REASONABLE EXPECTATIONS OF PRIVACY FOR YOUTH IN A DIGITAL AGE

Mary Graw Leary[*]

> The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment . . . . The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.[1]

INTRODUCTION

"Technology is changing everything." This often repeated claim is made in so many contexts that it has become a cliché, but like many clichés, it is often true. Perhaps its impact is greatest with regard to what Brandeis and Warren, in their seminal 1890 Harvard Law Review article, described as the most fundamental right: the right to be left alone. We see technology's effect on that "right" in criminal litigation. Here courts struggle to apply the basic rule that the Fourth Amendment protects only reasonable expectations of privacy. However, the electronic erosion of privacy in everyday life cannot help but impact which expectations of privacy remain reasonable. This is compounded by the fact that many people in their teens and twenties arguably approach privacy differently than their older counterparts, some choosing to expose their thoughts, activities, and images to the inquisitive eyes of friends, acquaintances, and even strangers. Consider: 93% of American homes

[*] Associate Professor, The Catholic University of America, Columbus School of Law. Special thanks to Thomas Clancy, Cliff Fishman, and Anne McKenna for their insight and comments. Thanks to Julie Kendrick for countless drafts and to Kristen Kelley for diligent research.

[1] City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010).

have computers and 84% of them have Internet access;[2] 66-71% of youth aged 8-18 own their own cell phones,[3] many of which have Internet access where youth engage in the most popular Internet activity, interacting with social networking.[4] On social networking sites, 64% of online 12-to-17-year-olds are not only obtaining content but creating and sharing it in the form of online journals, blogs, photo and video sharing.[5] As such activities become the norm, query what expectations of privacy remain reasonable. This is particularly apparent when one focuses on a subset of the population that has grown up in this new world order: youth.[6]

---

[2] VICTORIA J. RIDEOUT ET AL., KAISER FAMILY FOUNDATION, GENERATION M2: MEDIA IN THE LIVES OF 8- TO 18-YEAR-OLDS, at 21 (2010); *see also* SONIA LIVINGSTONE & MAGDALENA BOBER, ECONOMIC AND SOCIAL RESEARCH COUNCIL, UK CHILDREN GO ONLINE 8 (2005) (finding that in 2005, 75% of 9- to 19-year-olds access the Internet from a home computer, game console, or digital television).

[3] RIDEOUT ET AL., *supra* note 2, at 3, 18; AMANDA LENHART, PEW INTERNET & AMERICAN LIFE PROJECT, TEENS AND MOBILE PHONES OVER THE PAST FIVE YEARS: PEW INTERNET LOOKS BACK 4 (2009).

[4] RIDEOUT ET AL., *supra* note 2, at 21; HARRY NEWTON, NEWTON'S TELECOM DICTIONARY 1032-33 (25th ed. 2009) (defining social networking as "a website with a big database of information about people and their interests" characterized by the ability to create a personal profile, share photos or blogs, receive messages, limit it to a circle of friends, or open it to the public).

[5] AMANDA LENHART ET AL., PEW INTERNET & AMERICAN LIFE PROJECT, TEENS AND SOCIAL MEDIA: THE USE OF SOCIAL MEDIA GAINS A GREATER FOOTHOLD IN TEEN LIFE AS THEY EMBRACE THE CONVERSATIONAL NATURE OF INTERACTIVE ONLINE MEDIA 2, 4, 12 (2007).

[6] "Youth" is a general term. Some refer to this subset as, *inter alia*, "minors," "digital natives," or "teens." JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES 346 (2008) (defining digital native as a person born in the digital age (post 1980) who has access to networked technologies, with strong computer skills and knowledge); 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 (2008) (teenagers); MIZUKO ITO ET AL., JOHN D. & CATHERINE T. MACARTHUR FOUNDATION, LIVING AND LEARNING WITH NEW MEDIA: SUMMARY FINDINGS FROM THE DIGITAL YOUTH PROJECT 4 (2008) (youth). Because technology is so dynamic, trends among youth are so variable, and scholarship is so diverse in its demographic focus, no term is sufficient. The author adopts the imperfect terms "youth" or "digital native" to refer to the generation of technically connected young people who were born into a digitally connected norm, after the early 1990's when the Internet became a commercially available system used by the general public. *See, e.g.*, Indep. Newspapers, Inc. v. Brodie, 966 A.2d 432, 438 (Md. 2009). However, as discussed *infra* Part II C, for legal analysis, the article focuses on a subset of youth—public school students—as they

In this digital age, individuals and society as a whole struggle to balance the advantages of digital connectivity against the reality that this very connectivity inevitably gives others access, licitly or illicitly, to private information.[7] While risks to privacy are certainly not limited to youth, an argument can be made that conceptualizations of privacy for those who have grown up with this technology are unique. One could further argue that as a group, youth possibly demonstrate distinct expectations of privacy when compared with older generations.[8] This article concerns the intersection of youth, technology, expectations of privacy, and the Fourth Amendment. More specifically, the article examines whether this "norm" of increased information disclosure, which can be characterized as conditioned, combined with decreased privacy rights in certain contexts effectively strips or compromises the Fourth Amendment protections of a class of people—youth.

It may be too early to fully measure technology's effect on privacy expectations of society as a whole. By focusing on a subset of society—youth—some of the questions are more manageably explored. By specifically examining students, and the reality that youth, as a group, may have a different concept of privacy online, this article seeks to explore a Fourth Amendment issue never before faced. What is society to do when a large subset of citizens, as a result of social or technological

present the most pressing legal concerns due to the developed case law decreasing their privacy rights in a school setting.

[7] *See generally* MARY MADDEN ET AL., PEW INTERNET & AMERICAN LIFE PROJECT, DIGITAL FOOTPRINTS: ONLINE IDENTITY MANAGEMENT AND SEARCH IN THE AGE OF TRANSPARENCY 1 (2007); MARY MADDEN & ADAM SMITH, PEW INTERNET & AMERICAN LIFE PROJECT, REPUTATION MANAGEMENT AND SOCIAL MEDIA (2010); *see also* PALFREY & GASSER, *supra* note 6, at 23 ("Young people—among many others—are using the Internet to share more personal information about themselves than ever before.").

[8] *See*, *e.g.*, PALFREY & GASSER, *supra* note 6, at 7 ("Digital Natives' ideas about privacy . . . are different from those of their parents and grandparents."); Press Release, PR Newswire, What is Privacy? Poll Exposes Generational Divide on Expectations of Privacy, According to Zogby/Cong. Internet Caucus Advisory Comm. Survey (Jan. 30, 2007), http://www.prnewswire.com/news-releases/what-is-privacy-poll-exposes-generational-divide-on-expectations-of-privacy-according-to-zogbycongressional-Internet-caucus-advisory-committee-survey-54015452.html ("[A] vast chasm exists between what 18-24 year-olds believe is an invasion of privacy and what other Americans consider to be an intrusion.").

conditioning and not government action, demonstrates an arguably lesser expectation of privacy? Part I of this article examines data regarding digital natives and their interaction with current technologies. Part II reviews current law regarding expectations of privacy in general, under the *Katz* test,[9] and more specifically, for public school students, under *New Jersey v. T.L.O.*[10] and *Safford Unified School District v. Redding*.[11] The article further reviews what guidance the Court has offered in situations where the familiar two-pronged *Katz* test is not useful. Part III reviews possible solutions to this problem, calling into question the utility of the *Katz* test. The article explores whether a more value-laden approach outlined by Justice Harlan in his dissent in *United States v. White* may offer a more promising solution than the traditional *Katz* analysis. Because the jurisprudence addressing searches of public school students in a school setting is developing, Part IV applies the different approaches offered by the Court to a hypothetical modification of the facts in *Redding*. In *Redding*, the Supreme Court held that when school officials conducted a virtual strip search of a teenage girl to investigate allegations that she possessed ibuprofen, they violated the girl's Fourth Amendment protection against unreasonable searches.[12] Suppose instead of the virtual strip search, school officials had seized her cell phone and examined its digital contents. This article explores that scenario and concludes that, for several reasons, the Supreme Court's current approach to applying the Fourth Amendment (often referred to as the "reasonable expectation of privacy" approach) is inadequate to sufficiently address the issues presented in this all-too-common scenario. It further argues that the proposal of Justice Harlan in *White* may be the pathway out of the problem.

---

[9] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The "*Katz* test" refers to the two-pronged test proposed in Justice Harlan's *Katz* concurrence and later adopted in full by the Court.

[10] New Jersey v. T.L.O., 469 U.S. 325 (1985).

[11] Safford Unified Sch. Dist. #1 v. Redding, 129 S. Ct. 2633 (2009).

[12] *See infra,* note 134.

I. YOUTH, TECHNOLOGY, AND THE INTERNET

A. Youth and Technology

Much discussion is occurring regarding online activity's ability to compromise the user's privacy, regardless of his or her age. Indiscriminate sharing of information or ignorance of vulnerabilities are not activities limited to youth.[13] However, significant discussion is also taking place about the digital divide between older and younger generations.[14] It has been suggested that many people can roughly be categorized into two groups: "digital natives," i.e., those who were born and grew up in a post-commercialization of the World Wide Web, and "digital immigrants," i.e., those who have had to assimilate to a post-World Wide Web universe.[15] This divide manifests itself in

---

[13] MADDEN ET AL., *supra* note 7, at ii (Forty-three percent of online adults "neither worry about their personal information nor take steps to limit the amount of information that can be found out about them online."). MADDEN & SMITH, *supra* note 7, at 2 (noting that some Internet users are careful in how they project themselves online. Others "embrace an open approach" and "do not restrict what they share.").

[14] *See*, *e.g.*, SYDNEY JONES & SUSANNAH FOX, PEW INTERNET & AMERICAN LIFE PROJECT, PEW INTERNET PROJECT DATA MEMO: GENERATIONS ONLINE IN 2009, at 1-2, 5 (2009); *see also* MADDEN ET AL., *supra* note 7, at 20; PALFREY & GASSER, *supra* note 6, at 109, 125, 131 (discussing the technology gap between young people and many of their parents).

> Digital media and online communication have become pervasive in the lives of youth in the United States. Social network sites, online games, video-sharing sites, and gadgets such as iPods and mobile phones are now fixtures of youth culture. . . . [L]ess than a decade ago these technologies had barely registered in the lives of U.S. children and teens.

ITO ET AL., *supra* note 6, at 4; *see also id.* at 36. However, scholars caution against an assumption that youth are unconcerned with privacy. *See generally* Susan C. Herring, *Questioning the Generational Divide: Technological Exoticism and Adult Constructions of Online Youth Identity*, *in* YOUTH, IDENTITY & DIGITAL MEDIA 71, 86 (David Buckingham ed., 2008); *see also Protecting Youths in an Online World*: *Hearing Before the Subcomm. on Consumer Prot., Prod. Safety, and Ins. Comm. on Commerce, Sci., and Transp.*, 111th Cong. 2-5 (2010) (prepared statement of the Federal Trade Comm'n); danah boyd & Eszter Hargittai, *Facebook Privacy Settings: Who Cares?*, FIRST MONDAY, Aug. 2, 2010, at 2.

[15] *E.g.*, NEWTON, *supra* note 4, at 369 (referencing a 2005 Rupert Murdoch speech describing one who came to the Internet later in life as a "digital immigrant"); Herring, *supra* note 14, at 71 ("Children born in the mid- to late-1980s and the 1990s have been labeled the 'Internet Generation': the first generation to grow up in a world where the

a number of ways. This article will focus on one of those data points: youth and their expectation of privacy regarding media use. By "media use" this article speaks generally about the interconnectivity of the technological devices that allow for the consumption and creation of Internet content.[16] Technology is arguably reshaping social norms for young people, who are more likely than older citizens to read blogs, write their own blogs,[17] use social networking sites,[18] create personal profiles on those sites, update friends about their lives, or keep track of and communicate with friends on the Internet.[19] Prior to discussing the ramifications of this on privacy expectations, this article will review what is known about youth and their consumption and creation of content through media.[20]

Internet was always present." This generation is also called the "Net Generation," the "Net-Gen," "Generation i," the "Digital Generation," or the "Millenials.").

[16] *See* RIDEOUT ET AL., *supra* note 2, at 2, 10 (tracking media use such as the watching of television programming on a variety of platforms, listening to music, using computers, playing video games, reading print, or watching movies).

[17] "The word *blog*, used as a noun, is a contraction of the words *Web* and *Log* and generally describes a site that 'contains dated text entries in reverse chronological order (most recent first) about a particular topic.' (citation omitted). A blog can serve as an online newsletter or as a personal journal—where an individual can post concerns, ideas, opinions, etc.—and it can contain links to web sites or can use images or video." Indep. Newspapers v. Brodie, 966 A.2d 432, 437 (Md. 2009); *see also* NEWTON, *supra* note 4, at 197.

