TEMPLE LAW REVIEW

VOL. 84 NO. 3 **SPRING 2012**

ARTICLES

LOW EXPECTATIONS: HOW CHANGING EXPECTATIONS OF PRIVACY CAN ERODE FOURTH AMENDMENT PROTECTION AND A PROPOSED SOLUTION

Teri Dobbins Baxter[*]

Technology has changed the lives of every American, but it has revolutionized the way that young people socialize and become socialized. Youths' increasing use of technology to interact with their peers and shape their identities has led to a change in the way personal information is shared and the privacy expectations that are held with respect to that information. Various studies have found that, in general, younger generations have lower privacy expectations than their older counterparts. This Article considers how these changing attitudes towards privacy among youth have the potential to erode Fourth Amendment protection for everyone. The Article then proposes modest changes to the current test for Fourth Amendment protection that take into consideration the changes in society brought about by rapidly developing technology. Specifically, the Article proposes a test that asks: (1) whether a person has taken steps to reasonably limit access to the information or place targeted for search or seizure; and (2) if so, whether society is prepared to protect the information or space from government intrusion.

I. INTRODUCTION

Technology has changed the way people live their lives. Many of these changes are for the better: advances in medical technology have saved lives; technology has led to safer cars, faster and more powerful computers, and the ability to communicate with others around the world instantly and relatively cheaply. But technology has also

[*] Professor of Law, Saint Louis University School of Law; J.D., Duke University 1997; B.A., Duke University 1993. The Author thanks Melissa Haberer and Lynn Harke for their invaluable research assistance and Saint Louis University School of Law for the research grant that made this Article possible.

brought about significant cultural shifts. One prominent example is the way that people, particularly young people, socialize and become socialized.

Youth may spend almost as much time interacting with their peers and others via technological devices as they spend in face-to-face interactions. This has led to a change in the way personal information is shared and the privacy expectations that are held with respect to that information. In general, younger generations have lower privacy expectations than their older counterparts. This Article considers how changing attitudes towards privacy have the potential to erode Fourth Amendment protection for everyone. The Article then proposes changes to the current test for Fourth Amendment protection that take into consideration the changes in society brought about by rapidly developing technology.

The current test for Fourth Amendment protection against unreasonable search or seizure asks whether there is a subjective expectation of privacy that society is prepared to accept as reasonable.[1] After a brief discussion in Part II of the development of the Fourth Amendment to its current state, Part III of this Article explores the varying subjective expectations of privacy among different age groups. It discusses expectations of youth and how those expectations may differ markedly from the expectations of more senior Americans.

Part III also examines how the younger generation may impact Fourth Amendment jurisprudence in the future. Fourth Amendment litigation involving new technologies and new uses of existing technology has already begun, and courts are defining privacy rights in these arenas, often cautiously—even reluctantly—and sometimes inconsistently. It is undisputed that technology is advancing at an extraordinary pace; and younger generations are leading the way in embracing and utilizing these technologies. Moreover, youth are driving and influencing what and how technology develops and how it is used, since they are the biggest market for such technology. As a result, youth are in a position to affect the development of privacy law in a way that is unprecedented.

Part IV then considers how differing expectations of privacy could lead to different levels of protection for people in varying age groups. In a Fourth Amendment case, the courts could find the subjective part of the test satisfied for some individuals, particularly older individuals, and not for others. Thus, older litigants could be afforded greater protection than their younger counterparts in the same circumstances. Alternatively, in the near term, Fourth Amendment jurisprudence could be skewed to reflect the expectations of older Americans while evolving over time to reflect younger perceptions, resulting in less protection.

Part V focuses on the objective component of the current Fourth Amendment test. When courts ask whether a person's expectation of privacy is one that society is prepared to accept as reasonable, which segments of society's expectations are considered? Given that judges—particularly Supreme Court Justices—tend to be older, one could assume that their own expectations will prevail or will at least be given a great deal of weight. This Article examines recent cases to assess the accuracy of that

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

assumption. Part V also questions whether courts should favor those who want greater protection in cases in which the expectations of various groups are inconsistent.

Next, Part VI identifies legislative responses to technology and its effect on privacy rights. Both federal and state statutes limit the government and private parties' ability to use technology to gain access to private information. This Part further discusses the limits to the effectiveness of legislation as a means of protecting privacy.

Finally, Part VII proposes a new test—which is simply a variant of the current test—for Fourth Amendment protection that does not include an absolute subjective expectation of privacy. This proposed test narrows the objective inquiry to focus on whether society is willing to protect the information or place from government intrusion, as opposed to whether society is willing to recognize a more general expectation of privacy. This new test would acknowledge the reality that absolute privacy is almost impossible to maintain in today's society, and would not require people to choose between fully participating in society, particularly areas involving technology, or protecting themselves from government searches or seizures.

II. FOURTH AMENDMENT APPLICATION: PAST AND PRESENT

The Fourth Amendment to the United States Constitution states: "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[2] The test adopted by the Supreme Court for Fourth Amendment protection has both a subjective and an objective component.[3] The first part of the test asks whether the target of the search or seizure has a subjective expectation of privacy in the object, area, or information to be searched or seized.[4] If a subjective expectation of privacy is found, the court then asks whether society is prepared to recognize that expectation as reasonable.[5] This has been characterized as an objective inquiry.[6]

This test has been used for the last forty years to decide Fourth Amendment cases.[7] In that time, courts have had the sometimes difficult task of applying the test in the context of new and developing technologies. The foundation for more recent cases was laid in cases addressing more familiar technology, such as the telephone. In *Smith v. Maryland*,[8] the Court considered whether a pen register attached to a suspect's home telephone at the government's request and without a warrant was an unreasonable search in violation of the Fourth Amendment.[9] The Court held that there was no Fourth Amendment violation because the pen register was not a search; there was no search

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

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

4. *Id.*

5. *Id.*

6. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 740 (1979) (citing *Katz*, 389 U.S. at 353).

7. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 33 (2001); California v. Ciraolo, 476 U.S. 207, 211 (1986); *Smith*, 442 U.S. at 740; Terry v. Ohio, 392 U.S. 1, 9 (1968).

8. 442 U.S. 735 (1979).

9. *Smith*, 442 U.S. at 736–38.

because telephone users have no legitimate expectation of privacy in the numbers that they dial, even from their home telephone.[10]

The Court reasoned that telephone users know that the telephone company has access to and can record the numbers that they dial for legitimate business purposes.[11] "Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret."[12] Without an objectively reasonable subjective expectation of privacy, the pen register could not violate the Fourth Amendment.[13] Moreover, even if the user could prove a subjective expectation of privacy, it would not be objectively reasonable since the user must voluntarily disclose the dialing information to the telephone company in order to complete the call.[14] "This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[15] The Court's conclusion in *Smith* relied heavily on the assumption that telephone users understand how the telephone service works and that the telephone company has access to dialing information.[16] Technology has advanced rapidly and tremendously since *Smith* was decided and the Court has had to address circumstances in which the mechanics of the technology at issue are not as well known to, or as easily understood by, the general population.

In *Kyllo v. United States*,[17] the defendant challenged a search of his home by government officers using thermal imaging technology.[18] In that case, an agent of the Department of the Interior suspected that the petitioner was growing marijuana in his home.[19] In order to confirm his suspicions, the agent used a thermal imaging device to detect whether the petitioner's home was producing more heat than would be expected, or more than surrounding homes, to support his theory that the petitioner was using heat lamps to grow the marijuana indoors.[20] The readings were taken from the streets in front of and behind the petitioner's home and showed higher than normal heat radiating from the structure.[21] Based upon this and other evidence, a search warrant was issued for petitioner's home and evidence of marijuana growing was collected.[22] The petitioner challenged the validity of the warrant, complaining that the thermal imaging constituted a warrantless search in violation of the Fourth Amendment.[23] The district court rejected the petitioner's claim, finding that the imaging did not show any people

10. *Id.* at 742–44.
11. *Id.*
12. *Id.* at 743 (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).
13. *Id.*
14. *Id.* at 743–44.
15. *Id.*
16. *Id.* at 742–44.
17. 533 U.S. 27 (2001).
18. *Kyllo*, 533 U.S. at 29–30.
19. *Id.* at 29.
20. *Id.* at 29–30.
21. *Id.* at 30.
22. *Id.*
23. *See id.* at 30.

or activities in the home, did not capture any conversations or intimate details of the home, and showed only crude visual heat images.[24] Based on its findings, the district court upheld the warrant and denied the motion to suppress.[25] The court of appeals affirmed.[26]

The Supreme Court granted certiorari.[27] The Court began its discussion with recognition that warrantless searches of homes have been held, with few exceptions, to violate the Fourth Amendment.[28] As technology has developed, however, the Court had several opportunities to address when a search has taken place for Fourth Amendment purposes:[29]

> As Justice Harlan's oft-quoted concurrence described it, a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable. We have subsequently applied this principle to hold that a Fourth Amendment search does *not* occur—even when the explicitly protected location of a *house* is concerned—unless "the individual manifested a subjective expectation of privacy in the object of the challenged search," and "society [is] willing to recognize that expectation as reasonable."[30]

Applying this test, the Court held that no search occurred in *Smith v. Maryland*, even though the pen register recorded numbers dialed from the suspect's home,[31] and later held that aerial surveillance of a home and its surrounding property did not constitute a search even though technology (flight) allowed government officials to view what had previously been private.[32]

Kyllo presented the Court with a slightly different set of circumstances because the officers did not merely observe the petitioner's home with their naked eyes. Instead, sense-enhancing technology allowed the officers to observe what would not have been apparent without the technology.[33] The Court made note that

> [i]t 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. . . . The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.[34]

24. *Id.*

25. *Id.*

26. *Id.* at 30–31. A divided court initially reversed but later withdrew its opinion and affirmed. *Id.*

27. *Id.* at 31.

28. *Id.* at 31.

29. *See id.* at 33 (citing California v. Ciraolo, 476 U.S. 207, 213–14 (1986); Smith v. Maryland, 442 U.S. 735, 743–44 (1979)) (discussing cases in which the Court determined that the aerial surveillance of one's home and surrounding area was not a search, nor was the use of a pen register to obtain the numbers dialed from one's home).

30. *Id.* at 33 (alteration in original) (quoting *Ciraolo*, 476 U.S. at 211).

31. *Smith*, 442 U.S. at 741, 743–44. See *supra* notes 8–16 and accompanying text for a more in-depth discussion of *Smith*.

32. *Ciraolo*, 476 U.S. at 209, 213–14.

33. *Kyllo*, 533 U.S. at 29–30.

34. *Id.* at 33–34.

The Court noted that although the *Katz* test may be difficult to apply in some circumstances,[35] ample precedent exists for finding that a subjective and reasonable expectation of privacy exists inside of homes.[36] The Court held that the warrantless use of thermal imaging to gather information about activities inside of the home constituted an unreasonable search.[37] "Where . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[38] The language of the opinion implies that if a device *is* in general public use, the Court may not find that a search has occurred (or, alternatively, that the search was reasonable). Given the rapid pace of technological development and the degree to which technology formerly available only to governments and universities is now available to the general public, the protection formerly provided by the Court in *Kyllo* may be significantly eroded today.

After *Kyllo*, the Court's attention moved from government surveillance of physical spaces to computer searches. In 1986 the Court addressed the Fourth Amendment's application to searches of the work computers of government employees.[39] The Court confirmed that government employees have a reasonable expectation of privacy in their workplace,[40] but went on to note that the expectation of privacy may be diminished in shared spaces or in light of the legitimate need for access by coworkers or supervisors.[41] Consequently, whether a reasonable expectation of privacy exists in a particular circumstance must be determined on a case-by-case basis.[42]

Having concluded that a reasonable expectation of privacy exists, the Court then had to determine whether a search of an employee's private area is reasonable.[43] In order to answer that question, the Court was first tasked with determining the appropriate standard of reasonableness to be applied to searches of government workplaces.[44]

> [W]e conclude that the 'special needs, beyond the normal need for law enforcement make the . . . probable-cause requirement impracticable . . . . We hold, therefore, that public employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related

35. *See id.* at 34 (citing criticisms of the *Katz* test as circular and unpredictable, particularly as applied to surveillance of phone booths, automobiles, or the area surrounding residences).

36. *Id.*

37. *Id.* at 40.

