unread terms of service.[108]

The latest major case on privacy in e-mail content, *Rehberg v. Paulk*, suggests the opposite result from *Warshak* but is no more

created by ISPs that treat customer e-mail as confidential. *Id.* at 205.

99. United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007).

100. 490 F.3d 455 (6th Cir. 2007), *vacated*, 532 F.3d 521 (6th Cir. 2008) (en banc).

101. *Id.* at 482.

102. *Id.* at 469–70.

103. *Id.* at 473 (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

104. *Id.* at 474.

105. *Id.* at 473.

106. Warshak v. United States, 532 F.3d 521, 523 (6th Cir. 2008) (en banc).

107. *Id.* at 526–27.

108. *See, e.g.*, GOOGLE TERMS OF SERVICE, *supra* note 57, at 8.3.

conclusive.[109] In *Rehberg*, the Eleventh Circuit was presented with the issue of whether a chief investigator violated the Fourth Amendment when he subpoenaed an Internet service provider to obtain Rehberg's personal e-mails.[110] When reviewing cases from other circuits, the court found that "[s]ome circuit decisions suggest in dicta that a person loses a legitimate expectation of privacy in e-mails sent to and received by a third-party recipient."[111] However, instead of deciding the case on Fourth Amendment grounds, the court "resolve[d] this case narrowly" by holding that "at a minimum Rehberg ha[d] not shown his alleged constitutional right was clearly established."[112] The ultimate result of this holding was that Rehberg's constitutional claim was denied, suggesting that the court would have decided against the right to privacy in Rehberg's e-mail content if it had decided the issue. The Supreme Court recently granted certiorari to hear the case and will hopefully provide more guidance on this issue.[113]

Ultimately, determining whether a privacy interest exists in e-mail may depend on security measures that the individual seeks to employ, such as encrypting messages,[114] and on the degree of privacy provided by the terms of service agreement between the customer and the e-mail service provider. However, focusing on these two factors could leave e-mail content open to warrantless government searches in the majority of instances because personal encryption is not regularly used and terms of service tend to undermine digital privacy. As a result, privacy expectations that both society and individuals are likely willing to accept as reasonable are instead subject to unbridled government intrusion. Ultimately, this weakens the protection of Fourth Amendment rights that are guaranteed by the Constitution and ought to be preserved.

V. PROPOSALS FOR CHANGE

The reasonable expectation of privacy standard is flawed, as detailed above, and provides inadequate protection for individual

109. 611 F.3d 828 (11th Cir. 2010), *cert. granted*, 131 S. Ct. 1678 (2011).

110. *Id*. at 843.

111. *Id*. The Eleventh Circuit seemed to be focusing on the assumption of risk that the recipient would disclose the content, and then analogized that to third party ISPs.

112. *Id*. at 846.

113. *Rehberg*, 131 S. Ct. at 1678.

114. This could be analogous to "sealing" first class mail.

privacy. The digital age has further exposed the limitations of this standard as judges have applied the fact-intensive standard to decrease individuals' privacy based on the nature of new technologies, rather than on society's actual expectations.[115] To prevent further weakening of privacy interests, it is important that legislatures and courts act to change the current reasonable expectation of privacy standard so that it more coherently fits into the digital context. This Part details potential solutions to this critical problem.

A. Giving Society's Expectations Back to Society

One simple change that could address some of the problems in modern digital privacy law is to reform how the *Katz* test itself is applied. Practical application of the objective prong by courts denies to individuals Fourth Amendment protection even if a vast majority of people in society expect privacy in an identical situation. Instead of focusing on what a judge recognizes as society's expectation of privacy,[116] which is mostly decided on the basis of the nature of the technology instead of shared expectations, society's broad interests in privacy would be better served if the test accounted for what society *actually* expects in matters of privacy. To do this, courts should take an empirical approach, rather than a purely subjective one, when determining societal expectations on privacy issues. This would help overcome the problem that currently exists where judicial views on privacy matters "trickle[] down to the general population where it eventually becomes reasonable, regardless of whether it actually was reasonable to begin with."[117]

One commentator attempted to measure public expectations of privacy when he gathered data on how intrusive the public felt various forms of public surveillance were.[118] A small group of people

115. *See supra* Part II.B.