[18] Social Networking sites are defined as "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system." danah m. boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMM. 2 (2007). boyd prefers the term "social network sites" because participants do not network as much as communicate with people already part of their network. *Id.*; *see also* PALFREY & GASSER, *supra* note 6, at 350 (defining "social networking sites" as "a site . . . that connects . . . people in order to enable the flow of information among users"). Scholarship utilizes both terms as will this article. The MacArthur Foundation Report uses the term "networked publics" to "describe participation in public culture that is supported by online networks." ITO ET AL., *supra* note 6, at 10.

[19] JONES & FOX, *supra* note 14, at 3.

[20] Of course, one should be cautious about over-generalization. No subset of society can be indiscriminately grouped under one label as acting uniformly. What follows is a collection of general trends. Certainly within the imperfect label "youth," *see supra* note 6, there are individual behaviors outside of these trends and many factors (access to technology, chief among them) contribute to practices. *See* Alice Marwick, Diego

Two aspects of youth participation with the Internet are relevant to the privacy discussion. These include first, the number of different platforms through which youth are accessing the Internet, and second, their online activities that include both media consumption and content creation.

Media use is no longer limited to any one platform, such as the television or the computer. The explosion of mobile media and its access to the Internet has fueled an increase in both media consumption and content creation.[21] The Kaiser Foundation found that young people spend an average of 7:38 hours a day "using media," excluding computer use for schoolwork.[22] "Media use" encompasses television content, music, video games, print, movies, and the Internet.[23] This amount of time represents a significant increase, in the past five years, of all forms of media use with the exception of reading.[24] The increase of the availability and use of mobile and online media has fueled this growth with "[t]he vast majority of young people now carry[ing] devices on which they listen to music and in many cases connect to the Internet and watch videos."[25] This transformation of the cell phone from a telephone into a media content delivery platform facilitated the "explosion in media consumption among America's youth."[26]

Murgia Diaz, & John Palfrey, *Youth, Privacy and Reputation* 12-21 (Berkman Ctr. Research, Publ'n No. 2010-5 & Harvard Pub. Law, Working Paper No. 10-29, 2010), *available at* http://ssrn.com/abstract=1588163; *cf.* MADDEN & SMITH, *supra* note 7.

[21] RIDEOUT ET AL., *supra* note 2, at 2-3. Cell phone ownership grew among teens from 39% to 66% in just five years. *Id.* at 3, 10, 18. The Pew Center reports that 71% of teens own cell phones, with 84% of 17-year-olds doing so. LENHART, *supra* note 3, at 7-8.

[22] RIDEOUT ET AL., *supra* note 2, at 2. If one were to include multi-tasking among different forms of media separately, then the total time would rise to 10:45. *Id.* at 4.

[23] *Id.* at 2, 6-7, 10. In another study, students in seventh, eighth and ninth grades reported spending an average of 21 hours per week engaged in "various online activities." SAMUEL C. MCQUADE, III & NEEL SAMPAT, ROCHESTER INSTITUTE OF TECHNOLOGY, SURVEY OF INTERNET AND AT-RISK BEHAVIORS 29, 31 (2008).

[24] RIDEOUT ET AL., *supra* note 2, at 2.

[25] *Id.* at 3.

[26] *Id.* at 3, 18; LENHART, *supra* note 3, at 8 (cell phone is the dominant form of communication for teens); MCQUADE & SAMPAT, *supra* note 23, at 28 (as students get older, devices are increasingly used for interactive communication). Cell phones are no longer simply devices with which to speak to others, but "have morphed from a way to hold a conversation with someone to a way to consume more media." RIDEOUT ET AL.,

This increase in platforms provides youth with more varied ways not only to consume, but to create content and share information. This reality directly affects what young people perceive as private. For example, computers used to be necessary in order to engage in the most popular computer activity—interacting within social networking sites.[27] Now, with most cell phones having Internet connectivity, this activity can be done from multiple platforms and locations. One can take a picture or video, update his or her location, notify contacts, a.k.a. "Friends," "fans," or contacts,[28] and post the picture or video on the Web without ever sitting down at a computer.[29]

An important aspect of media use is content creation. It is here, at the social networking site, as well as other fora, in which content creation occurs and has the potential to signifi-

supra note 2, at 3; *see also* AARON SMITH, PEW INTERNET & AMERICAN LIFE PROJECT, MOBILE ACCESS 2010, at 2 (2010), *available at* http://www.pewinternet.org/~/media//Files/Reports/2010/PIP_Mobile_Access_2010.pdf (noting the growth of the use of non-voice data applications on cell phones). For example, one study reports seventh to twelfth graders spend an average of 90 minutes per day sending an average of 118 text messages. RIDEOUT ET AL., *supra* note 2, at 18.

[27] RIDEOUT ET AL., *supra* note 2, at 21 (noting that 25% of seventh to twelfth graders' recreational time is spent on social networking sites, and 15% watching videos on YouTube-type web sites).

[28] Following the lead of Professor Grimmelmann, this article will use the term "'contact' to describe a user with whom one has an explicit link on a social network site." James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1143 (2009). The label given to one's network of contacts will be used generally, or with respect to Facebook "Friends" as distinct from the colloquial "friends." "Friends" are people within a social networking site who enjoy privileges such as being able to view one's profile or other information. PALFREY & GASSER, *supra* note 6, at 347.

[29] *See* ITO ET AL., *supra* note 6, at 26 ("[P]ersonal photos . . . are readily available in social contexts mean[ing] that visual media become more deeply embedded in the everyday communication of young people."). Much social networking time is spent both creating content and exploring that of others. The numbers participating in this are staggering, with Facebook claiming to have more than 500 million active users who produce 60 million status updates per day, upload 3 billion photos each month, and share 530 billion pieces of content each week. *Press Room: Statistics*, FACEBOOK, http://www.facebook.com/press/info.php?statistics (last visited Jan. 21, 2011). Additionally, MySpace claims to have more than 100 million active users. Gregory Spizer, *Understanding of Social Media Intrinsic to Modern League Practice*, 241 LEGAL INTELLIGENCER 5 (2010). Teens joined MySpace *en masse* in 2004, and most teens with profiles have them on MySpace. boyd & Ellison, *supra* note 18, at 7; AMANDA LENHART & MARY MADDEN, PEW INTERNET & AMERICAN LIFE PROJECT, PEW INTERNET PROJECT DATA MEMO: SOCIAL NETWORKING WEBSITES AND TEENS: AN OVERVIEW 1-2 (2007).

cantly implicate privacy. Sixty-four percent of youth online between the ages of 12 and 17 have participated in creating content by sharing photographs, stories, video, and art; creating or working on web pages or blogs for themselves or for others; and creating an online journal or maintaining their own web page.[30] This may initially appear merely as a new way for youth to communicate and, therefore, raises no more privacy implications than the adoption of the telephone. However, youth's sense of the private nature of this material is remarkable and has created some concern. Social network sites require the member to post a profile replete with personal information. For example, "[a] fully filled-out Facebook profile contains about forty [data points of] personal information, including . . . religious views[,] . . . contact information[,] . . . [and] sexual preference," all information previously considered by the law as personal.[31] Their social networking pages can contain personal information about their location, plans, associates, much like a personal diary and address book, simply all online. Blog creation or commentary doubled between 2004 and 2006.[32] Forty-seven percent of online teens have uploaded pictures where others can see them, and 14-25% have posted videos.[33] While a minority of teens (21%) consistently shares photos without re-

[30] Thirty-nine percent share photos, stories, and art; 33% create work on blogs and web pages for others; 28% create their own journal; 27% maintain their own web page, and 26% remix content to create their own. LENHART ET AL., *supra* note 5, at i, 34; *see also* Livingstone, *supra* note 6, at 4 ("[M]ore than ever before using media means creating as well as receiving."). Girls are more active in content creation, with 55% of such creators being girls. LENHART ET AL., *supra* note 5, at 4; *see also* MADDEN ET AL., *supra* note 7, at 19 (reporting in 2007 that 33% of adult Internet users post creative content online and 36% upload photos, while 47% of teens do so).

[31] Grimmelmann, *supra* note 28, at 1149-51 (listing all information available on a Facebook profile and how it is used); *see also* DAVID KIRKPATRICK, THE FACEBOOK EFFECT: THE INSIDE STORY OF THE COMPANY THAT IS CONNECTING THE WORLD 201 (2010) ("Many users willingly fill out extensive details about their career, relationships, interests, and personal 'history.'").

[32] LENHART ET AL., *supra* note 5, at ii, 8. Additionally, four out of five social networking users posted messages on a wall (89% of girls and 79% of boys). LENHART & MADDEN, *supra* note 29, at 6.

[33] LENHART ET AL., *supra* note 5, at i, ii, 14 (14%), 13 (47%); RIDEOUT ET AL., *supra* note 2, at 22 (25%). This is in contrast to 8% of adult Internet users. MADDEN ET AL., *supra* note 7, at 19.

strictions, only 38% restrict access "most of the time."[34] However, "for the most part, teens who post video files want them to be seen," with 46% of video posters reporting they never restrict access to videos.[35]

> The vast array of data points that make up "personal information" in the age of online media are nearly impossible to quantify or neatly define. Name, address, and phone number are just the basics in a world where voluntarily posting self-authored content such as text, photos, and video has become a cornerstone of engagement in the era of the participatory Web. The more content we contribute voluntarily to the public or semi-public corners of the Web, the more we are not only findable, but also knowable.[36]

Additionally, social networking sites offer various avenues to communicate, such as private messages, messages posted on friends' web pages, or comments on others' blogs to name a few.[37]

B. Online Youth and Privacy

Recent scholarship stresses that while digital natives may conceptualize privacy differently, that does not translate into devaluing privacy.[38] Despite a media panic, much research indicates youth use this new media more to reach out to friends with whom they usually socialize than to be in contact with adult strangers.[39] When asked about their attitudes toward

---

[34] LENHART ET AL., *supra* note 5, at iii, 14.

[35] *Id.*

[36] MADDEN ET AL., *supra* note 7, at i.

[37] LENHART & MADDEN, *supra* note 29, at 6. Ninety-one percent of youth who use social networking use it to stay in touch with friends they see frequently and 72% do so to schedule or coordinate with friends. *Id.* at 2, 6. Twenty-six percent of youth send messages (email or Instant Messages ("IM")) through social networks. Also, of all of the youth who use social networks, 54% send IM or texts through such sites. LENHART ET AL., *supra* note 5, at 8, 12.

[38] *See, e.g.*, Marwick et al., *supra* note 20, at 60; ITO ET AL., *supra* note 6; MADDEN & SMITH, *supra* note 7; boyd & Hargittai, *supra* note 14.

[39] ITO ET AL., *supra* note 6, at 26; Livingstone, *supra* note 6, at 4-5 (referring to a "media panic" that "amplif[ies] public anxieties" associated with social networking and that teenagers have "no sense of privacy or shame").

privacy, youth express a concern about both corporate access and social access to personal information.[40] Indeed, Livingstone suggests that the distinction between youth and older citizens is not a lack of concern about privacy but a different definition of privacy in which young people define it without regard to the types of information revealed, but rather, regarding control over who learns the information.[41]

While research does support a notion that youth and young adults care about privacy, and are at times more active in managing their online reputation than older users, it also supports that such attitudes do not always translate into practices that protect privacy.[42] For example, a study comparing young adults' privacy attitudes and actions within social networks found a "dichotomy between [Facebook] members' stated privacy concerns (high) and actual information hiding strategies" due to peer pressure, unawareness, and a level of trust toward Facebook.[43] While youth appear to recognize the vulnerability of private information disclosed to peers who might forward that information to others, some scholarship suggests

---

[40] Chris Hoofnagle et al., *How Different Are Young Adults From Older Adults When It Comes To Information Privacy Attitudes and Policies*, SSRN Research Paper 3, 12 (Apr. 14, 2010), *available at* http://ssrn.com/abstract=1589864 (finding that when young adults were asked about attitudes regarding collection and use of personal information, their response did not differ greatly from adults); Allessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook* (PET 2006) (similar study of university community members found attitudinal concern).

[41] Livingstone, *supra* note 6, at 10; MADDEN & SMITH, *supra* note 7, at 5-6 (noting the debate among scholars and the argument that Internet users sensitivity to privacy concerns are "highly dependent on context" and often "oversimplified."). Marwick et al., *supra* note 20, at 60-61. Defining and conceptualizing privacy is a herculean task. For a thoughtful discussion of various conceptualizations of privacy, and their critiques, see DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 14-38 (2008).