38. *Id.*

39. O'Connor v. Ortega, 480 U.S. 709 (1987).

40. *Id.* at 717.

41. *Id.* at 717–18.

42. *Id.* at 718.

43. *Id.* at 719.

44. *Id.*

> misconduct, should be judged by the standard of reasonableness under all the circumstances.[45]

Under this test, a court must first determine that the search was reasonable at the inception, and, second, that the scope of the actual search was reasonable.[46]

This test was applied to a search of a public university employee's computer in *Biby v. Board of Regents*.[47] In that case, the employee claimed that he had a reasonable expectation of privacy in the files on his work computer and that a search of the computer by university employees violated his rights under the Fourth Amendment.[48] The Eighth Circuit Court of Appeals affirmed summary judgment in favor of the university, finding that the employee had not established a reasonable expectation of privacy in his computer files. This finding was based, in part, on a university computer policy which allowed for searches of university computers in response to a discovery request in litigation.[49]

The courts of appeals have also begun to address the application of the Fourth Amendment to electronic communications such as email. In *United States v. Warshak*,[50] the Sixth Circuit held that people usually have a subjective expectation of privacy in the content of their emails that society is prepared to accept as reasonable.[51] The court began its Fourth Amendment analysis by noting the protection granted to "traditional forms of communication," such as letters and telephone calls.[52] Courts have found a reasonable expectation of privacy in the content of those communications notwithstanding the fact that intermediaries such as mail carriers and the telephone company have the ability (and sometimes the right) to intercept such communications.[53] In *Katz*, the Court held that telephone conversations are protected by the Fourth Amendment because callers were "surely entitled to assume that the words [they] utter[ed] into the mouthpiece w[ould] not be broadcast to the world."[54] Similarly, with respect to letters, the Sixth Circuit stated "trusting a letter to an intermediary does not necessarily defeat a reasonable expectation that the letter will remain private."[55]

The Sixth Circuit noted that email has assumed a "prominent role" in modern communication.[56]

> Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken

45. *Id.* at 725–26 (omission in original) (quoting New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring)).

46. *Id.* at 726 (citing *T.L.O.*, 469 U.S. at 341; Terry v. Ohio, 392 U.S. 1, 20 (1967)).

47. 419 F.3d 845, 850–51 (8th Cir. 2005).

48. *Biby*, 419 F.3d at 850.

49. *Id.* at 850–51.

50. 631 F.3d 266 (6th Cir. 2010).

51. *Warshak*, 631 F.3d at 288.

52. *Id.* at 285.

53. *Id.*

54. *Id.* (second and third alterations in original) (quoting Katz v. United States, 389 U.S. 347, 352 (1967)).

55. *Id.*

56. *Id.* at 284.

> place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button. Commerce has also taken hold in email. . . . In short, "account" is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life.[57]

Finding strong similarities between email and traditional forms of communication, and in light of the role email plays in today's society, the court held that "common sense" dictated providing equal Fourth Amendment protection to email.[58] Consequently, government officials seeking access to email must comply with the warrant requirement unless some recognized exception applies.[59] "As some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise."[60]

The Ninth Circuit reached similar conclusions in *United States v. Forrester*.[61] In that case, the government conducted warrantless computer surveillance that allowed it to discover "the to/from addresses of [the defendant's] e-mail messages, the IP addresses of the websites that [the defendant] visited and the total volume of information sent to or from [the defendant's] account."[62] The defendant claimed that the surveillance violated his Fourth Amendment rights.[63] The Ninth Circuit disagreed, reasoning that the surveillance conducted by the government was "constitutionally indistinguishable" from the pen register that was approved by the Supreme Court in *Smith v. Maryland*.[64] Similar to telephone numbers that are provided to the phone company in order to facilitate the call, email addresses are voluntarily provided to the email service provider to enable the messages to be routed to the intended recipient.[65] Likewise, the court found email addresses identical to addresses on physical mail for constitutional purposes; both may be "searched" without a warrant.[66]

Although the court found no reasonable expectation of privacy in the address information, it distinguished addresses from the content of the email.[67]

> E-mail, like physical mail, has an outside address "visible" to the third-party carriers that transmit it to its intended location, and also a package of content that the sender presumes will be read only by the intended recipient. The

57. *Id.*

58. *Id.* at 285–86.

59. *Id.* at 286.

60. *Id*. But note that courts have held that government surveillance of IP addresses visited, "to/from addresses" on emails, and the "total volume of information sent to or from" an email account does not violate the Fourth Amendment. *E.g.*, United States v. Forrester, 512 F.3d 500, 509 n.4, 511 (9th Cir. 2008).

61. 512 F.3d 500 (9th Cir. 2008).

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

63. *Id.* at 509.

64. *Id.* at 510 (citing Smith v. Maryland, 442 U.S. 735, 742, 744 (1979)).

65. *Id*. (citing *Smith*, 442 U.S. at 742).

66. *Id*. at 511 (noting that cases dating back to the nineteenth century have held that the government may not conduct warrantless searches of the contents of mail but may observe information printed on the outside of letters or packages).

67. *Id*.

> privacy interests in these two forms of communication are identical. The contents may deserve Fourth Amendment protection, but the address and size of the package do not.[68]

Whereas lower courts have tackled Fourth Amendment issues related to technology, the United States Supreme Court does not seem as comfortable with these issues as some of the courts of appeals. The Supreme Court had an opportunity to address the issue of privacy in text messages sent using government-issued electronic devices in *City of Ontario v. Quon*.[69] In that case, a police officer claimed that his employer, the police department, violated his Fourth Amendment rights by obtaining and reading transcripts of text messages he sent and received using the wireless pager issued to him by the police department.[70] The department's computer usage policy stated that "[u]sers should have no expectation of privacy or confidentiality when using these resources."[71] However, a supervisor told Officer Quon that he would not audit the messages if Quon paid for any usage that exceeded the monthly allotment.[72]

The district court and the Ninth Circuit Court of Appeals both found that the officer had a reasonable expectation of privacy in the text messages in spite of the computer policy,[73] presumably finding that the statements and subsequent actions of the supervisor overrode the written policy.[74] The district court nevertheless held that the search of the text messages was reasonable and therefore did not violate the Fourth Amendment.[75] The court of appeals reversed that ruling, and held that the search was unreasonable in scope.[76]

In deciding the case, the Supreme Court acknowledged that the case "touche[d] issues of farreaching significance," but determined that the Fourth Amendment question could be resolved without deciding whether the officer had a reasonable expectation of privacy in the text messages.[77] When addressing privacy expectations in this context, the Court counseled restraint:

> The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. In *Katz*, the Court relied on its own knowledge and experience to conclude that there is a reasonable expectation of privacy in a telephone booth. It is not so clear that courts at present are on so sure a ground. Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the

68. *Id.*
69. 130 S. Ct. 2619 (2010).
70. *Quon*, 130 S. Ct. at 2625–26.
71. *Id.* at 2625.
72. *Id.*
73. *Id.* at 2626–27.
74. *See id.* at 2629.
75. *Id.* at 2626–27.
76. *Id.* at 2627 (citing Quon v. Arch Wireless Operating Co., 529 F.3d 892, 908 (9th Cir. 2008)).
77. *See id.* at 2624.

> existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices.
>
> . . . .
>
> A broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted. It is preferable to dispose of this case on narrower grounds.[78]

The Court not only appeared concerned about the continued evolution of technology and its impact on privacy expectations, it also seemed skeptical about the judiciary's understanding of such technology. Unlike the telephone booth, with which the *Katz* Justices were familiar, emerging technology may be beyond the experience and understanding of members of the judiciary.[79] Lacking a firm understanding, courts might not feel confident deciding what expectations are reasonable, at least not without input from other sources. The Court's admitted discomfort opens the door to discussions of the varying and shifting expectations of privacy among different segments of society.

III. SUBJECTIVE EXPECTATIONS

Much research has been done examining how people of various ages view privacy. Some concerns exist across generations. For instance, both older and younger users may not sufficiently understand how the technology works to realize the privacy implications of using the technology.[80] Privacy controls are not always transparent; it may not be clear what information is private and what is publicly available.[81] For

78. *Id.* at 2629–30 (citations omitted).

79. For instance, Chief Justice Roberts asked at oral argument: "Maybe—maybe everybody else knows this, but what is the difference between a pager and e-mail?" Transcript of Oral Argument at 29:18–20, City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (No. 08-1332). *See also id.* at 44:16–18 (Justice Kennedy, in trying to determine what happens when a person receives a text message while simultaneously receiving one from another device, wondering if there would be "a voice mail saying that your call is very important to us; we'll get back to you"); *id.* at 49:20–22 (Justice Scalia inquiring if one could print out text messages received on a mobile device).

80. *See* Patricia Sanchez Abril, *A (My) Space of One's Own: On Privacy and Online Social Networks*, 6 NW. J. TECH. & INTELL. PROP. 73, 76, 78 (2007) (noting that although social network privacy expectations "seem to be overwhelmingly generation specific," both younger ("digital natives") and older ("digital immigrants") generations are "fundamentally mistaken" in their assumptions about social network privacy).

81. *See* Sonia Livingstone, *Taking Risky Opportunities in Youthful Content Creation: Teenagers' Use of Social Networking Sites for Intimacy, Privacy and Self-Expression*, 10 NEW MEDIA & SOC'Y 393, 408 (2008) (finding that risks may exist through "poorly designed site settings" that make it unclear as to who can see what information on the site); Robert Sprague & Corey Ciocchetti, *Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws*, 19 ALB. L.J. SCI. & TECH. 91, 121–23 (2009) (noting that users rarely read privacy policies, that such policies are often confusing, and that personal information can be collected passively, without the user's knowledge); *cf.* ANDREW FRACKMAN ET AL., INTERNET AND ONLINE PRIVACY 19–22 (2002) (discussing a variety of ways in which information is passively collected on the internet); danah boyd, *Why Youth⁄Social Network Sites: The Role of Networked Publics in Teenage Social Life*, *in* YOUTH, IDENTITY, AND DIGITAL MEDIA 119, 131 (David Buckingham ed., 2008) (discussing how teens envision an online audience that is connected to their social world offline, but "their audience online may not be who they think it is"); Julia B. Earp et al., *Examining Internet Privacy Policies Within the Context of User Privacy Values*, 52 IEEE TRANSACTIONS ENG'G MGMT. 227, 233–34 (2005)

example, a Facebook user may believe that his profile is only available to a limited number of people, and would be surprised to realize that the profile—and all of the information included on the profile—was available to anyone with a Facebook account.[82] Thus, the user may have a subjective expectation of privacy even though that expectation is inconsistent with reality.

Although both older and younger users may be misinformed about who has access to their posted information, older users are more likely to be distressed to learn the truth.[83] This is because younger users may view the sites differently.[84] Younger users may view the sites as a means of maintaining contact with existing friends *and* making new friends—expanding their social networks.[85] This view is consistent with the intent of the Facebook founders and the concept of social networking sites.[86] Consequently, these younger users may not be surprised or distressed to learn that their profiles are available to a wider audience than originally intended. Or, if they are distressed, it is due to concerns about access by their parents or other known individuals rather than the government or a stranger's access.[87] On the other hand, older individuals may be

(discussing a study concluding that website privacy policy content does not reflect user privacy values and may result in a loss of users' trust in organizations); Lauren Gelman, *Privacy, Free Speech, and "Blurry-Edged" Social Networks*, 50 B.C. L. REV. 1315, 1328–29 (2009) (noting that sites like Facebook create an "aura of privacy," but that site features and social pressures incent disclosure, making it "increasingly challenging to maintain" limited disclosure); Yasamine Hashemi, Note, *Facebook's Privacy Policy and Its Third-Party Partnerships: Lucrativity and Liability*, 15 B.U. J. SCI. & TECH. L. 140, 144–146 (2009) (discussing Facebook user protest over Facebook's third-party partnerships, which made profile information public without many users being aware).

82. *See* danah m. boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMM. 210, 222 (2008) (discussing a "privacy paradox," which occurs because students may desire to protect their online privacy but are unaware of the public nature of the social network sites).