116. The Supreme Court seemed to acknowledge that society's expectations are defined by judges when Justice Kennedy wrote that "[i]n *Katz*, the Court *relied on its own knowledge and experience* to conclude that there is a reasonable expectation of privacy in a telephone booth." City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010) (emphasis added).

117. R. Bruce Wells, Comment, *The Fog of Cloud Computing: Fourth Amendment Issues Raised by the Blurring of Online and Offline Content*, 12 U. PA. J. CONST. L. 223, 237–38 (2009) (citing Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 106–07 (2008)).

118. Orin S. Kerr, *Do We Need a New Fourth Amendment?*, 107 MICH. L. REV. 951, 954 (2009) (reviewing CHRISTOPHER SLOGOBIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2007)).

summoned for jury duty in Florida was asked to rank various forms of surveillance on a scale of 1-100, after which the results were compiled and compared.[119] The results showed a range of the public's expectation in privacy from the minimal intrusiveness of "[l]ooking in foliage in the park" to the maximum intrusiveness of "[s]earching a bedroom."[120] Although the study was not conducted widely and focused only on certain forms of surveillance, it shows the feasibility of statistically measuring what privacy interests the public is willing to recognize as reasonable. A similar approach could be used in criminal cases to determine what society actually believes is reasonable, particularly with regards to digital privacy issues where a judge may not be in a position to fully understand the technology and gauge the mindsets of those who use it.[121]

Admittedly, taking an empirical approach in every case presents a potential problem of cost for the parties litigating the issue. However, using empirical evidence does not suggest that the parties will need to conduct unique statistical studies in each situation, which may not be reliable anyway as the parties bring their biases into the analysis. Rather, if courts were to show their willingness to engage in empirical inquiries, it is probable that independent studies would be conducted on the nature of privacy interests. Such research could form the basis for expert testimony that would serve the same purpose as conducting unique studies for each case, would be more neutral, and would more accurately reflect public notions of privacy.

This proposed modification in applying the test would improve the *Katz* formula by changing the second prong to more accurately reflect society's expectations. Admittedly, it is not completely immune from some of the same problems as the current test, but it fares significantly better. Determination of society's views would still be somewhat subject to judges' individual views on privacy. Although a judge would hear evidence on what society expects and is willing to recognize as reasonable, ultimately, the nuances and gaps in the rule will be filled in case-by-case with what individual judges think is reasonable. However, requiring judges to consider empirical

119. *Id.*

120. *Id.*

121. It is interesting to note that on the "Transactional Surveillance" survey, investigating "Web sites visited" ranked high on the list for intrusiveness (18/25), just behind "Search of car" and "E-mail addresses sent to and received from," the latter of which ranked even higher (21/25). *Id.* at 956.

evidence or expert testimony concerning society's actual expectations would narrow judicial discretion and help judges more accurately gauge society's views.

B. Limiting the Third Party Doctrine

The third party doctrine was established prior to the digital age, and its advocates could not have fully contemplated society's heavy reliance on digitally stored information.[122] With so much personal information at risk, perhaps it is time to put an end to the third party doctrine, or at least limit its application to the more traditional privacy contexts it was designed for. With the wealth of digital information in the hands of third parties, digital privacy is almost completely undermined by the third party doctrine. That doctrine has become "increasingly archaic and problematic" as the third party is increasingly "a seemingly anonymous and automated online media service provider."[123] Eliminating this doctrine would prevent the loss of any and all privacy protection in the digital context, and allow the reasonable expectation of privacy inquiry to be more fully carried out.

One scholar has optimistically pointed out that trends in the past decade suggest that the third party doctrine is already in decline and will continue until extinction.[124] Hopefully, this trend will continue for the sake of digital privacy. The third party doctrine has already significantly undermined digital privacy by allowing the government to collect service providers' records without a warrant, and if the doctrine is not limited, the problem will only become worse as technology advances.[125] By putting the vast majority of our digital privacy in the hands of service providers, we are unintentionally giving up privacy in many areas of our lives that should remain private. Requiring such a sacrifice of privacy just to access the benefits of modern technology is nonsensical, and the third party doctrine should be limited to avoid this result.