[42] boyd & Hargittai, *supra* note 14, at 2 (noting that research suggests that young adults (18- to 29-year-olds) are conscious of privacy issues and more actively manage the access to profiles; but acknowledging a lack of information regarding the extent to which these changes meet their privacy preferences). Hoofnagle et al., *supra* note 40, at 17-18 (finding differences between attitudes regarding collection of personal data and the practices of protecting such personal data); Acquisti & Gross, *supra* note 40.

[43] Acquisti & Gross, *supra* note 40, at 13, 17; *see also* Livingstone, *supra* note 6, at 10-11 (teenagers' primary goal is not to hide information from strangers, but to share private experiences with friends).

they are arguably (or seem to be) less aware of the fact that their online activities expose private information to the world at large.[44] The picture is not clear, however. Research among young adults suggests an emerging landscape in which those 18-29 year olds who are more skilled and engaged on social networking sites are more likely to modify their profile and manage their reputation.[45]

"The divergence in privacy norms between heavily wired teens and their parents (to say nothing of their grandparents) is striking; the personal information *already* online would suffice to ruin the political careers of millions of young people if they were judged by the standards we apply to adult politicians."[46] One-third of online teens display personal information with no limitations at all.[47] Moreover, the remaining two-thirds only limit it "in some way."[48] This may reflect in some cases actual and effective limits, but in other cases, minimal limits such as only allowing "only contacts" to view their information,

[44] On the one hand, the Pew Center reports "fewer communications are private anymore . . . [and] the most commonly experienced bullying is having someone take a private email, IM, or text message, and forward it to someone else or post it publicly." AMANDA LENHART, PEW INTERNET & AMERICAN LIFE PROJECT, CYBERBULLYING AND ONLINE TEENS 2-3 (2007); *see also* MCQUADE & SAMPAT, *supra* note 23, at 13, 16, 27 (noting that students are more likely to be victimized, including hacking and bullying, by other students whom they know); boyd & Hargittai, *supra* note 14 (calling for more research on the alignment and between preferences and practices). Notwithstanding this, scholars observe that the "backbone" of social networking sites remains the "visible profiles that display an articulated list of Friends who are also users of the system." boyd & Ellison, *supra* note 18, at 2; *see also* MADDEN & SMITH, *supra* note 7, at 6 (discussing how young adults online are more active online managers of reputation, but many adults take the "path of least resistance" in managing their reputation online).

[45] boyd & Hargittai, *supra* note 14, at 18, 20, 25; MADDEN & SMITH, *supra* note 7.

[46] Emily Nussbaum, *Say Everything*, N.Y. MAG., Feb. 12, 2007, at 24 ("More young people are putting more personal information out in public than any older person ever would—and yet they seem mysteriously healthy and normal, save for an entirely different definition of privacy.").

[47] In fact, 77% of teens who create a profile say it is visible online. LENHART & MADDEN, *supra* note 29, at 5. Although a comparable percentage of adults (82%) report the same, a much larger percentage of youth (55% and 20% of adults) have profiles. MADDEN ET AL., *supra* note 7, at 20.

[48] LENHART & MADDEN, *supra* note 29, at 5; LENHART ET AL., *supra* note 5, at 13; MADDEN ET AL., *supra* note 7, at 20.

but then accepting any request to be a contact, thus exposing their private information to large numbers of people.[49]

One may wonder why people, particularly young people, compromise their privacy so extensively through social networking sites. Some scholars believe that users need to perceive a benefit in exchange for privacy disclosure risks. Grimmelmann argues that social networking sites offer three important motivators: identity, relationship, and community.[50] The Internet allows one to create an identity, to advertise it to develop relationships (some fleeting), and to establish oneself as a leader in a given community. Disclosure of information, for example, compiling a large number of contacts to establish oneself as popular, appears inversely related to privacy risks.[51] Livingstone argues that teenagers are attracted to online interaction because it is a space to experience adolescence (for some, to construct personalities, for others, to take risks) without observation.[52] "The complex relationship between opportunity and risk is not distinct to the Internet but is, rather, a feature of adolescence."[53]

---

[49] *In Study, Facebook Users Share with Stranger*, WALL ST. J., Aug. 14, 2007, at B3 (discussing research from Sophos Security firm claiming 41% of Facebook users were willing to share personal information with a stranger); *Facebook: The Privacy Challenge*, SOPHOS.COM, http://www.sophos.com/security/topic/facebook.html (last visited Nov. 8, 2010) (Forty-six percent of Facebook users accepted Friend requests from fictional stranger, 89% of users in their 20s divulged birth dates, and 30-40% of users disclosed data about friends and family); David Ramsay, *Marshwood Middle School Parents Told 58 out of 60 Kids Accepted Unknown Facebook Friend*, SEACOAST ONLINE (Nov. 21, 2009, 2:00 AM), http://www.seacoastonline.com/articles/20091121-NEWS-911210335 (reporting that Internet safety expert connected with 60 honors students and 58 of them allowed her to "Friend" them without knowing who she was).

[50] Grimmelmann, *supra* note 28, at 1151-56; *see also* PALFREY & GASSER, *supra* note 6, at 25 (discussing the importance of identity to the digital native and the reasons why they share information, including to build trust with others); boyd & Ellison, *supra* note 18, at 7; Livingstone, *supra* note 6, at 10 ("[T]eenagers must and do disclose personal information in order to sustain intimacy . . . ."); *see also id.* at 5.

[51] Contacts or "Friends" may be added by friends or strangers. Grimmelmann, *supra* note 28, at 1175. The visibility of said profiles and list of contacts is crucial and varies among social networking sites, many of which are by default available to the public or others, whose visibility the user limits to a circle of contacts. boyd & Ellison, *supra* note 18, at 3. While "Friends" require confirmation from both parties, some others do not. *Id.*

[52] Livingstone, *supra* note 6, at 5.

[53] *Id.*

While the idea of youth creating and experimenting with different social identities is not new, a significant difference is that youth are doing so in digital formats that can be easily accessed by anyone and difficult to manage.[54]

1. Commercial Interest in Obtaining Personal Information and Risk-Taking Youth

Notwithstanding a perception of privacy, research indicates that youth often use the Internet to publicly share a variety of sensitive information.[55] While youth may characterize some of this material as limited in access, the accuracy of this perception is likely to continuously falter, particularly as the companies that facilitate social networking make more and more of their information searchable, and repeatedly change their privacy policies.[56]

---

[54] PALFREY & GASSER, *supra* note 6, at 30, 44. While 55% of online teens create profiles, only 20% of adults did so in 2006. MADDEN ET AL., *supra* note 7, at 1. While Madden reports that young adults (18-29) most actively manage their privacy settings, they also "are by far the most likely to say that they have posted content to social networking sites that they later regret sharing." MADDEN AND SMITH, *supra* note 7, at 30.

[55] MCQUADE & SAMPAT, *supra* note 23, at 9, 15, 29. Acquisti and Gross note that the combination of weak security controls by design combined with decreasing costs for data mining mean "ostensibly private social network" data is public. Acquisti & Gross, *supra* note 40, at 2 ("unprecedented phenomena of information revelation"). For example, children as young as the fourth through sixth grades "frequently" engage in social networking activities involving posting "personal, potentially exploitable, information about themselves online." MCQUADE & SAMPAT, *supra* note 23, at 9; *see also id.* at 15 (Twenty-two percent of tenth through twelfth graders provide personal information online); *id.* at 29 ("[P]robably due to the increased popularity of social networking sites many students [in grades seven through nine] are using the Internet to publicly post a variety of sensitive information.").

[56] While youth may feel that they are the customers of the social networking site, this is indeed a misperception. A customer is an entity who pays the social networking sites for the service. Profits for most social networking sites do not come from members, but the advertisers who seek the personal information available on social networking sites for targeted marketing. *See Is Social Network Advertising Ready for Prime Time?*, EMARKETER.COM, http://www.emarketer.com/Article.aspx?R=1007165 (last visited Nov. 8, 2010) (projecting that "US marketers will increase social network ad spending 13.2% in 2010, [up] to $1.3 billion"). "Facebook makes personal data provided by users available to advertisers, in aggregated form, for its own commercial gain." KIRKPATRICK, *supra* note 31, at 202. Indeed, one of Facebook's co-founders stated as much when he said Facebook "can provide really good, relevant advertising to people because they tell us exactly what they are interested in, and who they know, and those

Facebook itself is an excellent example of the changing tides of a social networking site. It originated as a closed network for Harvard University, grew rapidly to several hundred universities, eventually expanded to high school students, and ultimately opened unlimited access to anyone claiming to be over 13 years old.[57] While it originally kept profiles internal, currently "limited profiles" are searchable on the Internet with any search engine.[58] Although the changes admittedly did not occur without notice to members, more specific changes in privacy, which always move in the direction of decreasing privacy, take place. This is consistent with the Facebook Terms of Use,

people tell us what they're interested in." Alexei Oreskovic, *Revenue Tops $800 Million for Facebook*, TORONTO STAR, June 19, 2010, at B4. EMarketer reports that "social network users create a gigantic amount of data about themselves—their friend networks, likes and dislikes, content-sharing activities and more." *Is Social Network Advertising Ready for Prime Time?*, *supra*. This prompted an analyst to describe social networking sites' advertising as "a marketer's dream come true." *Id.* Such sites' customers, (i.e., profit sources) are online advertisers. The product they sell these advertisers is the users' information. So, far from being the customer, youth and all users of social networking sites are, in fact, the product sold. Acquisti argues that social networking sites are *imagined* communities because security-access controls are weak by design to make it easier for people to join and contact others through sharing of personal information, hence, its commercial value. Acquisti & Gross, *supra* note 40, at 3 (discussing financial profits such sites have made from marketers, among other things). Livingstone expounded on this concern by noting that privacy settings are inadequate in affording teenagers the level of intimacy they want. Livingstone, *supra* note 6, at 11 (noting the "(mis)match between technological affordances and teenagers' conceptions of friendship"); *see also* boyd & Hargittai, *supra* note 14, at 25 (noting the vulnerability of the population of least skilled Internet users is magnified by how companies set up or modify default privacy settings); PALFREY & GASSER, *supra* note 6, at 56 (documenting the evolution of default privacy settings on Facebook and MySpace to allow increased search ability). Similarly, big businesses search the web for information on individuals to obtain and store what they value. *Id.* at 45, 56-58, 65 (documenting the lack of awareness among young people to protect privacy and the challenge of staying current with privacy policies).

[57] FACEBOOK, *Privacy Policy*, http://www.Facebook.com/policy.php (last visited Aug. 25, 2010). Kirkpatrick argues, however, that its membership is "common among younger and younger children—it is now commonly used by many eleven-year-olds and those even younger, despite Facebook rules that users must be thirteen." KIRKPATRICK, *supra* note 31, at 205.

[58] Grimmelmann, *supra* note 28, at 1169.

which allow Facebook to change its privacy policies unilaterally.[59]

For example, in 2006, Facebook attempted to implement a new feature entitled "Newsfeeds," which displayed a list of a member's every action to all one's "Friends." This resulted in the broadcasting of every change in status, addition, or deletion of a Friend, comment made, or group joined to all of the member's Friends.[60] This outraged members, the largest group being Students Against Facebook Newsfeeds, which grew to boast several hundred thousand members.[61] Facebook partially retreated from its original plan and allowed users more control and also the ability to exclude certain items from appearing on other Friends' Newsfeeds.[62]

Similarly, in April of 2010, Facebook unilaterally moved to expand Facebook functions across the Web.[63] The new policy "required users to opt out if they wished to keep information private, making most of the information pubic by default."[64] The "opt out" provision required a member to sift through approximately 150 options and determine to whom the information would be made available, making what privacy controls

---

[59] *See*, *e.g.*, Caroline McCarthy, *Do Facebook's New Privacy Settings Let It Off the Hook?*, CNET NEWS, (May 26, 2010, 12:07 PM), http://news.cnet.com/8301-13577_3-20006054-36.html (noting that concern about "how easily and willfully [Facebook] could make a major turnaround in user experience" with its privacy changes); Grimmelmann, *supra* note 28, at 1183. Facebook also warns users that it may retain data on them even after they delete their accounts, that it may surveil them even when they're not using Facebook, that it uses their information for marketing purposes (including targeted ads), that it retains discretion over whether and when to share their information with their parties, and that sometimes Facebook even deliberately gives out accounts to let outsiders see what's going on inside. FACEBOOK, *supra* note 57, para. 9 "Other Terms"; *see also* KIRKPATRICK, *supra* note 31, at 204. Indeed, when some questioned the privacy implications of Twitter archiving all messages with the Library of Congress, a Library representative cited to the user's agreement to the terms of service. Steve Lohr, *It's History, So Be Careful Using Twitter*, N.Y. TIMES, Apr. 15, 2010, at B2.