83. *See* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1179–81 (2009) (suggesting that teenagers may be aware of risks, but are "notorious risk-takers" and therefore may not recognize the later consequences of disclosing personal information online); William McGeveran, *Disclosure, Endorsement, and Identity in Social Marketing*, 2009 U. ILL. L. REV. 1105, 1126 (2009) (stating that younger users have a more relaxed opinion about online information privacy); Kim Bartel Sheehan, *Toward a Typology of Internet Users and Online Privacy Concerns*, 18 INFO. SOC'Y 21, 30 (2002) (finding that "alarmed Internet users"—those who "are highly concerned about their privacy online"—tend to be older and more educated).

84. Grimmelmann, *supra* note 83, at 1179–81 (discussing the "divergence in privacy norms between heavily wired teens and their parents").

85. *See* Nicole B. Ellison et al., *The Benefits of Facebook "Friends": Social Capital and College Students' Use of Online Social Network Sites*, 12 J. COMPUTER-MEDIATED COMM. 1143, 1143, 1155 (2007) (noting that users may utilize social network sites to meet new people and reporting a study finding a "slight tendency for newer [college] students to use Facebook to meet new people"); Emily Nussbaum, *Say Everything*, N.Y. MAG., http://nymag.com/news/features/27341 (last visited May 26, 2012) (interviewing social network site users who disclose personal information to the public in order to have fun, show their creativity, stay connected with friends, and meet strangers).

86. *See* Mark Zuckerberg, *From Facebook, Answering Privacy Concerns with New Settings*, WASH. POST (May 24, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/05/23/AR2010052303828.html (Facebook's founder stating: "Six years ago, we built Facebook around a few simple ideas. People want to share and stay connected with their friends and the people around them. . . . If people share more, the world will become more open and connected. And a world that's more open and connected is a better world").

87. Livingstone, *supra* note 81, at 405 ("[B]eing visible to strangers . . . is not so much a concern . . . as that of being visible to known but inappropriate others – especially parents."); *see also* boyd, *supra* note 81, at

dismayed at the thought of those that they do not know having access to their information.[88]

Although some privacy concerns are consistent across age groups, research has shown that youth generally have significantly lower expectations of privacy than adults.[89] This may be the result of several factors. First, they have much less control over most aspects of their lives.[90] They are subject to the rules and restrictions of their parents or guardians, school officials, and other adults. At home they may not have complete control over access to their physical spaces (such as bedrooms) and may have no choice but to allow parental monitoring of their phone and computer usage.[91] At school, backpacks, desks, and lockers may be subject to inspection.[92] In short, youth are unable to claim the same level or privacy that adults enjoy.

Professor Seounmi Youn conducted a study in 2002 that collected responses from 326 Midwest public high school students.[93] Based on the students' responses to the survey, Professor Youn found that teens were concerned with protecting their privacy, and that the teens conducted risk and benefit appraisals to determine whether to disclose information online.[94] The higher the perceived risk associated with the disclosure, the less likely the teens were to disclose personal information.[95] If, however, the teens believed that the disclosure would result in a benefit, they were more willing to disclose personal information.[96] Moreover, the data indicated that teens

131–32, 134–35 (noting that many teens engage in deceptive tactics online in order to "protect themselves from the watchful eye of parents").

88. *See* Abril, *supra* note 80, at 76–78 (discussing how digital immigrants view privacy in terms of control, but do not understand technology well enough to realize that even if they originally control disclosure of personal information online, this information can be disseminated throughout the online world); *cf.* Livingstone, *supra* note 81, at 404 ("[S]ocial networking sites typically display as standard precisely the information that previous generations often have regarded as private . . . .").

89. Sheehan, *supra* note 83 (finding in a study that younger, less-educated internet users have the lowest privacy concern whereas younger, better-educated internet users have a slightly more moderate level of privacy concern compared with older users); *see also* McGeveran, *supra* note 83, at 1126 ("[U]sers of social networks, especially younger users, simply have particularly relaxed preferences about information privacy.").

90. Roper v. Simmons, 543 U.S. 551, 569 (2005) (explaining that "juveniles have less control, or less experience with control, over their own environment").

91. *See* boyd, *supra* note 81, at 134–35 ("For many teens, home is a highly regulated space with rules and norms that are strictly controlled by adults."). Many teens also engage in deceptive tactics online in order to "protect themselves from the watchful eye of parents." *Id.* at 131–32; *see also* Eszter Hargittai, *Whose Space? Differences Among Users and Non-Users of Social Network Sites*, 13 J. COMPUTER-MEDIATED COMM. 276, 291 (2008) (finding that students who live at home with their parents tend to use Facebook less than those who live with roommates or alone, reasoning that parents could put limits on their Internet use, that students who live with parents may have less time online if they have to share the computer, or that students who live at home know less of their peers so have less interest in following them online).

92. *See, e.g.*, New Jersey v. T.L.O., 469 U.S. 325, 342, 346–48 (1985) (holding that a search for cigarettes that subsequently found marijuana in a student's purse by a school official was permissible in scope because the measures were reasonably related to the search objectives and were not intrusive in light of the age and sex of the student).

93. Seounmi Youn, *Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk-Benefit Appraisal Approach*, 49 J. BROADCASTING & ELECTRONIC MEDIA 86, 95–96 (2005).

94. *Id.* at 104.

95. *Id.*

96. *Id.*

were likely to downplay possible risks of disclosure and that "benefit perception was more important than risk perception in predicting teenagers' willingness to disclose information."[97] The study did reveal attempts by teens to protect themselves by providing false or incomplete information, thus allowing them to receive the promised benefits while minimizing disclosure of true personal information.[98]

Additionally, technological literacy may play a role in risk assessment. By the time children reach adolescence they may have a greater understanding than their adult counterparts of how technology works.[99] Kids today are exposed to technology at a very young age, and they tend to be comfortable with technology.[100] They may have a higher level of comprehension of the many systems involved, the many people who have access to those systems, and the information that is transmitted using the technology.[101] They know that the information they send using their cell phones or post or submit on the internet is available to people they do not know.[102] Consequently, they do not suffer from the misconception that their privacy is absolute when they are on a cell phone or use a computer.[103]

Not only do young people understand their lack of privacy, they are less likely to be concerned about it.[104] Never having had a great deal of privacy, they feel no sense of

97. *Id.*

98. *Id.* at 104. *But see* Alyson L. Young & Anabel Quan-Haase, *Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook*, 4 INT'L CONF. ON COMMUNITIES & TECHNOLOGIES 265, 270–71 (2009) (finding that university students used fake or inaccurate information less frequently than other strategies as an online protective measure).

99. *See* Curt J. Dommeyer & Barbara L. Gross, *What Consumers Know and What They Do: An Investigation of Consumer Knowledge, Awareness, and Use of Privacy Protection Strategies*, 17 J. INTERACTIVE MKTG. 34, 47 (2003) (finding that men and younger people in research study were more aware of privacy protection strategies); Youn, *supra* note 93, at 86, 89 (discussing how teenagers today grew up with the Internet and are more knowledgeable about it, often having to coach their parents about how to use the Internet).

100. *See* Abril, *supra* note 80, at 76–77 (describing the younger generation as "digital natives" because they grew up with the Internet and are therefore "cyber-savvy"); Youn, *supra* note 93, at 86, 89 (noting that "about 75% of 14- to 17-year-olds and 65% of 10- to 13-year-olds used the Internet in 2001" and that "there is general agreement that today's teenagers are knowledgeable and literate with the Internet").

101. *Cf.* Abril, *supra* note 80, at 76–77 (asserting that "digital natives' complex expectations of privacy on OSNs rest on a combination of technology, the anonymity of the multitude, and assumptions about the presence of their unintended audiences"); Dommeyer & Gross, *supra* note 99, at 47–49 (finding that men and younger people are more aware of and likely to use privacy protections).

102. *See* Livingstone, *supra* note 81, at 404 ("[T]eenagers may disclose personal information with up to several hundred people known only casually.").

103. *See* Ralph Gross & Alessandro Acquisti, *Information Revelation and Privacy in Online Social Networks*, 2005 ACM WORKSHOP ON PRIVACY IN THE ELECTRONIC SOC'Y 71, 72–73, 79–80 (providing research suggesting that university students were aware that privacy settings were present, but chose to disclose personal information in order to receive the benefits of public disclosure); Nussbaum, *supra* note 85 (interviewing social network site users who disclose personal information to the public because it's fun, allows them to be creative, keeps them connected with friends, and helps them meet strangers).

104. Gail Salaway et al., *The ECAR Study of Undergraduate Students and Information Technology, 2008*, 8 EDUCAUSE CENTER FOR APPLIED RES. 91–93 (2008) (finding through a research study of students that "[o]verall, [social network site] users do not appear to be overly concerned about privacy and security issues"); Sheehan, *supra* note 83, at 30 (finding in a study that younger, less-educated internet users have the lowest privacy concern, whereas younger, better-educated internet users have a slightly more moderate level of

loss—they cannot miss what they never had. Moreover, they may not feel any need for greater privacy. Whereas they might like to keep things private from their parents, they may not feel the need to protect information from peers or strangers.[105] They may be unable to anticipate the ways in which the information that they disseminate now may be used to their disadvantage in the future. For adolescents, the possibility that the information they post on a social network site will hurt their chances of getting into their college of choice or landing the job of their dreams may be too remote to change their beliefs or behavior.[106] Finally, they may like the idea that they can access information about other people; in other words, their desire to protect their own privacy may be overridden by their desire to invade the privacy of others.[107]

These "digital natives"[108] may seem reckless to the older generation ("digital immigrants"), but Professor Abril argues that digital natives are cognizant of privacy issues and are willing to protest when they believe their privacy rights have been violated.[109] Abril further notes that young internet users' "complex expectations of privacy" on online social networks may be explained in part by a feeling of "anonymity of the multitude."[110] Although they know that their activities can be viewed by others in cyberspace, they believe that no one is focused on them or knows them (other than their friends) and that this anonymity protects them.[111] Professor Abril draws an analogy to drivers who engage in private behavior in their cars knowing that other drivers and pedestrians can see them but feel a false sense of privacy because they believe that no one is focused on them; and, if they are, they are unlikely to recognize or ever see them again.[112]

privacy concern compared with older users); *see also* Grimmelmann, *supra* note 83, at 1179–81 (discussing the "divergence in privacy norms between heavily wired teens and their parents"); McGeveran, *supra* note 83, at 1126 (stating that younger users have a relaxed opinion about online information privacy and believe that people who do not like sharing personal information should not participate in online social networks).

105. Livingstone, *supra* note 81, at 405 (describing teenagers' attitude toward online disclosure as one where there is little concern with strangers but a preference against disclosing unintended information to people they know—especially parents).

106. *See* boyd, *supra* note 81, at 133 (discussing teens facing expulsions from school and legal investigations for content on their MySpace pages, which they presented in order to relate to their perceived audience (peers), without regard for their invisible audiences); Grimmelmann, *supra* note 83, at 1179 ("Later regret about initial openness is an especially serious problem for the most active social-network site users: young people.").

107. *See* boyd, *supra* note 81, at 122 (noting reasons for youth joining social networking sites are to engage in "social voyeurism" and to create an online persona); Adam N. Joinson, *'Looking at', 'Looking up' or 'Keeping up with' People? Motives and Uses of Facebook*, 26 CHI. CONF. ON HUM. FACTORS IN COMPUTING SYSTEMS 1027, 1034–35 (2008) (finding that a subset of Facebook users wishing to use the site to meet new people often employ privacy settings less stringent than the default).

108. Abril, *supra* note 80, at 76 (adopting the terminology coined by John Palfrey, Jr., Commentary, *We Googled You*, HARV. BUS. REV., June 2007, at 42).

109. *See id.* at 76 n.18 (describing protests by Facebook users when the site introduced new features that users perceived as privacy violations).

110. *Id.* at 77.

111. *See id.* ("While young digitals know on some level that their online behavior is ultimately subject to the unforgiving scrutiny of the Internet, they demand the right to exercise their situational personalities and still be shielded from unintended audiences. Theirs is a conception of privacy rooted in their perceived entitlement of selective *anonymity*.").

112. *Id.* at 76–77.

Although this diminished sense of privacy among youth may not be new, the consequences may be more far-reaching. The attitudes that youth have toward online privacy may persist into adulthood, causing a shift in the privacy attitudes of society as a whole. If youth become comfortable with the idea that information shared online or via cell phones is not private, and that belief continues as they grow older, the result may be that in future decades older adults (today's youth) will have diminished privacy expectations.