---

122. *See* Andrew William Bagley, *Don't Be Evil: The Fourth Amendment in the Age of Google, National Security, and Digital Papers and Effects*, 21 ALB. L.J. SCI. & TECH. 153, 174 (2011). Cloud computing involves storing data and running programs using an outside computer such as a third-party server.

123. *Id*. at 173–74.

124. Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 39–40 (2011).

125. *See* Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV. 1381, 1401–03 (2008).

C. Shared Privacy

As a counterpart to limiting the third party doctrine, courts and legislatures could approach the problem from the other end and *create* an intermediate level of privacy between public and private, a sort of "shared privacy" concept. Rather than having "private" refer only to an individual and "public" refer to everything else, the law could recognize that some information and content is shared with the expectation that it will be maintained in privacy by the other users privy to the communication. The law has formally recognized that this is possible by protecting attorney-client confidences and corporate trade secrets. While the interests in information disclosed online may not deserve such nearly absolute protections, recognizing that there may still be some expectation of privacy in shared communications is more consistent with how people actually interact with each other.

This shared privacy concept would have the benefit of protecting against warrantless government searches of subscriber information provided to Internet service providers, e-mail stored on third-party servers, and content provided to Internet service providers with the subjective expectation that it will remain private among the parties involved. This rule could still be tempered by the two prongs of the *Katz* test and the contractual expectations in the terms provided by Internet service providers. Should Internet service providers not desire to protect users' privacy for whatever reason, they could still make it known in their user agreements, provided that they actually draw attention to those terms to assure knowing assent.

To a very limited extent, this concept of "shared privacy" already exists. The Fourth Amendment implicitly recognizes that there is an intermediate level of privacy with certain relationships such as those between family members or between owners and houseguests.[126] Such shared privacy has even been allowed to be "portable," allowing "transmission from one private enclave . . . to another."[127] However, to be useful to digital privacy, this concept would have to be expanded to include Internet service providers, although there is a lesser degree of trust given to the third party than with family or house guests, and that trust is based on contract rather than close association.

126. Brenner, *supra* note 8, at 73.

127. *Id.* (citing Katz v. United States, 389 U.S. 347, 352 (1967)).

One drawback to creating this intermediate level of privacy is that it could potentially apply to well-settled forms of communication that are not protected by the Fourth Amendment, such as phone records or regular mail communications, as discussed above. Privacy law could be expanded to further protect traditional forms of communication, if desired, but otherwise, the rules and regulations regarding this "shared privacy" would need to be carefully crafted to apply only to digital communications. Or perhaps it could simply be limited to protect information shared with a company that is *critical* to enabling that company to provide service. This would still have application outside of cyberspace, but would narrow the protection to only critically shared information, such as contact information or location data from cell phone companies. Even then, this information would still be available to law enforcement, but only with a warrant supported by probable cause.[128]

Ultimately, expanding the concept of "shared privacy" and explicitly recognizing its application to the Fourth Amendment would enhance the privacy and trust between individuals and those with whom they conduct business.[129] This solution is relatively simple and would help restore the lost sense of digital privacy.

VI. CONCLUSION

The Fourth Amendment seeks to protect the privacy of individuals by preventing unreasonable searches and seizures by the government, but that interest is not currently served in the digital context by the reasonable expectation of privacy standard. The problems associated with both the subjective and objective prongs of the test, along with the third party doctrine, are continually undermining the privacy of individuals in the digital context. New digital technologies have challenged what judges are willing to recognize as reasonable, and unfortunately courts have not responded favorably. Courts have limited privacy rights in matters involving personal computers and have potentially dissolved any privacy rights in matters involving e-mail through commercial services. With the growth of technology, these privacy interests are likely to be threatened further unless something is changed.

128. *Id.* at 80.

129. *See id.*

Legislatures and courts have the ability to correct the current problems with the reasonable expectation of privacy standard by using empirical evidence to measure what society is willing to recognize as reasonable, eliminating or substantially narrowing the third party doctrine, and creating an intermediate category of privacy ("shared privacy") that recognizes the realities of sharing information in a digital world. Changing the current standard has the potential to maintain levels of privacy amidst technological progress and restore some protections that have been lost through the current reasonable expectation of privacy formula.

Brandon T. Crowther[*]

* J.D. candidate, April 2012, J. Reuben Clark Law School, Brigham Young University.