[60] Grimmelmann, *supra* note 28, at 1146.

[61] DANIEL J. SOLOVE, THE FUTURE OF REPUTATION 169 (2007).

[62] Grimmelmann, *supra* note 28, at 1146; boyd & Hargittai, *supra* note 14, at 4.

[63] Miguel Helft & Jenna Wortham, *Facebook Bows to Pressure Over Privacy*, N.Y. TIMES, May 27, 2010, at B1.

[64] Nick Bilton, *Price of Facebook Privacy? Start Clicking*, N.Y. TIMES, May 13, 2010, at B8.

were available "effectively unusable for many people."[65] Additionally, the site planned an "instant personalization" feature that allowed outside partner sites (such as Pandora.com and yelp.com) to gain access to personal data of members.[66]

After weeks of pressure from outraged users, privacy advocates, and government officials, Facebook announced a change to this policy.[67] Not retracting completely, the default remained that the information was publicly available. However, it did create a much simpler method of adjusting who could view one's information, creating simpler controls for the user who could now limit about fifteen categories of information to be visible to Friends, Friends of Friends, or everyone on the Internet.[68] The publicly available information in its directory of users was also limited to less information than it previously required of members.[69] These potentially privacy compromising actions by Facebook continue in 2011.[70]

---

[65] Helft & Wortham, *supra* note 63; Bilton, *supra* note 64 (asserting that the opt-out provision required users to click through more than 50 privacy buttons, choosing among more than 170 options); Mark Zuckerberg, *From Facebook, Answering Privacy Concerns With New Settings*, WASH. POST, May 24, 2010, at A19 (CEO of Facebook acknowledging that members felt privacy controls were too complex).

[66] Helft & Wortham, *supra* note 63; Chloe Albanesius, *Facebook Updates Privacy Policy, Promises Simpler Process,* PCMAG.COM., (May 26, 2010), http://www.pcmag.com/article2/0,2817,2364199,00.asp. Under "instant personalization," when a Facebook user visits a site, the site can use the user's public Facebook information, including the name, profile picture, and Friends' information to "personalize the experience." Clint Boulton, *Facebook Instant Personalization Protested by EFF, MoveOn.org*, EWEEK.COM, (May 2, 2010), http://eweek.com/c/a/Web-Services-Web-20-and-SOA (follow "3" hyperlink to the third page of articles; then click "Facebook Instant Personalization" hyperlink).

[67] Helft & Wortham, *supra* note 63.

[68] *Id.*; Albanesius, *supra* note 66; McCarthy, *supra* note 59 (describing the new privacy settings).

[69] Helft & Wortham, *supra* note 63. For a discussion of Facebook privacy related controversies and its relation to the corporate view of transparency, see KIRKPATRICK, *supra* note 31, at 199-214. Facebook is not alone. Google, in an attempt to create a social networking service, Google Buzz, initially automatically enrolled all Gmail users in this network and unilaterally connected people, thus sharing user's information with the public and making some posts public without Gmail users' knowledge. Miguel Helft, *Critics Say Google Invades Privacy with New Service*, N.Y. TIMES, Feb. 13, 2010, at B1; *see, e.g.*, Mukul Kumar, *Making Content Social,* FIN. EXPRESS, Feb. 25, 2010. While Google eventually made some changes in the program, it prompted some to wonder if automatically changing Gmail accounts to Google Buzz accounts and then pro-

2. Official Interest in Personal Information and Risk-Taking Youth

While such commercial activity combined with youth risk-taking demonstrates the immediate risks to privacy, Palfrey and Gasser persuasively note that the long-term impact for youth has yet to be determined:

> The problem of privacy is exacerbated for young people by the fact that we are just at the beginning of the digital age. . . . Digital Natives will be the first to experience the compounding effects of the creation of identities and digital dossiers over a long period of time. . . . The extent of the damage caused by harmful information—in terms of who can access it, when, how, and over what period of time—continues to increase as the use of technology increases.[71]

This all may seem simply a social problem. However, this view of privacy has implications for the Fourth Amendment when government and school officials utilize such information.

Law enforcement has long used social media in investigations, engaging in activity that could be considered government

---

ceeding to upload such personal information of some customers who are minors violated the Children's Online Privacy Protection Act. Danielle Citron, *Boyden on Google Buzz and COPPA*, CONCURRING OPINIONS, Feb. 17, 2010. An additional example of privacy sharing includes the increasing popularity of "location sharing apps" used on cellular phones, which allow people to "broadcast their whereabouts through check-ins on their mobile devices and connect with others nearby." *NPR Marketplace Morning Report: Facebook Privacy* (NPR radio broadcast Mar. 18, 2010).

[70] *See, e.g.*, Rob Pegoraro, *Facebook Address-Sharing Retreat Provides Further Proof of Law of Unintended Consequences*, WASH. POST. (Jan. 18, 2011, 2:11 PM), http://voices.washingtonpost.com/fasterforward/2011/01/facebook_address-sharing_backt.html.

[71] PALFREY & GASSER, *supra* note 6, at 63-64. Moreover, the Pew Internet & American Life Project reports that concern should extend beyond public digital footprints because corporate databases routinely archive such information. MADDEN ET AL., *supra* note 7, at 2-3 (five most popular search engines routinely archive users search terms, computer's address and unique identifier for their web browser for 13-18 months). Others note that "[t]he networked and public nature of these practices makes the 'lessons' about social life . . . more consequential and persistent." ITO ET AL., *supra* note 6, at 14. Indeed, Twitter is donating its archive of all public "tweets" as well as providing regular updates to the Library of Congress. Randall Stross, *When History Is Compiled 140 Characters At A Time*, N.Y. TIMES, May 2, 2010, at B5.

monitoring.[72] A released Department of Justice document identifies the utility of social networking sites to "reveal personal communications[;] establish motives and personal relationships[;] provide information[;] prove and disprove alibis[;] and establish crime or criminal enterprise."[73] It further discusses the reasons to "go undercover" on such sites to include "communicate with suspects/targets[;] gain access to non-public info[;] [and] map social relationships and networks."[74] Furthermore, when a suspect is arrested carrying a cell phone, police

---

[72] Griffin v. State, 995 A.2d 791 (Md. Ct. Spec. App. 2010) (police using MySpace posting as evidence of intimidation); Richard Lardner, *Break the Law and Your New "Friend" May Be the F.B.I.*, AP DATASTREAM, Mar. 16, 2010 (describing federal agents "logging on surreptitiously to exchange messages with suspects, identify target's friends or relatives and browse private information such as postings, personal photographs and video clips"); Ted Strong, *Nelson County Deputies Take Laptops for a Spin*, CHARLOTTESVILLE DAILY PROGRESS, July 4, 2010 (discussing use of social networking information as an investigative tool to track down information on suspects, locate evidence of a crime, and other activity); Tracy Gordon Fox, *Extra Eyes Watch Online, Police Look Over Kids' Shoulders*, HARTFORD COURANT, Oct. 29, 2006, at A1 (police arresting a high school sophomore after posting threatening messages on his MySpace account apparently aimed at "student body").

[73] Letter from Rena Y. Kim, Chief of Freedom of Info./Privacy Act Unit, Office of Enforcement Operation, to James Tucker, Elec. Frontier Found., Obtaining and Using Evidence from Social Networking Sites, *available at* http://www.eff.org/files/filenode/social_network/20100303__crim_socialnetworking.pdf. This document was released to the Electronic Frontier Foundation through a FOIA request and appears to be related to Federal Agent Training. Lardner, *supra* note 72 (locating a suspect through a Friend's profile). Campus and local police have used social media to identify and arrest criminals. Lindsey Reiser, *To Catch a Thief on Facebook – Campus Police Use Facebook to Identify Suspects*, ABC NEWS (Feb. 28, 2010), http://abcnews.go.com/print?id=9933416 (documenting campus and local police identifying and arresting suspects through reviewing social media). A recent state level training course entitled "Successful Use of Online Social Networking for Criminal Investigations and Intelligence" notes that

> [o]n-line social networking sites such as MySpace, Facebook are an untapped resource for many investigators. Gangs and other criminals use the Internet, particularly MySpace, Facebook and other social networking sites, to recruit new gang members, plan crimes, brag about their crimes, post pictures of themselves with their associates, steal identifying information from others and engage in other various types of illegal activity.

Successful Use of Online Social Networking for Criminal Investigations and Intelligence, PROJECT SAFE NEIGHBORHOODS (June 17, 2010), *available at* http://www.in.gov/ipac/June%2017%20Online%20social%20networking%20training.pdf.

[74] Letter from Rena Y. Kim to James Tucker, *supra* note 73.

often search it incident to the arrest.[75] Such a search often reveals considerable personal information about the possessor's previous whereabouts, conversations, and associations, all of which is information many people have previously considered private.

Schools, in an attempt to fulfill their compelling interest in a safe school community and the maintenance of a learning environment, have recognized that students are using technology at times to negatively affect that environment. Officials understand and take advantage of this use to protect the environment. For example, some school-based law enforcement and school officials regularly access social networking sites of students for a variety of reasons. On the one hand, a youth having a school resource officer as a Friend or contact on his social network site is considered a deterrent to online victimization by adults. However, that "Friend" and law enforcement official now has access to all the information on the student's social networking site and possibly that of many of his contacts. Specifically regarding students, officials also access social networking sites to interdict and prevent youth crime, such as uncovering plans for a party where alcohol will be served or for a fight between rival groups prior to such occurrences.[76] Additionally, school resource officers can become aware of past crimes such as cyber-bullying or threats to school community.[77] However, such intrusions may allow government officials to examine deeply personal matters such as diaries, location of students,

---

[75] *See infra* p. 1064 and notes 136-38 and accompanying text.

[76] Fox, *supra* note 72 (discussing how much underage drinking is promoted on such social networking sites and documentation of such is later posted). The Boston Globe reported that of twenty-two police departments, fourteen utilize social networking sites for investigations, citing examples of locating missing teens, identifying a vandal who caused $70,000 worth of damage, review for underage drinking parties, and brewing fights in schools. Julie Masis, *Predators Beware: Face on MySpace May Be Police Decoy*, BOSTON GLOBE, Feb. 8, 2009, at R3.

[77] *See* Fox, *supra* note 72 and accompanying text. Michael Burnbaum, *The Profile Police,* WASH. POST, Apr. 6, 2009, at A1 (discussing police using social networking sites to "break up fights, monitor gangs, and thwart crime in what amounts to a new cyber-beat").

personal information, and images, all without either procedure or any level of suspicion.[78]

> In this fast-changing digital environment, expectations of privacy among young people are shifting. . . . Revised expectations of privacy may have an implication for protections that the Digital Native may receive under the law now and in the future.[79]

Therefore, the impact of this shift in privacy can be great.

II. THE REASONABLE EXPECTATION OF PRIVACY

A. Justice Harlan's Two-Pronged Test

Currently, the analysis of modern Fourth Amendment search doctrine begins with *Katz v. United States*,[80] in which the Supreme Court articulated a transition from a property and trespass concept of government searches to a privacy-based framework.[81] In *Katz,* law enforcement placed a recording device on the outside of a public telephone booth and surreptitiously recorded contents of Katz's conversations. The Court, departing from the previously used trespass analysis, rejected the parties' framing the legal issue as whether a public phone booth was a "constitutionally protected area."[82] Rather, the majority framed the legal issue as whether Katz knowingly exposed information to the public or attempted to keep said information private. Articulating the new privacy basis, the Court asserted that "the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not subject to Fourth Amendment protection. But what he seeks to preserve as pri-

---

[78] Burnbaum, *supra* note 77 (discussing chagrin of students who feel such monitoring is an invasion of privacy); Sarah Randag, *Police Use Social Networking to Target Underage Drinkers*, A.B.A. J., Nov. 25, 2009, http://www.abajournal.com/news/article/police_use_social_networking_to_target_underage_drinkers/.

[79] PALFREY & GASSER, *supra* note 6, at 54.

[80] 389 U.S. 347 (1967).

[81] *Id.* at 353.