To understand why this view of the future is plausible, one must understand why older adults currently view privacy differently. They are more likely to think of privacy as it relates to physical spaces, such as their homes or cars,[113] and they think of privacy protection in terms of control.[114] Privacy in that context can be protected using physical barriers or by excluding people from those areas, and by hiding or destroying physical evidence of their activities.[115]

> Their era gave them the opportunity to successfully rewrite their personal histories through legal and social mechanisms: criminal records could be expunged, foolish marriages could be annulled, shameful teenage pregnancies could be covered up by "moving away," and all was forgotten. In their youth, newspapers yellowed and memories failed, leaving only the person's word as evidence (i.e., the laughably exonerating, "*I smoked marijuana but never inhaled*").[116]

Personal or intimate details shared via email, text message, Twitter, or Facebook posting can be widely disseminated very quickly. Online content can be saved indefinitely and searched quickly and easily. Such evidence cannot be easily erased or disavowed. Youth understand these truths and accept them.[117] Such knowledge will likely carry into adulthood and continues to shape perceptions of privacy.

In an article about youth revelations on the internet, Emily Nussbaum interviewed Xiyin Tang, a nineteen-year old Columbia University student who began a blog at age thirteen.[118] The online journal was distributed to 200 readers, yet Tang viewed her writing as personal: "I basically wrote as if there was no one reading it. And if people wanted to read it, then great."[119] But as readership grew, so did Tang's awareness of her audience, and she started to write with them in mind. Her style and content were

113. *See* Michelle N. Kwasny et al., *Privacy and Technology: Folk Definitions and Perspectives*, 26 CHI. CONF. ON HUM. FACTORS IN COMPUTING SYSTEMS 3291, 3295 (2008) (concluding that older adults tend to view privacy in terms of space rather than in terms of information).

114. *See* Abril, *supra* note 80, at 77 (noting that digital immigrants "grew up in a world where they had the luxury of control over their information").

115. *See id.* at 77–78.

116. *Id.* at 77 (footnote omitted). Older adults are also less likely to understand technology and may underestimate the degree to which others may intercept their conversations or the number of people who have access to the information they transmit using a cell phone or computer. *See id.* at 76–78 (discussing how digital immigrants view privacy in terms of control, but do not understand technology well enough to realize that even if they originally control disclosure of personal information online, this information can be disseminated throughout the online world).

117. *See* Nussbaum, *supra* note 85.

118. *Id.*

119. *Id.* (quoting Tang).

aimed to impress and grow her online community.[120] This self-awareness did not necessarily translate into caution.[121]

Nussbaum concludes that youth have become accustomed to thinking of every communication as potentially public.[122] They know that even a private email can be forwarded to an infinite number of others or the content can be copied and pasted onto a public website.[123]

> It's a form of communication that requires a person to be constantly aware that anything you say can and will be used against you, but somehow not to mind.
>
> . . . In essence, every young person in America has become, in the literal sense, a public figure. And so they have adopted the skills that celebrities learn in order not to go crazy: enjoying the attention instead of fighting it—and doing their own publicity before somebody does it for them.[124]

This perception of oneself is unlikely to change dramatically with age; instead, experience is likely to confirm and strengthen it. As a consequence, the view of self and privacy embraced by youth may become the predominant view of older adults in the near future.

IV. VARYING EXPECTATIONS, VARYING PROTECTION

Viewing these findings in the context of the subjective portion of the Fourth Amendment test, it is clear that whether a person has a subjective expectation of privacy in any given circumstance may depend, at least in part, on the person's age. An older adult may believe that information posted on a social networking site is private and thus have a subjective expectation of privacy with respect to that information. The expectation may be particularly strong if privacy settings have been set to limit access; but the expectation of privacy may also exist if the user does not understand that the default settings allow everyone to view the user's profile or if only some of the settings are set to limit access. Even though the content is available to third parties, they may view it as analogous to written letters, which are protected from government searches.[125] Consequently, they may assume that the postings are likewise protected. If the Court finds that society is prepared to accept that expectation as reasonable,[126] then the information will be protected by the Fourth Amendment.[127]

120. *Id.*

121. *Id.* As Nussbaum reports, "Xiyin knows there's a scare factor in having such a big online viewership—you could get stalked for real, or your employer could bust you for partying. But her actual experience has been that if someone is watching, it's probably a good thing. . . . All sorts of opportunities—romantic, professional, creative—seem to Xiyin to be directly linked to her willingness to reveal herself a little." *Id*.

122. *Id.*

123. *Id.*

124. *Id.*

125. *See* United States v. Jacobsen, 466 U.S. 109, 114 (1984) (finding a reasonable expectation of privacy in sealed, mailed letters).

126. This objective component will be discussed in Part V, *infra*. Whether "society" is prepared to accept a subjective expectation as reasonable may also depend upon the age of those whose opinions are considered. Younger citizens may be likely to conclude that it is unreasonable to believe that information

Conversely, a younger adult may have no subjective expectation of privacy with respect to anything posted on a social network site. Since younger users tend to use sites to keep in contact with friends and make new friends, they are more likely to view the sites as a means of displaying information instead of hiding it.[128] Under these facts, courts would not need to consider the objective portion of the Fourth Amendment test; if there is no subjective expectation of privacy, there is no Fourth Amendment protection.[129]

The point can be further illustrated by drawing upon the facts of *City of Ontario v. Quon*.[130] In *Quon*, the district court and Ninth Circuit Court of Appeals debated whether a search of text messages Officer Quon sent using his government-issued pager was reasonable under the Fourth Amendment.[131] There was disagreement on this point,[132] but the courts were in agreement that Quon had a subjective expectation of privacy in the messages[133] despite a department policy that specifically stated that "[u]sers should have no expectation of privacy or confidentiality when using these resources."[134] Moreover, Quon's expectation was held to be reasonable.[135]

A younger employee in the same circumstances may be more likely to take the department's stated policy at face value and not have a subjective expectation of privacy, particularly since the younger employee may only recently have graduated from school, which may have had a similar policy, or previously had a cell phone purchased by his or her parents who had a right to see the content of any text messages. Lacking a subjective expectation of privacy, that younger employee's text messages

posted on a social network site is private. See *infra* Part V for a discussion of the objective component of determining whether Fourth Amendment protection applies.

127. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (noting that in addition to a subjective inquiry, the court must execute an objective inquiry, and ask whether one's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable'" when determining whether the Fourth Amendment will apply).

128. *See* Ellison et al., *supra* note 85, at 1143 (explaining that some Facebook users use the site to interact with people they know and to meet new people); Nussbaum *supra* note 85 (describing social network site users who disclose personal information to the public in order to have fun, show their creativity, stay connected with friends, and meet strangers).

129. *But see* Smith v. Maryland, 442 U.S. 735, 741 n.5 (1979) (indicating that in some extraordinary circumstances Fourth Amendment protection may apply despite a lack of a subjective expectation of privacy).

130. 130 S. Ct. 2619 (2010).

131. *Quon*, 130 S. Ct. at 2626–27. See *supra* notes 69–78 and accompanying text for further discussion of *Quon*.

132. *See Quon*, 130 S. Ct. at 2626–27 (explaining that the district court found no Fourth Amendment violation whereas the appellate court found that the scope of the search was unreasonable).

133. *See id.* at 2626–27 (indicating that the district and appellate courts disagreed on the reasonableness of the search itself, not the plaintiff's subjective expectation of privacy); *id.* at 2629 (noting the Court assumed, arguendo, that plaintiff had a subjective expectation of privacy).

134. *Id*. at 2625. One of Quon's superiors told him that the messages would not be searched if Quon paid for any overages. *Id.* at 2629. This contradicted the stated policy and, according to the courts, justified Quon's subjective expectation of privacy. *See id*. at 2626–27 (noting the district court found the expectation of privacy was reasonable despite the policy that explicitly stated the information would not be private or confidential).

135. *See id.* at 2626–27 (indicating that both the district and appellate courts found plaintiff's expectation of privacy was "reasonable"); *id.* at 2629 (assuming that plaintiff's expectation of privacy was "reasonable").

would not be protected by the Fourth Amendment (he or she could be searched without proof that the search was reasonable by Fourth Amendment standards) even though Quon's messages could be protected.[136]

V. REASONABLE EXPECTATIONS AND SEARCHES

> We have no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable. Instead, "the Court has given weight to such factors as the intention of the Framers of the Fourth Amendment, the uses to which the individual has put a location, and our societal understanding that certain areas deserve the most scrupulous protection from government invasion."[137]

Whether "society" is prepared to accept a subjective expectation of privacy as reasonable may depend upon which segments of society are being considered. Youth and young adults may believe that any expectation of privacy when using many forms of technology is unreasonable.[138] This may reflect their greater understanding of the technology[139] and the risks involved in using almost any technology.[140] They may be familiar with successful attempts to hack into or access codes or accounts, and understand that few if any sites or accounts are truly secure.[141] Consequently, they may consider any subjective expectation of privacy to be unreasonable.

136. The search of the messages was ultimately held to be reasonable and not in violation of the Fourth Amendment; but the reasonableness of the search would have been irrelevant if Quon's expectation of privacy was not reasonable in the first instance. *See id.* at 2628–29 (explaining that a plaintiff's reasonable expectation of privacy must be determined on a "case-by-case" basis, but nonetheless deciding the Fourth Amendment issue based on the alternative grounds of the search's reasonableness).

137. O'Connor v. Ortega, 480 U.S. 709, 715 (1987) (quoting Oliver v. United States, 466 U.S. 170, 178 (1984)).

138. *See* Grimmelmann, *supra* note 83, at 1179–81 (discussing the "divergence in privacy norms between heavily wired teens and their parents"); McGeveran, *supra* note 83, at 1126 (stating that younger users have a relaxed opinion about online information privacy and believe that if people do not like sharing personal information, they should not participate in online social networks); Salaway et al., *supra* note 104, at 91–93 (presenting a study that showed the younger the student, the greater likelihood that he or she would reveal personal information over a social networking site); Sheehan, *supra* note 83 (finding that younger, less-educated internet users have the lowest privacy concern, whereas younger, better-educated internet users have a slightly more moderate level of privacy concern, as compared to older users); Youn, *supra* note 93, at 89–90, 104 (study suggesting that, because teenagers see certain activities as prevalent and popular and therefore not risky, they are more interested in the benefits they will receive from disclosing personal information than they are with the privacy risks associated with their online activity).

139. *See* Youn, *supra* note 93, at 86–89 (discussing how teenagers today grew up with the Internet and are more knowledgeable about it, often having to coach their parents about how to use the Internet); *cf.* Abril, *supra* note 80, at 76 (describing youth who grew up with the Internet as "digital natives"); Dommeyer & Gross, *supra* note 99, at 47–48 (finding that younger people were more aware of privacy protection strategies).

140. *Cf.* Dommeyer & Gross, *supra* note 99, at 47–48 (finding that youth have greater knowledge and awareness of privacy protections); Youn, *supra* note 93, at 91, 97 (study finding that teenagers are aware of potential risks online and therefore will often provide false information).

141. *Cf.* Grimmelmann, *supra* note 83, at 1179–81 (suggesting that teenagers may be aware of risks, but are "notorious risk-takers" and therefore may not recognize the later consequences of disclosing personal information online).

A. Youth, "Special Needs," and Lower Expectations

The reasonable expectation of privacy of students has received a great deal of attention from courts. As an initial matter, the Supreme Court has found "generally, students have a less robust expectation of privacy than is afforded the general population."[142] This is not to say that students have no privacy protection, but such expectations are diminished because of age and the particular needs of the school setting.[143] Even where a subjective, reasonable expectation of privacy is found, the courts have often held that searches of students are reasonable and, therefore, not in violation of the Fourth Amendment.[144]

In *New Jersey v. T.L.O.*,[145] the Court considered a student's claim that a school administrator's search of her purse violated her Fourth Amendment rights.[146] The search occurred after a teacher claimed to have caught T.L.O. and another student smoking in the girls' restroom.[147] Smoking violated school policy, and the girls were taken to the assistant vice principal.[148] Although her companion admitted to smoking, T.L.O. denied that she had been smoking in the restroom and further claimed that she did not smoke at all.[149] The assistant vice principal took T.L.O. into his office and examined the contents of her purse.[150] The search revealed a pack of cigarettes as well as evidence that T.L.O. had been smoking and perhaps selling marijuana.[151] In addition to receiving a suspension from school, T.L.O. faced juvenile delinquency charges.[152] T.L.O. sought to have the evidence obtained from her purse suppressed on the ground that the search violated her Fourth Amendment rights.[153]

The Court acknowledged that the Fourth Amendment protects students from unreasonable searches and seizures.[154] Moreover, the Court recognized that although the need to maintain security in schools is a legitimate and often difficult task, students—unlike prisoners—do not abandon all expectations of privacy when they go to school. "[T]here [wa]s no reason to conclude that [school children] have necessarily

142. Brannum v. Overton Cnty. Sch. Bd., 516 F.3d 489, 496 (6th Cir. 2008) (citing New Jersey v. T.L.O., 469 U.S. 325, 348 (1985) (Powell, J., concurring)).

143. *T.L.O.*, 469 U.S. at 352 (Blackmun, J., concurring).

144. *See, e.g.*, *id*. at 341–42 (holding that a teacher's search of a student is reasonable, and thus compliant with the Fourth Amendment, if it is "justified at its inception" and reasonable in scope (quoting Terry v. Ohio, 392 U. S. 1, 20 (1967))).

145. 469 U.S. 325 (1985).

146. *T.L.O.*, 469 U.S. at 329, 331.

147. *Id*. at 328.

148. *Id*.

149. *Id*.

150. *Id*.

151. *Id.*

152. *Id.* at 329 & n.1.

153. *Id*. at 329.

154. *Id*. at 336–37. This holding resolved a split in the lower courts, some of which had held that school officials acted *in loco parentis* and, as such, were exempt from the Fourth Amendment prohibition on unreasonable searches and seizures. *Id*. (citing R.C.M. v. State, 660 S.W.2d 552 (Tex. App. 1983)).

waived all rights to privacy in [legitimate, non-contraband items] merely by bringing them onto school grounds."[155]

However, the Court held that the need for school officials to maintain discipline and a safe environment called for relaxation of the warrant and probable cause requirements that prevail in other Fourth Amendment contexts.[156] With respect to the warrant requirement, the Court held that "requiring a teacher to obtain a warrant before searching a child suspected of an infraction of school rules (or of the criminal law) would unduly interfere with the maintenance of the swift and informal disciplinary procedures needed in the schools."[157] Likewise, the Court held that something less than probable cause was necessary to justify searches of schoolchildren by teachers and administrators.[158] Instead, the proper test was "reasonableness, under all of the circumstances."[159] Establishing reasonableness requires proof that: (1) the search was reasonable at its inception; and (2) that the scope of the search was reasonable in light of the circumstances.[160]

> Under ordinary circumstances, a search of a student by a teacher . . . will be "justified at its inception" when there are reasonable grounds for suspecting that the search will turn up evidence that the student has violated or is violating either the law or the rules of the school. Such a search will be permissible in its scope when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the age and sex of the student and the nature of the infraction.[161]

The Court held that the search of T.L.O.'s purse was reasonable at its inception and in scope and, consequently, did not violate her rights under the Fourth Amendment.[162]

In *United States v. Heckenkamp*,[163] a student whose personal computer was searched based upon suspicion that the student had used the computer to gain unauthorized access to the university computer system alleged that the warrantless search violated his Fourth Amendment rights.[164] The Ninth Circuit held that the student's subjective expectation of privacy in his computer was objectively reasonable,[165] even after he logged onto the university network, finding that the mere act of accessing a network does not extinguish privacy expectations.[166] Unlike the

155. *Id.* at 338–39.

156. *Id.* at 339–41. The Court noted, "It is evident that the school setting requires some easing of the restrictions to which searches by public authorities are ordinarily subject." *Id.* at 340.

157. *Id.* at 340.

158. *Id.* at 341.

159. *Id.*

160. *Id.* Note that this is the same test applied to searches of government employees' work spaces. *See* O'Connor v. Ortega, 480 U.S. 709, 725–26 (1987).

161. *T.L.O.*, 469 U.S. at 341–42 (footnotes omitted).

162. *Id.* at 346–47.

163. 482 F.3d 1142 (9th Cir. 2007).

164. *Heckenkamp*, 482 F.3d at 1143–46.

165. *Id.* at 1147.

166. *Id.* at 1146–47.

policy in *Biby*,[167] the University of Wisconsin policy at issue in *Heckenkamp* reinforced students' expectations of privacy. It stated that

> [i]n general, all computer and electronic files should be free from access by any but the authorized users of those files. Exceptions to this basic principle shall be kept to a minimum and made only where essential to . . . protect the integrity of the University and the rights and property of the state.[168]

Notwithstanding the reasonable expectation of privacy, the Ninth Circuit held that the search was reasonable under the "special needs" exception to the Fourth Amendment warrant requirement.[169] The search was conducted by a university administrator solely in his capacity as a system administrator for the purpose of protecting the integrity of the university network and not for any law enforcement purpose.[170] The university's actions were consistent with its policy, to which Heckenkamp had assented, because it was conducting the search in response to an "emergency situation[] that threaten[ed] the integrity of campus computer or communication systems."[171] The court further noted that the relationship between the student and the campus systems administrator was different from the "adversarial relationship" between criminal suspects and law enforcement.[172] No warrant was required under the circumstances and the search was held to have been reasonable.[173]

In *Brannum v. Overton County School Board*,[174] the issue was privacy in middle school locker rooms.[175] A middle school installed video surveillance cameras in the boys' and girls' locker rooms (and other locations throughout the building) as part of an effort to increase security at the school.[176] The cameras viewed and recorded students while changing clothes, so that some of the video included students while in their undergarments.[177] Neither students nor their parents ever consented to the surveillance; indeed, they were not informed that the videotaping was taking place.[178]

Applying the standards set out in *T.L.O.*, the Sixth Circuit first concluded that the students had a reasonable expectation of privacy in the locker rooms.[179] The court

167. See *supra* notes 47–49 and accompanying text for a discussion of the *Biby* case.

168. *Heckenkamp*, 482 F.3d at 1147 (alteration and omission in original).

169. *Id.*

170. *Id.* In fact, the Federal Bureau of Investigation was in the process of getting a search warrant and had asked the administrator to delay conducting his own search. The administrator, motivated by his concerns about the security of the university email server, conducted the search anyway. Thus, not only was the administrator not acting in concert with law enforcement officials, his actions were contrary to the law enforcement officials' desires. *Id.*

171. *Id.* at 1147–48.

172. *Id.* at 1148.

173. *Id.*

174. 516 F.3d 489 (6th Cir. 2008).

175. *Brannum*, 516 F.3d at 491–92.

176. *Id.* at 492.

177. *Id.*

178. *Id.* at 496.

179. *Brannum*, 516 F.3d at 496 ("[W]e are satisfied that students using the LMS locker rooms could reasonably expect that no one, especially the school administrators, would videotape them, without their knowledge, in various states of undress while they changed their clothes for an athletic activity.").

further found that the videotaping of the students without their knowledge or permission was unreasonable in scope and violated those expectations of privacy:[180]

> [W]e believe placing cameras in such a way so as to view the children dressing and undressing in a locker room is incongruent to any demonstrated necessity, and wholly disproportionate to the claimed policy goal of assuring increased school security, especially when there is no history of any threat to security in the locker rooms.[181]

The Supreme Court addressed the issue of student strip searches in *Safford Unified School District #1 v. Redding*.[182] In that case, another student told school officials that thirteen-year-old Savana Redding had given her prescription-strength ibuprofen and over-the-counter naproxen.[183] Such medications were prohibited on school grounds without permission.[184] Based upon this information and other pills found in a day planner that belonged to Redding, school officials called Redding into the assistant principal's office and questioned her.[185] After denying having any knowledge of the pills, Redding consented to a search of her belongings.[186] A search of her backpack revealed nothing.[187]

Redding was then taken to the school nurse's office and was instructed to remove her outer clothing and pull her undergarments away from her body so that school officials could search her for pills.[188] No pills were found.[189] Redding's mother filed suit alleging violation of Redding's Fourth Amendment rights.[190] The federal district court and a panel of the Ninth Circuit both held in favor of the school board, finding no Fourth Amendment violation.[191] After rehearing en banc, however, the Ninth Circuit held that the search was unreasonable and reversed.[192]

The Supreme Court agreed that the search was unreasonable and affirmed the Ninth Circuit's holding on the Fourth Amendment issue.[193] The Court first addressed Redding's expectations of privacy. Redding's "subjective expectation of privacy against such a search is inherent in her account of it as embarrassing, frightening, and humiliating. The reasonableness of her expectation . . . is indicated by the consistent experiences of other young people similarly searched, whose adolescent vulnerability

180. *Id.* at 497–98.

181. *Id.* at 498.

182. 129 S. Ct. 2633 (2009).

183. *Safford*, 129 S. Ct. at 2638.

184. *Id.*

185. *Id.*

186. *Id.*

187. *Id.*

188. *Id.* The school nurse and a female administrative assistant conducted the search and were the only other persons present. *Id.*

189. *Id.*

190. *Id.*

191. *Id.*

192. *Id.*

193. *Id.* at 2642–43. The court reversed the Ninth Circuit's holding that the rights at issue were clearly established, thus depriving the officials of qualified immunity. *Id.* at 2643–44.

intensifies the patent intrusiveness of the exposure."[194] The Court then turned to the factors set out in *T.L.O.* to determine whether the search was reasonable at its inception and in scope.[195]

While the search of her backpack and outer clothing was reasonable,[196] the Court found the search of her underwear excessive in light of the facts.[197] First, Redding was suspected of concealing pills that were available over the counter, as opposed to illegal or inherently harmful drugs.[198] The Court further found it implausible that Redding would be hiding pills in her underwear.[199] "[T]he categorically extreme intrusiveness of a search down to the body of an adolescent requires some justification in suspected facts, general background possibilities fall short; a reasonable search that extensive calls for suspicion that it will pay off."[200] Because the scope of the search was unreasonable, it violated Redding's Fourth Amendment rights.[201]

B. Which Segment of Society Determines what is Reasonable?

Realities of the school environment lead to lesser protection for youth, which may explain decreased subjective expectations of privacy among that age group. This decreased subjective expectation may also affect how a court might answer the second part of the Fourth Amendment test. The objective part of the Fourth Amendment test asks whether "society" is prepared to accept a given subjective expectation of privacy as reasonable.[202] Since "society" is presumably composed of people from all segments of the population, the answer may vary depending upon which group's beliefs prevail.

As the examples above and in Part IV demonstrate, varying privacy expectations could lead courts to provide greater protection to older adults than younger adults even though the information and surrounding circumstances at issue (postings on a social network site, text messages sent on government-issued pagers) are exactly the same. To the extent that varying expectations are inevitable, the courts must also decide whether the expectations of one group should prevail over those of another. Erring on the side of protection, it seems logical that courts should prefer the viewpoint of older generations, particularly since their expectations have been shaped by prior precedent and their own experiences.

Adopting views typical of older citizens might result in greater protection for all citizens since they might be willing to accept as reasonable subjective expectations that younger citizens believe to be unreasonable. This can occur because cases brought before a court are decided based upon whether the particular judges or jury hearing the

194. *Id.* at 2641.

195. *Id.* at 2641–43.

196. *Id.* at 2641 ("If Wilson's reasonable suspicion of pill distribution were [sic] not understood to support searches of outer clothes and backpack, it would not justify any search worth making.").

197. *Id.* at 2642–43.

198. *Id.* at 2642. Although the ibuprofen pills Savana was suspected of bringing onto school property were prescription strength, the pills were equivalent to two over-the-counter strength pills. *Id.*

199. *Id.*

200. *Id.*

201. *Id.* at 2642–43.

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

case believe that "society" is willing to accept a person's subjective expectation as reasonable. If those judges adopt the more conservative view of privacy favored by older generations, the result will be a finding that "society" is willing to extend Fourth Amendment protection to the circumstances of that case. The result will be binding on the government even with respect to those who do not share that belief. Consequently, younger people may be protected even though they would not have found the expectation of privacy to be reasonable.