[82] *Id.* at 351.

vate, even in an area accessible to the public may be constitutionally protected."[83] However, this arguably ambiguous majority opinion further stated that "the Fourth Amendment cannot be translated into a general constitutional 'right of privacy.' That Amendment protects individual privacy against certain kinds of governmental intrusions, but its protections go further, and often have nothing to do with privacy at all."[84] Some scholars quite reasonably observed the ambiguity of the majority opinion.[85]

Seeking to clarify matters, Justice Harlan, concurring, coined his famous two-pronged analysis. According to Justice Harlan, the government engaged in a search when it examined an area in which a suspect had a "reasonable expectation of privacy."[86] When this occurs, a search warrant (absent an applicable exception) must be obtained. The reasonableness of the expectation is determined by analyzing the "two-fold requirement":

> [F]irst that a person [has] *exhibited* an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand conversations in the open would not be protected

---

[83] *Id.* (citations omitted). For an excellent discussion of the opinions and precedents of *Katz* and *White*, see generally Catherine Hancock, *Warrants for Wearing a Wire: Fourth Amendment Privacy and Justice Harlan's Dissent in* United States v. White, 79 MISS. L.J. 35 (2009).

[84] *Katz*, 389 U.S. at 350; *see also* THOMAS CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION 60 (2008) (noting that although Justice Stewart utilized the word "privacy," he was clear that both no general right of privacy exists and that he "explicitly refused to limit the protections afforded solely to a privacy analysis").

[85] Hancock, *supra* note 83, at 52 and *infra* note 111 and accompanying text (discussing the recognized and perhaps purposeful ambiguity of the majority opinion).

[86] Subsequent cases have interchanged the objective prong to include a "legitimate expectation of privacy" or a "justifiable expectation of privacy." *See, e.g.*, Illinois v. Andrews, 463 U.S. 765, 771 (legitimate); Smith v. Maryland, 442 U.S. 735, 740 (justifiable).

> against being overheard, for the expectation of privacy under the circumstances would be unreasonable.[87]

It is noteworthy that Justice Harlan's formula, unlike the *Katz* majority, *fully* embraced "privacy" as the definition of what the Fourth Amendment protects. In *Smith v. Maryland*, the Court linked the subjective prong of the two-pronged test with the majority's ambiguous privacy focus stating, "[t]he first [prong] is whether the individual, by his conduct, has 'exhibited an actual (subjective) expectation of privacy,' whether, in the words of the *Katz* majority, the individual has shown that 'he seeks to preserve [something] as private.'"[88] Thus, to invoke the protection of the Fourth Amendment, a person must first be able to demonstrate, *through his conduct*, that he sought to protect something as private. The implications of this requirement are particularly significant when considering youthful attitudes toward technology and information sharing.

B. The Court Has Expressed Concern with the Two-Pronged Test

Four short years after *Katz,* Justice Harlan[89] expressed concern about the application of his two-pronged test in his dissent in *United States v. White*. As Justice Blackmun later did in *Smith v. Maryland*,[90] he proposed an alternative to *Katz* when that test failed. In *White*, the police employed the use of an informant who wore a device that transmitted to government agents his conversations with White, which had occurred in the informant's home and car, White's home, and a restaurant.[91] At trial, the government could not locate the informant to testify, and the agents who conducted the surveillance testified as to the conversations.[92] In affirming admission of that evidence, the plurality opinion held that White had assumed a

---

[87] *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (emphasis added).

[88] Smith v. Maryland, 442 U.S. 735, 740 (1979) (emphasis added) (quoting *Katz*, 389 U.S. at 361, 351) (citations omitted).

[89] United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

[90] *See infra* notes 105-10 and accompanying text.

[91] *White*, 401 U.S. at 745-47 (majority opinion).

[92] *Id.* at 747.

risk that the person in whom he confided was either not an informant, or an informant with a transmitter.[93] As such, the Court concluded that the agents had not violated any legitimate expectation of privacy when the informant transmitted and agents monitored the conversations.

Harlan questioned this analysis.[94] In so doing, he challenged the plurality's position that there was no distinction between agents monitoring conversations and undercover informants participating in their conversations:

> The force of the contention [that there is no distinction] depends on the evaluation of two separable but intertwined assumptions: first, that there is no greater invasion of privacy in the third-party situation, and, second, that uncontrolled consensual surveillance in an electronic age is a tolerable technique of law enforcement, given the values and goals of our political system.[95]

Regarding the plurality's use of the reasonable expectation of privacy test, Justice Harlan questioned its utility and conceded its limitations. He acknowledged that the current approach "represent[s] an advance over the unsophisticated trespass analysis of the common law," but stressed that "*they too have their limitations* and can, ultimately, lead to the *substitution of words for analysis*. The analysis must, in [his] view, transcend the search for subjective expectations or legal attribution of assumptions of risk."[96]

This caution, that the analysis not become a rote application of words, seems to arise from an understanding that expectations of privacy are not just labels. He elaborated: "Since it is the task of the law to form and project, as well as mirror and reflect, we should not, as judges, merely recite the expecta-

---

[93] *Id.* at 752.

[94] First, he questioned the plurality's factual treatment equating the facts of *White*, which involved third party monitoring, with the facts of *Lewis* and *Hoffa*, which involved confidential informants relaying their conversations to law enforcement, or *Lopez*, which involved a recording device on a government agent. *Id.* at 784-85 (Harlan, J., dissenting).

[95] *Id.* at 785.

[96] *Id.* at 786 (emphasis added).

tions and risks without examining the *desirability of saddling them upon society*."[97] Therefore, Justice Harlan articulated that his approach in *Katz* may have "misconceived" the true concern of the Fourth Amendment by focusing incorrectly on the individual, rather than the impact of the practice on the whole of society.[98]

Justice Harlan then offered an alternative when the two-pronged test fails. The alternative is rooted in the Court engaging in a more fundamental analysis of "examining the desirability of saddling [such expectations] upon society."[99] His solution is more than just an objective test of what society will approve. Rather, for him "[t]he critical question, therefore, is whether under our system of government, as reflected in the Constitution, we *should* impose on our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement."[100] Harlan proposed answering this question with a balancing test of "[1] assessing the nature of a particular practice and [2] the likely extent of its impact on the individual's sense of security [3] balanced against the utility of the conduct as a technique of law enforcement."[101]

---

[97] *Id.* (emphasis added). Scholars today echo this notion of the need to examine more fundamental questions that an unreflective adherence to the reasonable expectation of privacy test allows. "[T]he phrase 'reasonable expectation of privacy' is essentially a legal fiction that masks a normative inquiry into whether a particular law enforcement technique should be regulated by the Fourth Amendment." Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1037 (2010).

[98] *White*, 401 U.S. at 788 n.24 (Harlan, J., dissenting).

[99] *Id.* at 786.

[100] *Id.* (emphasis added). For a discussion on Harlan's "should" question, see Hancock, *supra* note 83, at 76-78. Hancock describes a series of Harlan opinions as "reflect[ing] the view that the *Katz* expectations concept was a vessel that could be filled with arguments that defined privacy based on artificial criteria resembling legal fictions of the *Olmstead* regime." *Id.* at 89.

[101] *White*, 401 U.S. at 786 (Harlan, J., dissenting). This focus on individual security hearkens back to early attempts by the Court to address the Fourth Amendment. For example, in *Boyd v. United States*, the Court found an order compelling the production of records violated the Fourth Amendment. The Court noted, "It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property . . . ." Boyd v. United States, 116 U.S. 616, 630 (1886).

For Justice Harlan, the question became not simply whether an individual had an expectation, but rather, whether the Court should impose upon the citizenry the risk to their security without Fourth Amendment protection. This analysis was invoked by Justices Marshall and Brennan in their dissent in *Smith* where Justice Marshall not only quoted Justice Harlan's discussion of "saddling" risks on society, but also challenged the assessment of risk approach by reminding that:

> [W]hether privacy expectations are legitimate within the meaning of *Katz* depends not on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in free and open society. By its terms, the constitutional prohibition of unreasonable searches and seizures assigns to the judiciary some prescriptive responsibility.[102]

While Justice Blackmun later acknowledged Justice Harlan's cautionary note in his *White* dissent, Justices Marshall and Brennan explicitly embraced Harlan's fundamental approach to "evaluate the 'intrinsic character' of investigative practices with reference to the basic values underlying the Fourth Amendment."[103]

A decade after *Katz*, in *Smith v. Maryland*,[104] Justice Blackmun writing for the majority sounded a similar caution. Justice Blackmun recognized situations in which the subjective expectations of privacy prong would not suffice, and also offered an alternative approach. *Smith* involved a case in which law enforcement requested that the telephone company install a device that recorded outgoing phone numbers dialed from Smith's home, but not the content of the ensuing conversations.[105] The Court upheld this warrantless procedure partly because it concluded that Smith had no reasonable expectation of privacy in the phone numbers dialed due to his awareness of

---

[102] Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting).

[103] *Id.* at 751.

[104] 442 U.S. 735 (1979).

[105] *Id.* at 737.

the numbers' exposure to the phone company.[106] However, within this discussion, the Court recognized situations in which the two-pronged test would not be applicable. After discussing the two prongs, the Court stated that "[s]ituations can be imagined, of course, in which *Katz*'s two-pronged inquiry would provide an inadequate index of Fourth Amendment protection."[107]

> For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, *individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects.* Similarly, if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well. 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.[108]

Thus, the Court cautioned that the government could not limit privacy expectations merely by announcing its intent to spy on its citizens; if the government did so, the expectation-of-privacy test would be inadequate, and a "normative inquiry" would be necessary.[109] But in predicting potential threats to

---

[106] *Id.* at 743.

[107] *Id.* at 741 n.5.

[108] *Id.* (emphasis added).

[109] The term "normative" can be somewhat ambiguous in that it is considered to have two meanings. First, it is defined as "[e]stablishing or conforming to a norm or standard." BLACK'S LAW DICTIONARY 1086 (8th ed. 2004). Second, it has also reflected, not a societal standard, but what most of society actually does do: "actual . . . standard determined by the typical or most frequent behavior." *Id.* Therefore, one meaning suggests an inquiry into an authoritative standard, while the other suggests an inquiry into the average or median standard of a group. Whichever was intended by Justice

privacy and Fourth Amendment protection, the Court did not envision what appears to be happening today—that a substantial segment of society would deliberately or unwittingly diminish its own right to privacy.

By and large, the Court has continued to apply Justice Harlan's two-pronged test in *Katz*.[110] However, the Court has also recognized flaws to this approach under certain circumstances or, in Justice Scalia's case, all circumstances.[111] When the test fails, Justice Blackmun counsels applying a strictly normative approach. Justice Harlan proposed a more fundamental inquiry into the nature of a practice, its impact on the individual's sense of security, and the utility of the practice.

C. In Public School Settings Students Have Limited Privacy Rights

Before addressing whether today's youths' subjective attitudes toward privacy have undermined their constitutional protections, it is worth reviewing how the Supreme Court has applied the Fourth Amendment to searches by public school officials.[112] While this line of cases is imperfect because it focuses on students, not youth more generally, it provides the clearest lens through which to examine the implications of the arguably distinct privacy expectations. The issue arises both in suspicion-based searches and suspicionless searches. In both

Harlan, the question still remains: whose normative should be applied—all of society's or a subset class's normative? How should that normative be measured?

[110] *E.g.*, Bond v. United States, 529 U.S. 338 (2000); California v. Ciraolo, 476 U.S. 207 (1986); Smith v. Maryland, 442 U.S. 735 (1979).

[111] Justice Scalia has written that the *Katz* test established only "that, unsurprisingly those 'actual (subjective) expectations of privacy' that society is prepared to recognize as 'reasonable,' bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable. When that self-indulgent test is employed . . . to determine whether a 'search or seizure' within the meaning of the Constitution has occurred (as opposed to whether that 'search or seizure' is an 'unreasonable' one), it has no plausible foundation in the text of the Fourth Amendment." Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring).

[112] Since the Fourth Amendment protects against only government intrusions into privacy, Fourth Amendment issues arise in school settings only in public schools; searches by officials in private schools are not subject to Fourth Amendment standards or restrictions.

contexts the Court recognized that in a school setting, a school's need to maintain order and discipline, and preserve the learning environment necessarily diminishes a student's privacy rights.[113]

The Court first held that public school students are protected by the Fourth Amendment on school property in *New Jersey v. T.L.O.*[114] In *T.L.O.*, a school official searched T.L.O.'s purse, having suspected her of smoking on campus.[115] In this case, the Court concluded that the Fourth Amendment does apply to searches conducted by school officials.[116] However, while at school, students do not enjoy the same degree of protection as adults. As a rule, to search an adult, a public official must have probable cause to believe evidence of a crime will be found, and, often, must obtain a search warrant before conducting the search. In *T.L.O.*, the Court concluded that neither of these requirements applied in the public school setting.[117] The Court reasoned that the central requirement of the Fourth Amendment is that a search or seizure must be "reasonable."[118] Specifically, "what is reasonable depends on the context in which the search takes place."[119] In a public school context, that determination is made by "balancing the need to search against the invasion which the search entails."[120] For a school setting, the Court determined that balance was between the "substantial interest of teachers and administration maintaining discipline in the classroom and on school grounds" and the

---

[113] New Jersey v. T.L.O., 469 U.S. 325, 341 (1985).