This is not to say that the views of youth can or should be ignored. As they age, their privacy expectations may become the norm and reflect the views of an increasing share of the population. As discussed above, subjective privacy expectations among youth are diminishing even outside of regulated spaces such as schools. If these attitudes persist into adulthood, the expectations of society as a whole may shift and diminish over time. Consequently, "society" may be less willing to accept that certain subjective expectations are reasonable. As youth continue to influence society, courts must be aware of the changes and make decisions regarding the reasonableness of privacy expectations accordingly. Even if judges—particularly older judges—maintain heightened expectations of privacy, if the government can establish that large segments of society do not support those expectations, the judges will have to choose between their own beliefs and those of other, potentially larger, segments of society.

VI. LEGISLATIVE RESPONSES

Legislation may be the easiest way for privacy rights to be protected in the absence of a subjective expectation of privacy; but the law tends to lag considerably behind technology.[203] Congress has enacted many statutes that affect electronic communication and internet use. The Electronic Communications Privacy Act (ECPA) governs the interception of wire and electronic communications.[204] The ECPA amended the Federal Wiretap Act to extend protections that previously applied to the interception of oral and telephone communications to electronic and data transmissions.[205] The ECPA prohibits the interception or disclosure of such communications unless: the party intercepting is a party to the communication; the intercepting party has the consent of a party to the communication; or the intercepting party is authorized by law to intercept or conduct electronic surveillance.[206] Even those authorized parties cannot disclose the information without a court order, statutory authorization, or certification.[207] If a communication is available to the general public, then it is not unlawful to intercept or access it.[208]

203. *See* Tracy Mitrano, *A Wider World: Youth, Privacy, and Social Networking Technologies*, EDUCAUSE REV., Nov.–Dec. 2006, at 16, 20.

204. 18 U.S.C. §§ 2510–2522 (2006).

205. *In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 18 (1st Cir. 2003) ("The paramount objective of the Wiretap Act is to protect effectively the privacy of communications.").

206. 18 U.S.C. § 2511(2)(b)–(d). Examples of authorized persons are landlords or internet service providers. *Id.* § 2511(a)(ii).

207. *Id.* § 2511(a)(ii)(A)–(B).

208. *Id.* § 2511(g)(1). Communications of a "computer trespasser" (one who uses a protected computer without authorization) can also be intercepted if the owner of the protected computer gives consent or if there

Federal agencies, including the Federal Bureau of Investigation, can obtain permission to intercept certain communications if they can establish that the communication may provide evidence of a crime relating to federal offenses such as counterfeiting, fraud, extortion, obscenity, location of a fugitive, smuggling of aliens, firearms, production of false identification documents, or terrorism.[209] If a governmental agency is granted permission to intercept the communications or if they have obtained any knowledge of the contents of the communications, then they can disclose this information and evidence to other law enforcement officers.[210] Privileged communications remain privileged even if intercepted.[211] While intercepting communications, if the agency discovers communications related to another crime, they can intercept those communications if they obtain a court order using the guidelines of the statute.[212]

The Stored Communications Act (SCA) is Title II of the ECPA and protects information that is being stored or temporarily stored.[213] The SCA makes it unlawful to intentionally access, without authorization or by exceeding authorization, a facility where electronic communication service is provided.[214] An electronic communications service provider can disclose only a customer's electronically stored information under the following circumstances: to the recipient of the communication; by consent of the originator of the communication; as authorized by law under 18 U.S.C. § 2511; for purposes of providing the service; to a law enforcement officer if the communications appear criminal; to the National Center for Missing or Exploited Children; or to a government agency if the service provider has a good faith belief that there is imminent danger to a person.[215] The provider can also disclose the customer's record for many of the same reasons.[216]

If the communication has been stored for less than 180 days, then the government entity must obtain a warrant in order to obtain the information.[217] If it has been stored for more than 180 days, the entity can obtain the communications by warrant, subpoena, or court order.[218] If the investigation regards telemarketing fraud then the entity can obtain the customer records by warrant, court order, consent by the customer,

is an investigation. *Id.* §§ 2510(21), 2511(2)(i). Foreign communication does not have the same standard because it is governed by the Foreign Intelligence Surveillance Act. *Cf. id.* § 2511(e) ("Notwithstanding any other provision of this title . . . it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.").

209. *Id.* § 2516.

210. *Id.* § 2517.

211. *Id.*

212. *Id.*

213. 18 U.S.C. §§ 2701–2711.

214. *Id.* § 2701(a). To violate the statute, the individual accessing the electronic communication service without authorization must "obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage in" the service's system. *Id.* § 2701(a)(2)

215. *Id.* § 2702(b).

216. *Id.*

217. *Id.* § 2703(a).

218. *Id.* § 2703(a)–(b). *But see* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that the SCA is unconstitutional to the extent that it allows disclosure of email content without a warrant).

or a written request.[219] The subpoena or court order may also include an order to have the service provider make a backup copy of the communications.[220] In that case, the provider has to make a copy without notifying the customer.[221] Afterwards, the government will give notice to the customer, thus giving the customer the opportunity to file a motion to quash.[222]

The First Circuit had occasion to apply the ECPA in a class action brought against several pharmaceutical companies and Pharmatrak, a company that developed a service called "NETcompare" that provided the pharmaceutical companies with intra-industry website traffic and usage comparisons.[223] "NETcompare was marketed as a tool that would allow a company to compare traffic on and usage of different parts of its website with the same information from its competitors' websites. . . . This information-gathering was not visible to users of the pharmaceutical clients' websites."[224] When the companies signed up for the services, they conditioned their participation upon Pharmatrak's assurance that no personal information about the website users would be collected.[225] Despite those assurances, some personal information was collected.[226] The lawsuit was filed by and on behalf of users whose information had been collected by Pharmatrak, alleging that the data collection violated the ECPA.[227] The district court granted Pharmatrak's motion for summary judgment on the ground that the pharmaceutical companies consented to Pharmatrak's activities by contracting for Pharmatrak's services.[228] This consent brought Pharmatrak within the "consent" exception to the ECPA.[229]

On appeal, the First Circuit set out the elements of an ECPA claim: the defendant must have intentionally intercepted, endeavored to intercept, or procured another to intercept the contents of an electronic communication using a device.[230] The defendant can defeat an ECPA claim if its conduct falls within a statutory exception, including the consent of one of the parties to the communication.[231] The First Circuit then disagreed with the district court on the issue of the pharmaceutical companies' consent.[232] First, it held that the party claiming the benefit of the consent exception has the burden of

219. 18 U.S.C. § 2703(c).

220. *Id.* § 2704.

221. *Id.* § 2704(a). The lack of notice is intended to prevent deletion of the communication before it can be intercepted. *Id.* § 2705(a)(1), (2)(C).

222. *Id.* § 2704.

223. *In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 12 (1st Cir. 2003).

224. *Id.* at 15.

225. *Id.* at 12.

226. *Id.* at 15. The information included names, addresses, telephone numbers, email addresses, birthdates, gender, insurance status, level of education, occupation, medical conditions, and reasons for visiting the websites. *Id.* Of the estimated 18.7 million users, the plaintiff's expert was able to develop 232 user profiles using this information. *Id.*

227. *Id.* at 12.

228. *Id.* at 13.

229. *Id.*

230. *Id.* at 18.

231. *Id.* at 19.

232. *Id.* at 20.

proving consent.[233] Next, the court clarified what constitutes consent under the ECPA.[234]

"Consent may be explicit or implied, but it must be actual consent rather than constructive consent."[235] Consent cannot be implied merely by purchase of a service.[236] Instead, implied consent requires circumstances that "*convincingly*" demonstrate knowledge of and consent to the interception.[237] Applying this standard, the court held that the pharmaceutical companies did not consent to the interceptions that allegedly violated the ECPA.[238] "Far from consenting to the collection of personally identifiable information, the pharmaceutical clients explicitly conditioned their purchase of NETcompare on the fact that it would *not* collect such information."[239] Furthermore, the court held that the undisputed facts showed that the website users did not even know about the Pharmatrak program and, therefore, could not have consented to Pharmatrak's collection of personal information.[240]

Finally, the court addressed the requirement that data or electronic communications be "intercepted" by the defendant.[241] Interception is "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[242] Prior to the ECPA's enactment, a debate emerged among courts with respect to how narrowly this definition should be construed.[243] Some courts argued that interception occurred only if the acquisition was contemporaneous with the transmission.[244] If the transmission was stored for a period of time before the acquisition, then no "interception" was held to have occurred.[245]

The debate continued after the ECPA was enacted, with some circuits distinguishing between acquisitions while the transmission was in transit and acquisitions from storage.[246] The First Circuit found it unnecessary to choose sides in the debate, since the alleged acquisitions by Pharmatrak were contemporaneous with the transmissions,[247] but the court noted that it was concerned about the interpretation of terms in the statute in the era of rapid development and use of technology:[248]

> We share the concern of the Ninth and Eleventh Circuits about the judicial interpretation of a statute written prior to the widespread usage of the internet and the World Wide Web in a case involving purported interceptions

233. *Id.* at 19.
234. *Id.* at 19–20.
235. *Id.* at 19.
236. *Id.* at 20.
237. *Id.* (quoting Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998)).
238. *Id.* at 20.
239. *Id.*
240. *Id.* at 21.
241. *Id.*
242. Electronic Communications Privacy Act, 18 U.S.C. § 2510(4) (2006).
243. *Pharmatrak*, 329 F.3d at 21.
244. *Id.*
245. *Id.*
246. *Id.*
247. *Id.* at 22.
248. *Id.* at 21.

> of online communications. In particular, the storage-transit dichotomy adopted by earlier courts may be less than apt to address current problems. As one court recently observed, "[T]echnology has, to some extent, overtaken language. Traveling the internet, electronic communications are often—perhaps constantly—both 'in transit' and 'in storage' simultaneously, a linguistic but not a technological paradox."[249]

The court ultimately reversed the grant of summary judgment and remanded to the district court to determine whether Pharmatrak had the requisite intent to intercept necessary for liability under the ECPA.[250]

The *Councilman* case quoted in *Pharmatrak* involved interpretation of the Wiretap Act as it existed before amendment by the ECPA.[251] The *Pharmatrak* opinion quoted the district court opinion in *Councilman*.[252] After deciding *Pharmatrak*, the district court holding in *Councilman* was appealed to the First Circuit.[253] The issue before the court was the alleged storage-transit dichotomy in the Wiretap Act.[254]

Councilman ran an online book listing service called Interloc, Inc.[255] Interloc's services included providing email services for its users.[256] Interloc gave users an email address at the interloc.com domain and acted as an email service provider.[257] Councilman was indicted for allegedly intercepting, copying, and reading incoming emails from Amazon.com before delivering those email messages to the intended recipient.[258] The messages were allegedly intercepted to give Councilman a competitive advantage.[259]

Councilman moved to dismiss the indictment for failure to state a claim under the Wiretap Act.[260] The Wiretap Act only prohibited interception of electronic communications.[261] Councilman argued that the messages in question were in electronic storage when intercepted; he further argued that communications in electronic storage were not "electronic communications" and, therefore, the interceptions did not violate the Wiretap Act.[262] The district court agreed with Councilman and granted the motion to dismiss.[263] On appeal to the First Circuit, the

249. *Id.* at 21–22 (alteration in original) (citations omitted) (quoting United States v. Councilman, 245 F. Supp. 2d 319, 321 (D. Mass. 2003)).

250. *Id.* at 22–23 (noting that the ECPA does not impose liability for inadvertent interceptions).

251. *Councilman*, 245 F. Supp. 2d at 320–21.

252. *Pharmatrak*, 329 F.3d at 21–22.

253. United States v. Councilman, 418 F.3d 67 (1st Cir. 2005).

254. *See id.* at 72.

255. *Id.* at 70.

256. *Id.*

257. *Id.*

258. *Id.*

259. *Id.* at 70–71.

260. *Id.* at 71.

261. *See id.* (citing 18 U.S.C. § 2511(1)(a)).

262. *Id.*

263. *Id.*

full court granted rehearing *en banc* after a divided panel affirmed the district court's ruling.[264]

The court began with the text of the statute.[265] Councilman argued that the plain text of the Wiretap Act exempted electronic communications that were in storage.[266] His argument relied on a comparison of the definition of "wire communication" before and after it was amended by the ECPA and the definition of "electronic communication."[267] The ECPA amended the term "wire communication" to include "any electronic storage of such communication."[268] On the other hand, the term "electronic communication" does not mention storage.[269] Comparing these terms, Councilman concluded that the "plain text" of the statute excludes electronic storage from the Wiretap Act.[270]

The court disagreed that the plain text supported Councilman's conclusion. It held that Councilman's conclusion with respect to Congress's intent was not clear from a plain reading of the statute; instead, it required an "inferential leap."[271] Unable to resolve the issue after reading the plain text and applying canons of statutory construction, the court turned to the legislative history for guidance.[272] The court found that the legislative history indicated that Congress intended to include "transient electronic storage that is intrinsic to the communication process for such communications" in the definition of "electronic communication."[273] Thus, the court rejected the distinction between "in transit" and "in storage" communications proposed by Councilman.[274]

The court then discussed the intersection of the ECPA and the SCA. The government's claim was brought under the former and Councilman argued that it should have been brought under the latter.[275] If the plaintiffs had brought their claim under the SCA, Councilman's actions could have fallen under an exception that allows service providers to view the electronic communications in some instances, such as for transferring the messages to their destination or to provide the services necessary for their users.[276] Councilman argued that if he did not violate the SCA, then he could not have violated the Wiretap Act.[277]

264. *Id.*

265. *Id.* at 72–76.

266. *Id.* at 73.

267. *Id.*

268. *Id.* (citing 18 U.S.C. § 2510(1); ECPA § 101(a)(1)(D)).

269. *Id.* (citing 18 U.S.C. § 2510(12)).

270. *Id.*

271. *Id.*

272. *Id.* at 76–79.

273. *Id.* at 79.

274. *Id.* "Indeed, we doubt that Congress contemplated the existential oddity that Councilman's interpretation creates: messages—conceded by stipulation to be electronic communications—briefly cease to be electronic communications for very short intervals, and then suddenly become electronic communications again." *Id.* at 78.

275. *Id.* at 80.

276. *Id.* at 81–82.

277. *Id.* at 82.

The First Circuit noted that previous courts had found that the overlap of statutes does not hinder a claim—the prosecution can choose which to bring a claim under.[278] Moreover, the service provider exception under the Wiretap Act is much narrower than the SCA in that it only allows for necessary interception to provide service.[279] The court held that Councilman did not fall under the Wiretap Act exception because his interception was not necessary to provide any services promised to his users.[280] This case is instructive, therefore, not only for its statutory interpretation discussion, but also because it highlights the limitations of statutes as a means of protecting online privacy. If the ambiguity in the statute had been resolved in Councilman's favor (as it was by the district court and a panel of the First Circuit), Councilman's actions—copying and reading emails intended for others—would have been legal.

States have also adopted legislation aimed at protecting privacy in general, and protecting young people from technology related threats in particular. For example, California has adopted, and is in the process of adopting, several statutes aimed at internet use and privacy. Effective since 2005, a statute known as the "Shine the Light" law[281] requires that certain businesses (including online businesses) must, upon request, reveal to a customer the third parties with which the business has shared his or her personal identifying information within the past year.[282] This could assist customers in determining if a business that they frequent was providing their names and personal information to a third party which had sent spam or junk mail to the customer.

Another California statute requires online services that collect personal data from visitors to post their privacy policy on their website.[283] New York has a similar statute, the Internet Security and Privacy Act, that requires state agencies to post privacy policies on their websites and provides elements to be included therein.[284] These elements include the following: what information will be used and how it will be used, circumstances under which collected information may be disclosed, how long the information will be retained, the procedures by which the user can obtain their information from the agency, the means by which the information is collected, the consequences for not providing the information, and the steps taken to protect the confidentiality of the information.[285] Although both of these laws inform users about how their personal information is being shared and used, nothing prevents businesses or online services from sharing the information. Consequently, instead of strengthening privacy protection, the knowledge that personal information is being shared may *decrease* subjective expectations of privacy, thereby *decreasing* Fourth Amendment protection.

278. *Id.*

279. *Id.*

280. *Id.*

281. *See generally California's "Shine the Light" Law Goes into Effect Jan. 1, 2005*, PRIVACY RIGHTS CLEARINGHOUSE (Dec. 29, 2004), www.privacyrights.org/ar/SB27Release.htm.

282. CAL. CIV. CODE §§ 1798.83–1798.84 (West 2011).

283. CAL. BUS. & PROF. CODE §§ 22575–22578 (West 2011).

284. N.Y. STATE TECH. LAW §§ 201–208 (McKinney 2011).

285. *Id.* § 203.

Utah's Government Internet Information Privacy Act[286] prevents the state government from collecting personally identifiable information on a government entity's website, unless the website contains a privacy policy statement that identifies the government operator, provides telephone and electronic contact information, identifies the information collected and how it is used, the procedures for a user to request access to the information collected, and the security measures taken to prevent unintended disclosure of personal information.[287] Presumably, if the privacy policy is posted and contains the required information, the government can collect personally identifiable information. This is particularly important in the Fourth Amendment context, since the information that is voluntarily given to the government eliminates the need for a warrant.[288]

Connecticut has enacted legislation aimed at workplace privacy.[289] An employer who engages in electronic monitoring of its employees must give them prior written notice about the types of monitoring that may occur.[290] The written notice can be posted in a place that is readily viewed by employees.[291] However, an employer can monitor without written notice if it believes that the employee is engaging in illegal activities.[292]

Delaware has a similar law.[293] It requires employers to give employees notice if they intend to monitor or intercept telephone conversations, electronic mail transmissions, or Internet access and usage. However, in Delaware, employers must give notice at least once each day that the employee accesses the employer-provided email or Internet access services.[294] In light of these laws, it may be difficult for employees whose employers have given the required notice to claim any expectation of privacy in their workplace computers, phones, or other technological devices.

VII. PROPOSED CHANGES TO THE FOURTH AMENDMENT TEST

A. Defining the Problem

Rapid advances in technology have led to litigation, legislation, and significant scholarship.[295] Despite all of this attention, there is still a great deal of uncertainty with

286. UTAH CODE ANN. §§ 63D-2-101–104 (West 2011).

287. *Id.* § 63D-2-103.

288. Other states also require government websites to post their privacy policies, including: Arizona, Arkansas, California, Colorado, Delaware, Iowa, Illinois, Maine, Maryland, Michigan, Minnesota, Montana, New York, South Carolina, Texas, Utah, and Virginia. *Privacy Policies: Government Websites*, NAT'L CONF. OF STATE LEGISLATURES, http://ncsl.org/issues-research/telecom/state-laws-related-to-internet-privacy.aspx#govpolicies (last visited May 26, 2012).

289. CONN. GEN. STAT. ANN. § 31-48d (West 2011).

290. *Id.* § 31-48d(b)(1).

291. *Id.*

292. *Id.* § 31-48d(b)(2).

293. DEL. CODE ANN. tit. 19, § 705 (West 2011).

294. *Id.* § 705(b)(1).

295. *See, e.g.*, Abril, *supra* note 80, at 78–81 (redefining tort law in the face of issues raised by online social networks); Matthew J. Hodge, *The Fourth Amendment and Privacy Issues on the "New" Internet:*

respect to privacy and Fourth Amendment protection when technology is at issue. This uncertainty persists, in part, because courts often seem unwilling or unable to address how privacy rights are affected by technology. The privacy expectations in even widely used technology such as email and various smartphone applications have not been resolved.[296]

The Supreme Court itself appears reluctant to address privacy expectations involving new technologies, in part because of its own lack of understanding and discomfort with such technology. As technology becomes an even more prevalent presence in our everyday lives (especially the lives of youth and young adults), we will be faced with greater uncertainty about our privacy rights. Living with such uncertainty forces us to choose between outdated and cumbersome modes of interaction that have been declared private and protected by the courts, and the faster, more convenient modes of interaction that may not be protected under the Fourth Amendment.

For example, attempts to completely control access to a website may be difficult or impossible, particularly websites sponsored by another website.[297] Shutterfly is a photo processing website that allows users to upload photographs.[298] The photo owner can then order prints of the photos from the site and invite others to view and order prints of the photos.[299] Shutterfly also allows users to create websites.[300] The creator can post photos and videos that have been uploaded to Shutterfly and can invite others (i.e., other participants) to view the website.[301] Only those invited by the creator can view the site; those users must have a Shutterfly account and must sign into Shutterfly with their username and password before accessing the website.[302] Such Shutterfly websites are not completely private (since all invited participants can view the

Facebook.com and MySpace.com, 31 S. ILL. U. L.J. 95, 102–05 (2006) (interpreting *Smith v. Maryland*, 442 U.S. 735 (1979) in the internet context); Brian Kane & Brett T. Delange, *A Tale of Two Internets: Web 2.0 Slices, Dices, and is Privacy Resistant*, 45 IDAHO L. REV. 317 (2009) (discussing the roles of informed parents and consumer preferences in counteracting online privacy problems); Stan Karas, *Privacy, Identity, Databases*, 52 AM. U. L. REV. 393 (2002) (analyzing technology in the context of privacy laws); Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085 (2002) (arguing in favor of recognizing a right to privacy in state constitutions); Samantha L. Miller, Note, *The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet*, 97 KY. L.J. 541 (2008) (considering self-regulation, U.S., and European law in the context of online privacy); John S. Wilson, Comment, *MySpace, Your Space, or Our Space? New Frontiers in Electronic Evidence*, 86 OR. L. REV. 1201 (2007) (considering online privacy in the context of e-discovery in litigation).

296. Some courts have addressed this issue. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that email content is protected by the Fourth Amendment). But uncertainty persists, since the responses have not been uniform and the Supreme Court has declined to weigh in.

297. *See* boyd & Ellison, *supra* note 82, at 222 (explaining the diminished control that users of social networking sites enjoy over the privacy of the personal information on their profile pages); Earp et al., *supra* note 81, at 234 (showing that privacy policies of websites often do not accord with users' privacy preferences).

298. SHUTTERFLY, http://www.shutterfly.com (last visited May 26, 2012).

299. *My Pictures*, SHUTTERFLY, http://www.shutterfly.com/nav/signedOutMyPics.sfly (last visited May 26, 2012).

300. *Share Sites*, SHUTTERFLY, http://www.shutterfly.com/sites/create/welcome.sfly?fid=1dbff8d2a7aed2cb (last visited May 26, 2012).

301. *Id.*

302. *Id.*

contents) but viewing is limited to invited participants.[303] The site is, therefore, different from a social networking site that presumes public access and requires steps to keep content private. But similar to social networking sites, the site sponsor—Shutterfly—has access to the contents of the website.[304] Moreover, Shutterfly's privacy policy notes that personal information may be shared with third parties.[305]

Shutterfly website creators and participants may use the site as a means of communication and as a way to share photos with friends and loved ones.[306] The function is similar to conversations that at one time took place through phone calls and the postal service. Instead of having a dozen copies of a photo made and mailing those copies to friends and relatives around the country, they can be posted on the website and viewed by those same persons. Thus, technology has introduced new ways of maintaining relationships and sharing intimate details of our lives. Whether the site creator or other participants have a reasonable expectation of privacy for Fourth Amendment purposes is unclear under current case law. Thus, for one concerned with privacy, the choice becomes: avoid the technology or websites or accept the risk that any expectation of privacy may not be recognized by law.

Similarly, email and social network users may know that the internet provider and some other entities have access to the account; but if the only way to maintain complete privacy is to avoid internet communication altogether, they may decide to accept compromised privacy for the sake of fast, efficient communication.[307] Avoidance may result in an inability to fully participate in an increasingly technologically oriented society. Opportunities to communicate with family, friends, and even employers may be severely limited. Many will conclude that the benefits outweigh the risks and choose to accept the limited privacy.[308]

To the extent that legislatures enact laws that define privacy rights, the subjective expectation of privacy may be easier to establish. However, if individuals, particularly younger individuals, consciously choose to make information public, or at least fail to

303. As an alternative, Shutterfly users can create a website that is open to the public, or a site that can only be accessed by those with the password. *Id.*

304. *Privacy Policy*, SHUTTERFLY, http://www.shutterfly.com/help/privacy.jsp (last visited May 26, 2012).