[114] *Id.* at 325. When searching students, the doctrine of in loco parentis did not isolate officials from the Fourth Amendment because they act as representatives of the state. *Id.* at 336.

[115] *Id.* at 328.

[116] *Id.* at 333-34; *see supra* note 114 and accompanying text.

[117] 469 U.S. at 340-41 ("The warrant requirement, in particular, is unsuited to the school environment: 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.").

[118] *Id.* at 337.

[119] *Id.*

[120] *Id.* (quoting Camara v. Mun. Court, 387 U.S. 523, 536-37 (1967)).

students' interest in privacy.[121] Not only was a warrant unnecessary, but the Court lowered the level of suspicion necessary for a search to be reasonable; probable cause was not required. Rather, a court must determine the reasonableness of a search with a two-fold inquiry. First, one must consider whether the action was "justified at its inception."[122] A search is "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."[123] Second, the search actually conducted must be "reasonably related in scope to the circumstances which justified the interference in the first place."[124] This standard is met 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."[125]

T.L.O., therefore, confirmed that, although the Fourth Amendment applies to students in a school search, students have limited privacy rights in a school setting. School officials are permitted to search students without probable cause or a warrant. They can do so if the search is based on a reasonable suspicion that it will produce evidence of violation of either a criminal law or school policy and it is not excessive in scope relating to the objective of the search and age or sex of the student. In *T.L.O.*, school officials had a reasonable suspicion that T.L.O. had cigarettes in her purse and, therefore, looked through it. The Court upheld this action as reasonable.[126]

This conceptualization of students as a group who possess decreased rights is apparent in the suspicionless search cases as well. In 1995 and again in 2002, the Court held that where

---

[121] *Id.* at 339-40. "[W]e have recognized that maintaining security and order in the schools requires a certain degree of flexibility in school disciplinary procedures." *Id.* (citing Goss v. Lopez, 419 U.S. 565, 582-83 (1975)).

[122] *Id.* at 342 (quoting Terry v. Ohio, 392 U.S. 1, 20 (1968)).

[123] *Id.* (emphasis added).

[124] *Id.* at 341.

[125] *Id.* at 342.

[126] *Id.* at 343-44 (validating a subsequent student search for cigarettes based on the reasonableness of the original search).

school officials could demonstrate that a significant drug problem existed within a school or a district and that less intrusive measures had not or would be unlikely to address the problem, it was reasonable to mandate that students could not participate in extracurricular activities unless the student and parents agreed that some participants would be required to submit urine samples for drug testing, under conditions that adequately protected the student's privacy and rigorously controlled information concerning test results.[127] The Court explicitly articulated that "the legitimacy of certain privacy expectations . . . may depend upon the individual's legal relationship with the state."[128] Students in their "legal relationship with the state" stand with a decreased expectation of privacy that is considered with the level of intrusion and balanced against the severity of the need for school officials to search.[129]

The Court next considered a suspicion-based search of a public school student in 2010, in *Safford Unified School District #1 v. Redding*, where it departed from previous cases and ruled in favor of the student. In *Redding,* school officials had received information that students were bringing prescription medication to school for recreational consumption.[130] The school had previously had a student hospitalized for such abuse.[131] Information linked the petitioner as a possible source of pills found on school grounds.[132] As a result, school officials not only searched the petitioner's belongings, but subjected her to an unconstitutional "strip search."[133] An 8-1 majority held that, even assuming school officials had reasonable suspicion to believe that a middle school girl possessed prescription strength and over-the-counter medication, forcing her to submit to a

---

[127] Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653-54 (1995); Bd. of Educ. v. Earls, 536 U.S. 822 (2002).

[128] *Vernonia Sch. Dist.*, 515 U.S. at 654 (upholding random drug testing procedure for student athletes under the special needs exception to the warrant requirement).

[129] *Id.* at 657.

[130] Safford Unified Sch. Dist. #1 v. Redding, 129 S. Ct. 2633, 2640 (2009).

[131] *Id.* at 2648. (Thomas, J., concurring in part and dissenting in part).

[132] *Id.* at 2640 (majority opinion).

[133] *Id.* at 2642-43.

search only slightly less intrusive than a strip search was an excessive intrusion into her privacy.[134]

While the Court announced no change in the standard, the opinion offers some guidance regarding the Court's conceptualization of students as a group and their expectations. First, the Court indicated that a search has "reasonable grounds" if there is a "*moderate chance* of finding evidence of wrongdoing."[135] This terminology of "moderate chance" appears to be an attempt to more precisely describe the "reasonable grounds" standard rather than to change the standard. Second, the Court stated that Redding did have a reasonable expectation of privacy in the personal items she carried in her backpack.[136] This is not insignificant, particularly given how many youths carry among their personal items cell phones or other mobile electronic devices capable of storing and accessing nearly unlimited amounts of personal information.[137] Third, the Court said that the strip search was an invasion of the girl's subjective expectation of privacy, in part because it was "inherent in her account . . . as embarrassing, frightening and humiliating."[138] Therefore, the intrusiveness of a search can be measured in part by the level of embarrassment and humiliation caused. Fourth, the Court clearly conceptualized students as a group. Although *Redding* involved a suspicion-based search of one student, the Court drew at least one conclusion from her status as a student. The Court noted that "[t]he reasonableness

---

[134] *Id.* at 2643-44 (a strip search of a student violated the Constitution, but school officials were entitled to qualified immunity). Previous school-search cases held in favor of the school. *See* Bd. of Educ. v. Earls, 536 U.S. 822, 838 (2002) (deeming constitutional a school policy that requires all students who participate in any extracurricular activity to undergo drug testing because the policy "is a reasonable means of furthering the School District's important interest in preventing and deterring drug use among its schoolchildren"); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 665 (1995) (holding school's policy, conditioning that student athletes participating in sports consent to random drug testing, constitutional under Fourth Amendment inquiry); New Jersey v. T.L.O., 469 U.S. 325, 343-44 (1985) (validating a subsequent student search for drugs based on the reasonableness of the original search).

[135] *Redding*, 129 S. Ct. at 2639 (emphasis added).

[136] *Id.* at 2641 n.3.

[137] *See supra* part I.A.

[138] *Redding*, 129 S. Ct. at 2641.

of her expectation . . . is indicated by the consistent experiences of other young people similarly searched whose adolescent vulnerability intensifies the patent intrusiveness of the exposure."[139] Granted, the reasonableness of the expectation against a near-strip search is easier to defend than the same expectation against a search of a cell phone. However, the Court's emphasis on the reasonable expectations of school children generally, as a distinct class with "adolescent vulnerability," provides a useful perspective in evaluating the degree to which reasonable expectations of privacy exist, and therefore, the justification school officials should be required to demonstrate when invading them. Finally, *Redding* underscores a qualifying statement the Court made in *T.L.O.* which, until *Redding*, was at times overlooked—that in measuring reasonableness, a court must consider the "age and sex" of the student.[140] This aspect of the test combined with (1) the fact that students possess a reasonable expectation of privacy in personal possessions, and (2) that the emotions experienced by the subject youth and the "consistent experience" of similarly situated youth combine to create an interesting result. One now has room to argue that the two-pronged *Katz* test can be viewed through a lens of the unique characteristics and common experience of students and youth as a group. As such, the privacy norms of the group are relevant and may derail the *Katz* test.

D. The Court Has Recognized the Role that Technology Can Play in Reshaping Expectations of Privacy

As background to examining the hypothetical question posed in this title, this article has reviewed the *Katz* test, the Court's expressed reservations of the *Katz* test, and the Court's articulations regarding students and their privacy. We now turn to an analysis of the Court's statements regarding technology and the Fourth Amendment. The intermingling of expectations of privacy and technology has a long history. In their historic 1890 piece, *The Right of Privacy*, Samuel Warren and

---

[139] *Id.*

[140] New Jersey v. T.L.O. 469 U.S. 325, 342 (1985).

Louis Brandeis recognized that the basic concept of the right to privacy was dynamic, and technology affected that right: "Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society."[141] They too expressed concern about technology, a.k.a., "modern enterprise and invention," which can increase the invasion on one's privacy subjecting its members "to mental pain and distress."[142]

Technology affects privacy not only with regard to its use by the government to surveil individuals, but also in the way individuals use it in their daily lives. The Court has referenced technology to both increase Fourth Amendment freedoms and, more often, to restrict them. One reason the *Katz* Court abandoned its trespass analysis and embraced recognition of the need to protect "intangible" conversations was the increased importance of the telephone in daily life.[143] In *Katz* that recognition contributed to the Court finding a reasonable expectation of privacy. In contrast, twenty years later, in *California v. Ciraolo,*[144] the Court cited public use of technological advances to justify denying reasonable expectation of privacy in a defendant's yard:

> In an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet.[145]

The Court, therefore, held that the flight, which was deliberately undertaken to look into the suspect's backyard, was not a "search" at all. In essence the Court equated targeted aerial surveillance over someone's home (and, later, in *Riley v.*

---

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

[142] *Id.* at 196.

[143] Katz v. United States, 389 U.S. 347, 352 (1967) ("To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.").

[144] California v. Ciraolo, 476 U.S. 207, 215 (1986).

[145] *Id.* at 215.

Florida, a helicopter flight from 400 feet over a barn surrounded by fences posted with "no trespass" signs) with seeing into someone's yard from a public sidewalk.[146] These cases support the implication that when social custom and technology make conceptualizing privacy problematic,[147] the Fourth Amendment no longer affords any protection from government use of that technology targeted at a specific location.[148]

On the same day as *Ciraolo*, the Court recognized in *Dow Chemical Co. v. United States* that modern technology may make aerial observation of curtilage invasive when it discloses intimate associations otherwise imperceptible to police.[149] "In common with much else, the technology of photography has changed in this century. These developments have enhanced industrial process and indeed all areas of life; they have also enhanced law enforcement techniques."[150] The Court later stated in *Kyllo v. United States* 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."[151]

---

[146] *Id.* at 213; Florida v. Riley, 488 U.S. 445 (1989).

[147] *Ciraolo*, 476 U.S. at 215. The majority ignored the minimal likelihood that someone might randomly fly over Ciraolo's yard at 1,000 feet, would happen to look down, recognize marijuana cultivation, figure out whose house it was, and report the matter to the police. *Id.* at 223-24 (Powell, J., dissenting).

[148] In its more recent case of direct use of technology for monitoring, the Court discussed the use of thermal imaging technology to monitor suspects within the home. Kyllo v. United States, 533 U.S. 27, 29-30 (2001). The opinion written by Justice Scalia, a critic of the reasonable expectation of privacy analysis, did not analyze the technology within that framework. *Id.* at 39. Rather, the Court noted that when 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 a physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." *Id.* at 40.

[149] *Ciraolo*, 476 U.S. at 215 n.3; Dow Chem. Co. v. United States, 476 U.S. 227 (1986).

[150] *Dow Chemical*, 476 U.S. at 231.

[151] *Kyllo*, 533 U.S. at 33-34. Justice Scalia frames the question presented to the Court in *Kyllo* as "what limits there are upon this power of technology to shrink the realm of guaranteed privacy." *Id.* at 34. Justice Brandeis previously articulated such concerns noting that "[d]iscovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet." Olmstead v. United States 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting).

This approach has clear implications with regard to youths and their mobile devices. A school official or prosecutor might argue by analogy that although a diary was once considered the most personal of documents, now with so many young people keeping online diaries, shared with dozens or hundreds of readers, government perusal of such should be considered the equivalent of the overflights in *Ciraolo* and *Riley*, i.e., not an intrusion into privacy at all.[152]

In 2010 the Court declined the opportunity to rule broadly on the reasonable expectation of privacy in text messages[153] on an employee's work-issued alphanumeric pager.[154] In declining, the Court recognized the dynamic world of technology, noting it should "proceed with care" in part because "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology use before its role in society has become clear."[155] The Court recognized not only the dynamism in the technology itself, but also in social norms: "Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior."[156]

The Court is not alone in struggling to reconcile technological changes and the Fourth Amendment. Scholars have particularly identified the need to adjust the traditional Fourth Amendment analysis for the Internet and cyberspace.[157] Professor Kerr, for example, assumes a goal of "technology neutral-

---

[152] LENHART ET AL., note 5, at i-ii, 7.

[153] Text messages are messages in plain text sent through various devices both wired and wireless. The most common implementation of text messaging is short message service ("SMS"). This is how short messages can be sent to and from handheld wireless devices including phones. NEWTON, *supra* note 4, at 1116.