305. *Id.*

306. SHUTTERFLY, *supra* note 300.

307. The Stored Communications Act and other legislation may provide some protection for such hesitant users, but protection is not absolute. There are exceptions that allow for certain government searches, and it is still unclear whether or under what circumstances those exceptions might violate the Fourth Amendment. *Compare* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that email content is protected despite the fact that the service provider has access to the email), *with* City of Ontario v. Quon, 130 S. Ct. 2619, 2629–30 (2010) (insinuating a reluctance to extend to modern technology the quality of protection afforded letters and telephone conversations).

308. *Cf.* Katherine J. Strandburg, *Social Norms, Self Control, and Privacy in the Online World*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY 31, 36 (Katherine Strandburg & Daniela Stan Raicu eds., 2006) (study finding that many individuals "eventually revealed nearly as much personal information as those ostensibly less concerned with privacy," but "appeared to be much more conflicted about providing the personal information that was requested, providing it only after a period of delay"); Youn, *supra* note 93, at 104 (study suggesting that during a teenager's "risk and benefit appraisal[s]," "benefit perception was more important than risk perception in predicting [their] willingness to disclose information").

make efforts to keep it private, the subjective expectation of privacy may be absent notwithstanding such laws.

Moreover, as discussed above, younger generations have a better understanding of technology and the privacy limits when using that technology. Thus, they may have diminished privacy expectations simply because they are more knowledgeable. As they age and such knowledge becomes the norm, subjective expectations may diminish within society as a whole. It would be unfortunate if the price for greater understanding of technology was diminished Fourth Amendment protection.

The Court in *Smith v. Maryland* noted in a footnote that, in some circumstances, lack of a subjective expectation of privacy would not necessarily defeat Fourth Amendment protection.[309] The Court noted that if the federal government made a nationally televised announcement that all American homes would be subject to warrantless searches, citizens thereafter could not have a subjective expectation of privacy.[310] However, such a search would still violate the Fourth Amendment.

> In such circumstances, where an individual's subjective expectations had been "conditioned" by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a "legitimate expectation of privacy" existed in such cases, a normative inquiry would be proper.[311]

Obviously, the Court's example is extreme, but it recognizes that the subjective component of the Fourth Amendment test cannot be applied in a way that unduly diminishes Fourth Amendment protection.

In the absence of adequate legislative answers, the test for Fourth Amendment protection should change to reflect changing technology and social norms. Courts should acknowledge that technological advances have made it more difficult to maintain control over personal information and even physical spaces and adapt the subjective expectation requirement to reflect this reality.

In addition, the objective component of the Fourth Amendment test needs to be reexamined. Notwithstanding the diminished subjective expectation of privacy, society may still want to protect certain information or physical spaces from *government* intrusion, believing that the government should not be able to access their accounts and social network pages without a warrant or some recognized exception to the Fourth Amendment warrant requirement.[312] Moreover, American society is composed of many

309. Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979).

310. *Id.* The Court also gave the example of an immigrant from a country in which warrantless surveillance by the government was the norm. That person's experiences in his home country may leave him with no subjective expectation of privacy in circumstances in which most Americans would have such an expectation. *Id.*

311. *Id.*

312. Tamara Dinev et al., *Internet Privacy Concerns and Beliefs About Government Surveillance – An Empirical Investigation*, 17 J. STRATEGIC INFO. SYS. 214, 227–28 (2008); Ric Simmons, *Why 2007 Is Not like 1984: A Broader Perspective on Technology's Effect on Privacy and Fourth Amendment Jurisprudence*, 97 J. CRIM. L. & CRIMINOLOGY 531, 533–35 (2007); *cf.* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 13–16, 169–80 (2007) (describing the intrusiveness of current surveillance techniques). This may be consistent with some existing legislation that

different groups with widely varying views on privacy. Determining what "society" will accept as reasonable necessarily requires valuing or affirming one group's views over another's. This makes applying the current Fourth Amendment test difficult at best and inconsistent at worst.

B. A Proposed Solution

This Article proposes a modestly revised test for Fourth Amendment protection that reflects changes in society and our evolving notions of privacy. Specifically, the test asks: (1) whether a person has taken steps to reasonably limit access to the information or place targeted for search or seizure; and (2) if so, whether society is prepared to protect the information or space from unreasonable government intrusion.

Instead of asking whether a person believes that the place or information sought is completely private or "secret,"[313] the first inquiry seeks to determine whether access to the place or information has been reasonably limited. In other words, it acknowledges that some people may have been given or obtained access without destroying Fourth Amendment protection, particularly those who facilitate the communication. In the case of internet communications, a user may know that a website or social network communication may be viewed by several parties, including the service provider and others involved in the transmission process, yet the court could find that the user is entitled to Fourth Amendment protection.

Although the user cannot reasonably prevent *everyone* from obtaining access to the account or site, the user can take steps to protect the communications from *most* other persons. If the user password-protects the website and does not give the password out to anyone else, or attempts to limit access using the privacy settings available on the social network site, the first part of the new test may be satisfied. If, on the other hand, the user does not use a password, widely distributes the password, or logs on to the social network account from a public computer and leaves messages on the screen where they can be viewed and read by a large group of people, that user may be found to have failed to reasonably limit access and, consequently, forfeit Fourth Amendment protection. Similarly, a social network user who accepts the default "public" settings and makes no attempt to limit access to his or her page or communications may not claim Fourth Amendment protection.[314]

This new inquiry is similar to the current test and will not lead to new results in many cases. For instance, courts have consistently found letters delivered through the mail and the content of phone calls protected by the Fourth Amendment even though intermediaries—mail carriers and the telephone company—could open and read a letter

could be read to protect a subjective expectation of privacy when it comes to government searches and seizures, but the test would allow the court to find Fourth Amendment protection even if the existing legislation does not cover a particular circumstance. Thus, the protection would exist for new technologies or applications and would eliminate the delay between innovation and legislation.

313. *See Smith*, 442 U.S. at 743 ("Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.").

314. *Cf. id.* at 743–44.

or listen in on a phone call.[315] Likewise, the Sixth Circuit has held that email content is protected notwithstanding the internet service provider's ability to read the content.[316] Thus, the new test simply makes explicit what courts have already recognized in many instances.

The new inquiry does have the potential to expand protection beyond what is currently available, depending upon what courts deem to be "reasonably limited access." The test could be read broadly to allow individuals to disclose information to large segments of the public while denying access to the government. This is not the intent, nor is it likely that courts would so interpret it. Instead, although the facts of each case will determine what is reasonable, the wider and less discriminating the distribution, the less likely it is to be protected. The nature of the communication will also be relevant. A website disclosing personal information that is shared with dozens of family members may be protected, while a website that allows anyone to have access upon request may not be protected even if only a few people have actually visited the site.

The value in reframing the first part of the Fourth Amendment test is its ability to address and adapt to new circumstances, including new technologies. The current subjective portion of the test is better suited to a conceptualization of privacy based on protection of physical spaces and information reduced to a tangible form. It is less effective with respect to information transmitted or shared using electronic media or in light of changing notions of "privacy." Moreover, it punishes those who recognize that little, if anything, is truly private when communicated or stored using the most prevalent forms of technology. Because these more knowledgeable (and often younger) persons do not have a subjective expectation of privacy, the current test precludes Fourth Amendment protection. Those ignorant of the privacy risks are more likely to be protected.

The second part of the proposed test modifies the old test by focusing on society's willingness to protect the place or information from government intrusion rather than asking whether society believes that some information or some place is properly considered "private" for all purposes. Courts will still need to evaluate "society's" willingness to grant the government access to certain places or information, but this does not pose a new challenge. Instead, it simply narrows the focus of the current objective inquiry. Under the current test, courts focus on the privacy expectation of the search or seizure target and ask whether society accepts the subjective expectation as reasonable. The proposed test asks whether society accepts the right to protect the search or seizure target from government intrusion in light of the target's attempts to limit access to the place or information. Courts may acknowledge the reality that keeping anything, particularly electronic communications, truly private may be impossible, but also recognize that stripping all Fourth Amendment protection when communications are not completely private is an unreasonable response to a new reality.

This distinction may not entirely eliminate the age gap with respect to Fourth Amendment protection, but it may substantially close the gap since even younger

315. *E.g.*, United States v. Warshak, 631 F.3d 266, 285 (6th Cir. 2010).

316. *Id.* at 285–88.

generations desire to protect some information from certain groups of people. Their focus may be on providing access to friends while wanting to protect it from parents and teachers, but the mere fact that they want and attempt to limit access to certain personal information shows an understanding that information or places can be considered private even if it is known to persons other than oneself. As they age, they may agree that information provided to businesses or friends online should not be available to the government without a warrant or some exception to the warrant requirement. At the least, this new test would not require courts to consider only one perspective on privacy when assessing Fourth Amendment protection.

This second inquiry can be criticized to the extent that it appears to allow people to receive Fourth Amendment protection while giving access to everyone except the government. This, however, ignores the first part of the test, which requires reasonable limitation of access. The test should be applied in a way that reflects the function that electronic and wireless communications serve in today's society and grants such communications protection similar to that given to modes of communication that were used before modern technology existed. The second inquiry builds on the first by focusing on the content of the communication or character of the place targeted. Even information that is displayed or accessible to only one or two people may not be protected if the content is such that most people would not consider granting government access unreasonable. For example, a website that is intended to promote criminal activity is not one that society would be willing to protect from government intrusion.

Social networking sites provide a useful example of how courts might apply the proposed test. A person who maintains a Facebook profile may post personal pictures and information. If the user accepts the default privacy settings, the postings will be available to anyone who has a Facebook account. A court could appropriately hold that the user has not taken reasonable steps to protect the information posted on the Facebook profile. Consequently, the Fourth Amendment would not protect the information from a government search. Likewise, a user with thousands of "friends," many of whom have no personal connection with the user, may not be protected. If, on the other hand, the user changed the profile settings so that only those designated as "friends" had access to the profile, and only a dozen people were "friends" of the user, a court could find that the user has taken steps to reasonably limit access to the information. The Facebook page could be protected under the revised test, even though it would likely fail the current "subjective expectation of privacy" test. This is particularly true if the user—like many young users—does not consider the Facebook page to be truly private.

The court would then have to determine whether society is willing to protect the information from government intrusion. This inquiry allows the court to consider how society views social networking sites in general and Facebook in particular. The court can consider how popular the site has become with persons of all ages and its utility in allowing people to maintain contact over large distances in a way that is not possible with written correspondence. To the extent that a Facebook page serves the purpose formerly filled by written or telephone correspondence, the court might conclude that society is willing to protect such information from government intrusion. If the court views it as a quasi-public forum intended to distribute instead of hide information, as

may be the case for some individual and all business users, then the site content may not be protected.

This test should not expand protection dramatically. For example, the existence of the profile may not be protected from disclosure if that profile can be found by anyone, even though the content may be protected if access to the content is restricted to a smaller group of users. This distinction would be akin to the protection afforded to the content of phone or mail communications, while leaving unprotected the addressee of a letter or the phone number called. If, however, the profile could not be seen by the general public (so that its existence is kept private), the proposed test could provide more protection than currently exists; the existing test could find no subjective expectation of privacy with respect to the existence of the profile since information would have to be disclosed to the site sponsors in order to set up the site.

Between the extremes of users who make their profiles available to everyone and those who limit access to very few are, perhaps, the majority of users, whose settings allow for more than just "friends" to have access but restrict access to less than the entire Facebook population.[317] The proposed test is flexible enough to allow the courts to evaluate each case on its own facts. The test also allows for evolution of technology and expanded use of existing technology.

VIII. CONCLUSION

Society changes as technology changes. The lives of children today are shaped by access to technology that allows instant, affordable communication with people all over the world. Instead of face-to-face interactions, they develop and sustain relationships electronically. Information on any number of subjects is available whenever and wherever a person has access to a computer or even a cell phone. Their perceptions of privacy are necessarily influenced by their ability to share information quickly and easily with large groups of people. Specifically, research suggests that youth today have a diminished expectation of privacy as compared to their elder counterparts. Their diminished expectations can affect the Fourth Amendment protections afforded to everyone. To counter this trend, this Article proposes a revised test for Fourth Amendment protection that eliminates the need for a subjective expectation of complete privacy, and only requires the courts to inquire whether society is prepared to protect the information or space from government intrusion. The new test reflects the reality that little is truly private in this electronic age, yet the Fourth Amendment should not be rendered obsolete.

317. Courts may also find no Fourth Amendment protection if access is limited to "friends" but the user's friends number in the tens of thousands and include many people that the users has never met.