[154] City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (presenting the question of the expectation of privacy of both (1) the employee in his messages sent and received, and (2) third parties in their messages sent to the employee's pager).

[155] *Id.* at 2629.

[156] *Id.* In the context of the specific issue of *Quon,* the Court noted that "[a]t present, it is uncertain how workplace norms, and the law's treatment of them, will evolve." *Id.* at 2630.

[157] *See, e.g.*, Kerr, *supra* note 97; Adam Gershowitz, *The iPhone meets the Fourth Amendment*, 56 UCLA L. REV. 27 (2008); Morgan Cloud, *The Effect of Technology on Fourth Amendment Analysis and Individual Rights*, 72 MISS. L.J. 5 (2002).

ity," i.e., "the degree of privacy the Fourth Amendment extends to the Internet should try to match the degree of privacy protection that the Fourth Amendment provides the physical world."[158] In so doing he analogizes the distinction in traditional Fourth Amendment analysis of what is inside or outside containers to what is content and non-content in Internet communication, arguing for protection of content in Internet communications.[159] Particularly with the Internet, Kerr criticizes the use of the reasonable expectation of privacy test as failing to "mirror widely shared social expectations."[160] He concludes that when the Court identifies a law enforcement practice it feels should be regulated, it announces that there is a reasonable expectation of privacy, and when the practice need not be regulated, it announces that there is no expectation. Consequently, "asking what privacy most Internet users expect does not accurately represent the *Katz* test."[161] Furthermore, with regard to the rapidly changing technology today, courts likely should not yet choose from emerging social attitudes.

Electronic communication technology in mobile media devices such as the smartphone,[162] iPhone, PDA,[163] and laptop

---

158 Kerr, *supra* note 97, at 1007.

159 *Id.* at 1009-12.

160 *Id.* at 1037.

161 *Id.* at 1037-39.

162 A smartphone is a

> cellular telephone with built-in applications and Internet access. Smartphones provide digital voice service as well as any combination of text messaging, e-mail, Web browsing, still camera, video camera, MP3 player, video player, television and organizer. In addition to their built-in functions, smartphones have become application delivery platforms, turning the once single-minded cellphone into a mobile computer.

PC Magazine Encyclopedia, PCMAG.COM, http://www.pcmag.com/encyclopedia_term/0%2C2542%2Ct%3DSmartphone&i%3D51537%2C00.asp (last visited Nov. 8, 2010).

163 Otherwise known as a personal digital assistant, a PDA is

> [a] handheld computer for managing contacts, appointments and tasks. It typically includes a name and address database, calendar, to-do list and note taker, which are the functions in a personal information manager. Wireless PDAs may also offer e-mail and Web browsing, and data are synchronized between the PDA and desktop computer via USB or wireless. If the PDA includes a phone, it falls into the smartphone category.

computer raise particular concerns about the traditional test. For example, some acknowledge how current Fourth Amendment law could allow access to volumes of information through searches of cellular telephones and suggest altering legal rules to limit such searches.[164] Professor Cloud characterized the use of the two-part test as a failure when it comes to technology because the subjective prong has become irrelevant to the Court.[165] He advocates for a new value-based theory of Fourth Amendment protection with an approach emphasizing the technological equivalent of physical trespass triggering Fourth Amendment protections.[166] All these solutions speak to the problem of linking the Fourth Amendment to current technologies, as the technologies rapidly change and courts cannot uniformly remain informed of and in agreement with analogies.[167]

The current state of the Court's approach to what the Fourth Amendment protects, at least outside the home, can perhaps be summarized as follows. First, under this traditional analysis a suspect must demonstrate by his actions a subjective expectation of privacy and such an expectation must be one that society is willing to endorse.[168] Second, students have decreased privacy rights and the characteristics of their behavioral norms are relevant. Third, although the *Katz* test was

PC Magazine Encyclopedia, PCMAG.COM, http://www.pcmag.com/encyclopedia_term/0,2542,t=PDA&i=49021,00.asp (last visited Nov. 8, 2010).

[164] Gershowitz, *supra* note 157, at 27. In this piece, Gershowitz explores the options of changing nothing; limiting searches incident to arrests to searches for evidence of the crime of arrest; encouraging state legislatures to adopt more narrow statutes than the rule in United States v. Robinson, 978 F.2d 1554 (10th Cir. 1992), which allows the search of all personal items on arrest; limiting searches incident to arrest to only five steps of intrusion; or distinguishing between information on a phone and outside it. *Id.* at 45-57.

[165] Cloud, *supra* note 157, at 28-29.

[166] *Id.* at 44.

[167] *E.g.,* United States v. Bermudez, No. IP 05-43-CR-B/F, 2006 WL 3197181, at *13 (S.D. Ind. June 30, 2006) (rejecting a *Kyllo* challenge to using electronic devices to locate cell phones because cell phones are used to transmit signals to parties outside the home and thus their signals are "knowingly exposed to third part[ies], to wit, the cell phone compan[ies]), *aff'd sub nom.* United States v. Amaral-Estrada, 509 F.3d 820 (7th Cir. 2007).

[168] *See supra* note 87 and accompanying text.

first created to enhance privacy, as technology advances it has almost always resulted in a minimizing of privacy expectations.

Applying the *Katz* approach to the emerging generation of digital natives poses enormous problems. The problems derive from many factors: technology itself, their youth, actions of corporations controlling the technology, and the lack of judgment common in adolescents.[169] Research demonstrates that digital natives engage in somewhat risky behavior online and have a false perception of privacy.[170] The lack of complete development of teenagers' prefrontal cortex impedes their ability to evaluate risks and resist them.[171] Therefore, they may not manifest a subjective expectation of privacy similar to adults.

This failure to demonstrate a subjective expectation of privacy (at least one that society will recognize) may combine with decreased privacy rights of at least public school students to essentially create a "perfect storm" where under a traditional analysis, youths' expectation of privacy is compromised. Thus, the law may force an unforeseen scenario: the inapplicability of the *Katz* test to a class of society, not through government action, but citizen abandonment and corporate conditioning.

It is to this problem the article now turns. It is worrisome that the Court would allow an entire class of citizenry fewer Fourth Amendment protections based on the social norms of their behavior when those norms are just that—normal for their population. This is particularly troubling when that segment of the population has been recognized as less equipped to appreciate privacy implications of their conduct and, therefore,

---

[169] The Court has recognized, albeit in a very different context, that in particular, "developments in psychology and brain science continue to show fundamental differences between juvenile and adult minds." Graham v. Florida, 130 S. Ct. 2011, 2026 (2010); *see also* Roper v. Simmons, 543 U.S. 551, 569-70 (2005) (juveniles' lack of maturity makes them less deserving of severe punishment of death penalty).

[170] PALFREY & GASSER, *supra* note 6, at 166; Grimmelmann, *supra* note 28; Seounmi Youn, *Teenagers, Perceptions of Online Privacy and Coping Behaviors: A Risk-Benefit Appraised Approach*, 49 J. BROADCASTING & ELEC. MEDIA 86 (2005).

[171] PALFREY & GASSER, *supra* note 6, at 166; Grimmelmann, *supra* note 28, at 1179-80 ("Later regret about initial openness is an especially serious problem for the most active social network site users: young people."); LIVINGSTONE & BOBER, *supra* note 2, at 15-16; *see also*, *e.g.*, JONES & FOX, *supra* note 14; LENHART ET AL., *supra* note 5, at 2; MCQUADE & SAMPAT, *supra* note 23, at 28-32.

perhaps more in need of a judicial buffer between them and the state. On the other hand, given that many youths arguably seem to act differently about traditional privacy online, how can the law plausibly rule that they nevertheless have a reasonable expectation of it? The *Katz* test, therefore, may have less utility than ever before.

III. WHAT IF SAVANA REDDING HAD A CELL PHONE? – EXPLORING KATZ AND KATZ ALTERNATIVES.

Beginning with Justice Harlan's dissent in *White,* through Justice Blackmun's opinion in *Smith* and culminating in the majority opinion in *Kyllo*, the Court has shown that the reasonable expectation of privacy test is limited. Given that youth as a group may have a fundamentally different understanding of privacy than older generations, the question becomes whether we have reached a point where their "subjective expectations have become 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms" such that the analysis fails.[172] If so, what then the response? Several possibilities exist. First, a traditional analysis could be applied resulting in either a forced conclusion affording some rights to youth in spite of reality or a stripping of privacy protections for this large segment of society. These results are hardly desirous. Second, Justice Blackmun's suggestion of a normative analysis could be followed. Third, Justice Harlan's alternative test articulated in *White* could be embraced.[173] Each of these approaches has flaws, which will be explored by applying them to an amended factual premise of *Redding*, the Court's most recent school search case.

A. Factual Scenario

The hypothetical providing the vehicle through which to examine these issues will be those of *Redding*, with some modifications to reflect current practices of school searches and cell

[172] Smith v. Maryland, 442 U.S. 735, 741 n.5 (1979).

[173] A fourth approach is possible in which an entirely new test for technology be developed. Such a test is unwise in that tying laws to rapidly changing technology results in quickly obsolete laws.

phone policies. Here, this hypothetical assumes the school not only has a policy strictly prohibiting the nonmedical use, possession, or sale of any drug on school grounds, including "'[a]ny prescription or over-the-counter drug, except those for which permission to use in school has been granted.'"[174] The hypothetical also assumes the school has a policy, common among school systems, prohibiting cell phone use at school, advising that such phones will be confiscated if displayed on campus.[175]

In this hypothetical, one week before the search a student, J.R., reported to the school's vice principal that other students were bringing prescription drugs to recreationally consume at school.[176] He further reported he had previously taken such a pill from his classmate, which made him ill.[177] This school has a previous history of prescription medication abuse resulting in at least one hospitalization.[178]

On the day of the search, J.R. gave school officials a pill of prescription strength ibuprofen (400mg), which he claimed he received from M.G.[179] He further claimed that students were planning to consume the pills at lunch.[180] Officials removed M.G. from class. A day planner within M.G.'s reach was also removed, which contained additional contraband including several knives, lighters, a permanent marker, and a cigarette.[181] A razor blade, several white pills, and one blue pill (later identified as naproxen, an over-the-counter medication) were located within M.G.'s possession.[182] M.G. denied knowledge of the day

---

174 Safford Unified Sch. Dist. #1 v. Redding, 129 S. Ct. 2633, 2640 (2009).

175 *E.g.*, Klump v. Nazareth Area Sch. Dist., 425 F. Supp. 2d 622 (E.D. Pa. 2006) (seizure of cell phone permissible as possession of phone on campus violated school policy, but search was impermissible); Koch v. Adams, 2010 Ark. 131 (2010) (where school district had policy of seizing cell phones for two weeks for possessing cell phone in classroom); *see also* STUDENT DISCIPLINE LAW BULLETIN (West, 2010) (discussing an Ohio school policy of phone confiscation if student violates ban of phone-use on campus).

176 *Redding*, 129 S. Ct. at 2640.

177 *Id.*

178 *Id.* at 2648 (Thomas, J., concurring in part and dissenting in part).

179 *Id.* at 2640 (majority opinion).

180 *Id.*

181 *Id.* at 2638, 2640.

182 *Id.* at 2640.

planner but identified Susie Student (S.S.) as the source of the pills.[183] Others confirmed that S.S. and M.G. were friendly. J.R. identified S.S. as a student in whose house he had consumed alcohol prior to a school dance.[184]

The vice principal removed S.S. from her class and confronted her with the day planner and its contents. S.S. admitted ownership of the planner, but said she had lent it to M.G. a few days earlier.[185] She denied ownership of any of the pills, all of which violated school policy.[186] S.S. denied the vice principal's accusation that she was going to distribute pills in school. Officials searched her backpack and found nothing.[187]

Unlike the actual facts of *Redding,* assume S.S. had a smartphone hooked onto her backpack that buzzed (indicating incoming calls or texts) throughout her meeting with the vice principal with increased frequency as the lunch hour approached. Given the information regarding the possible distribution of pills at lunch, assume the vice principal took the smartphone and (1) looked through the recent calls to determine if M.G. or other students (potential drug purchasers) were trying to contact her; (2) examined her contacts list on her phone to determine shared contacts with M.G. or J.R.; (3) reviewed recent texts to see if there were any drug related messages; and (4) pressed one button on the screen and accessed her social networking account to determine if there were any postings or messages as to the lunchtime drug consumption.

B. Options for Examining the School's Actions

1. Traditional Analysis is Unsatisfying

The proposed hypothetical includes many separate wrinkles that highlight some additional inadequacies of the *Katz* analysis in this situation. Not only are there issues surround-

---

183 *Id.*

184 *Id.* at 2641.

185 *Id.*

186 *Id.* at 2638, 2641.

187 *Id.* at 2641. The Supreme Court found sufficient suspicion to justify the search of the backpack. *Id.* at n.3.

ing youth, but also surrounding the scope and ability of the reasonable expectation of privacy to be viable in a digital age.[188]

a. Applicability of the Fourth Amendment

As a threshold matter, the inquiry must begin by determining whether the Fourth Amendment applies at all, i.e., whether examination of the phone, accessing the call log, accessing the contacts, and accessing the social networking site were examinations into areas where a reasonable expectation of privacy existed. Such an inquiry is fact-driven and done on a case-by-case basis.[189] A superficial application may find that there is indeed a search. Significantly, the *Redding* Court concluded that the student had an expectation of privacy in her backpack as a personal container.[190] Therefore, the argument would proceed, S.S. surely has such an expectation in her phone as a personal container and, the government's examination of it constituted a search. As will be discussed below, although the cell phone search cases are split as to the reasonableness of the searches, almost all of these cases have found that the expectation of privacy in the phone exists.[191]

However, a more in-depth analysis indicates that whether one has a reasonable expectation of privacy in one's phone or text messages is far from clear. The Court did not resolve this in *Quon*.[192] Among the issues in *Quon* was whether a govern-

---

[188] Kerr, *supra* note 97, at 1012-15 (noting that one important difference between the physical and digital world is that the physical environment "limits the scale and location of evidence" but the digital environments normally do not).

[189] United States v. Chadwick, 433 U.S. 1, 23 (1977) ("small variations in the facts are determinative of the legal outcome"); D.H. Overmyer Co. v. Frick Co., 405 U.S. 174, 178 (1972) ("[H]ere, as in nearly every case, facts are important.").

[190] Safford Unified Sch. Dist. #1 v. Redding, 129 S. Ct. 2633, 2641 n.3 (2009).

[191] *See*, *e.g.*, Connecticut v. Boyd, 992 A.2d 1071, 1079 (Conn. 2010) (defendant had reasonable expectation of privacy in cell phone, but search permissible under automobile exception). *Compare* United States v. Finley, 477 F.3d 250, 259-60 (5th Cir. 2007) (implying a reasonable expectation of privacy but upholding search of cell phone incident to arrest by treating the phone as a container), *with* Ohio v. Smith, 920 N.E.2d 949, 955 (Ohio 2009) (reasonable expectation of privacy in cell phone violated by invalid search incident to arrest).

[192] City of Ontario v. Quon, 130 S. Ct. 2619, 2629-30 (2010).

ment employee had a reasonable expectation of privacy in texts (both sent and received) on his government-issued alphanumeric pager.[193] An additional question was whether those who sent him such messages also possessed an expectation that they were private.[194] The Court opted not to address these questions, and decided the case on the narrow grounds that the examination of the messages was reasonable. In so doing the Court explicitly stated it was too early to understand the privacy expectations in text messages, not only because of the technology's effect on shaping privacy expectations, but also "the degree to which society will be prepared to recognize those expectations as reasonable."[195]

This lack of clarity is apparent in cases that have addressed cell phone searches. While there are few published decisions regarding searching cell phones on school property, much less searches of smartphones, there have been analyses of warrantless phone searches in other capacities, the most common of which are cases dealing with the searching of cell phones incident to arrest or consistent with other exceptions to the warrant requirement.[196] Courts are split on this issue and

---

[193] *Id.* at 2630-31.

[194] *Id.* at 2629-30.

[195] *Id.* at 2630-31. After *Quon*, the Court of Appeals for the 11th Circuit ruled that federal law has not clearly established a reasonable expectation of privacy in emails sent through a third-party Internet service provider. Rehberg v. Paulk, 611 F.3d 828 (11th Cir. 2010).

[196] It should be noted that many cases discussing searches of cell phones incident to arrest predate or omit the relevance of *Arizona v. Gant*, 129 S. Ct. 1710 (2009), in which the Court limited the search of a vehicle incident to arrest, and perhaps all searches incident to arrests, to searches for evidence of the crime of arrest or for officer safety. *See* State v. Smith, 920 N.E.2d 949, 952 (Ohio 2009) ("[W]hen the interests in officer safety and evidence preservation are minimized, the court has held that this exception no longer applies."); United States v. Wall, No. 08-60016-CR, 2008 WL 5381412, at *3 (S.D. Fla. Dec. 22, 2008) (same). Of course, courts have analyzed cell phone searches in contexts other than incident to arrest. *See* Connecticut v. Boyd, 992 A.2d 1071, 1076 (Conn. 2010) (search of incoming numbers on cell phone valid under automobile exception to warrant requirement); People v. Chho, 2010 WL 1952659, at *4 (Cal. Ct. App. May 17, 2010) (same); Lemons v. Texas, 298 S.W.3d 658, 662 (2009) (approving search of phone photos based on consent suggested when defendant handed phone to officers after their request "to see the phone" and concluding neither *Park* nor *Finley* applied); *Wall*, 2008 WL at *4 (rejecting government arguments of exigency or inventory search in addition to rejecting search incident to arrest argument); United

the fault line in this division depends on the court's conceptualization of the cell phone. Those courts that consider phones as containers capable of holding other containers generally allow the searches. Those that consider phones items that themselves access vast personal information do not.[197]

A leading case for a conception of cell phones as merely containers, and one of few circuit court decisions on this issue, is *United States v. Finley.*[198] In *Finley* the police searched the defendant's work-issued cell phone incident to his narcotics arrest, examining his phone, call log, and text messages.[199] The court found nothing special about the fact that the item examined was a cell phone and treated it as a container on one's person and, therefore, searchable without any additional justification at arrest.[200] In the early cell phone cases, many courts followed suit.[201]

States v. James, No. 1:06CR134 CDP, 2008 WL 1925032, at *4 (E.D. Mo. Apr. 28, 2008) (allowing search of cell phone under the automobile exception, but rejecting arguments based on consent and exigent circumstances); New York v. McGee, No. 2006NY047717, 2007 WL 1947624, at *6 (N.Y. Crim. Ct. June 29, 2007) (rejecting search of photos on phone based on inventory search).

[197] For a discussion of these differing conceptualizations of some electronic devices as containers or not, see U.S. DEPT. OF JUSTICE, COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION, SEARCHING & SEIZING COMPUTERS AND OBTAINING EVIDENCE IN CRIMINAL INVESTIGATIONS 3-4, 33 (2009).

[198] United States v. Finley, 477 F.3d 250, 259-60 (5th Cir. 2007) (upholding search of cell phone as incident to arrest). The same circuit later rejected a search of a cell phone incident to arrest because the arrest was not valid. United States v. Zavala, 541 F.3d 562, 575-76 (5th Cir. 2008). *Zavala* has language differing from *Finley* and its conceptualization of the cell phone. *Zavala* recognized that "cell phones contain a wealth of private information including emails, text messages, call histories, address books, and subscriber numbers," calling them "similar to a personal computer that is carried on one's person." *Id.* at 577. The Court of Appeals for the Fourth Circuit followed *Finley*. United States v Murphy, 552 F.3d 405, 413 (4th Cir. 2009) (affirming denial of motion to suppress evidence from cell phone).

[199] *Finley*, 477 F.3d at 254.

[200] *Id.* at 259-60.

[201] *E.g.*, United States v. Deans, 549 F. Supp. 2d 1085, 1094 (D. Minn. 2008); United States v. Valdez, No. 06-CR-336, 2008 WL 360548, at *3 (E.D. Wis. Feb. 8, 2008) (although agreeing with Finley, noting the privacy concerns articulated in United States v. Park, No. CR 05-375 SI, 2007 WL 1521573 (N.D. Cal. May 23, 2007), were not implicated because the officer limited his search to call history and did not search voicemails or text messages); United States v. Dennis, No. 07-008-DLB, 2007 WL 3400500, at *7 (E.D. Ky. Nov. 13, 2007) (upholding search of cell phone history log as consistent with *Finley*); United States v. Mercado-Nava, 486 F. Supp. 2d 1271, 1277-79 (D. Kan. 2007)

At the same time another view of cell phones emerged, articulated first in the unpublished opinion of the Northern District of California in *U.S. v. Park.*[202] Factually, *Park* was not the strongest case for the government in that the police could not recall when they searched the cell phone's address book.[203] In rejecting that this was a search incident to arrest because it was not contemporaneous to arrest, the district court articulated a view of the cell phone as distinct from an ordinary container:

> [M]odern cellular phones have the capacity for storing immense amounts of private information. Unlike pagers or address books, modern cell phones record incoming and outgoing calls, and can also contain address books, calendars, voice and text messages, email, video and pictures. Individuals can store highly personal information on their cell phones and can record their most private thoughts and conversations . . . through email, and text, voice, and instant messages.[204]

This conceptualization of the cell phone has more recently been shared by many courts who favor this understanding of the cell phone as potentially highly personal.[205] One of the clearest discussions of this issue was made in *Ohio v. Smith*, where the Ohio Supreme Court analyzed the court split, con-

(upholding search of cell phone that involved the downloading of memory and the accessing of stored numbers).

[202] *Park*, 2007 WL 1521573.

[203] *Id.* at *3 (police agreed that phone was searched at least at the time of inventory).

[204] *Id.* at *8; *see also* Gershowitz, *supra* note 157, at 29 ("[T]he iPhone is a handheld wireless device that functions as a cell phone, BlackBerry, camera, music player, and video player, while simultaneously providing Internet access."). Gershowitz argues that the iPhone changes everything because of its capability of storing tremendously more information, as well as its ability to access additional information. *Id.* at 41-42.

[205] *E.g.*, State v. Smith, 920 N.E.2d 949, 953 (Ohio 2009) (rejecting *Finley* and embracing *Park* in a search based on those particular facts); United States v. Quintanua, 594 F. Supp. 2d 1291, 1299 (M.D. Fla. 2009) (citing to *Zavala* and rejecting search of photographs on phone as not justified under the dual rationale of officer safety and evidence preservation); United States v. Wall, No. 08-60016-CR, 2008 WL 5381412, at *3 (S.D. Fla. Dec. 22, 2008) (Court "declines to adopt the reasoning of *Finley*" and the analogy between pagers and cell phones in which evidence of incoming phone numbers could be lost if not immediately preserved, in favor of a *Park* analysis).

cluding that courts that treated cell phones like containers were immersed in old, outdated technology.[206] The Ohio Supreme Court further acknowledged this tension between treating cell phones as small computers or as ordinary containers: "Given their unique nature as multifunctional tools, cell phones defy easy categorization. . . . Their ability to store large amounts of private data gives their users a reasonable and justifiable expectation of a higher privacy in the information they contain."[207] This court recognized the "continuing rapid advancements in cell phone technology" in smartphones and their capability to both store large amounts of data as well as access the Internet.[208] In so doing, this court also rejected any requirement that officers discern the capability of cell phones before acting.[209] Notably, a four justice dissent rejected this analysis and embraced the concept of the two circuit court opinions in *Finley* and *Murphy*[210] that applied traditional Fourth Amendment principles asserting that a cell phone's digital address book is akin to traditional address books carried on the person.[211]

Notwithstanding these differing conceptions of cell phones in the case law, a shared recognition emerges from the cases: all cell phone searches are not equal. It is highly relevant exactly what the police examine on the phone. It matters if the police simply review the address book located on the phone, or access photos, text messages, or the Internet. In this hypothetical, S.S.'s expectations of privacy may vary between the numbers that appear on the screen during incoming calls and a password protected social networking site not actually located on the phone.[212]

---

[206] *Smith*, 920 N.E.2d at 954.

[207] *Id.* at 955.

[208] *Id.* at 954.

[209] *Id.; see also* United States v. Murphy, 552 F.3d 405, 412 (4th Cir. 2009).

[210] *Murphy*, 552 F.3d at 412 (4th Cir. 2009) (affirming denial of motion to suppress evidence from cell phone).

[211] *Smith*, 920 N.E.2d at 957. (Cupp, J., dissenting).

[212] Drawing a legal distinction between information physically located on or off the cell phone is likely an unwise choice, given that technology seems to be moving in the direction of "cloud" computing. With cloud computing, the actual data is physically located in a remote location and the device simply provides access to information stored

To further complicate matters, the conceptualization of the cell phone is anything but static. For example, even if one were to embrace a *Park* analysis that phones are special due to their ability to hold vast data, as technology has advanced, the ability to remove this data from phones may allow for police to search them due to this new exigency.[213] Technological advances create new exigencies. The Computer Crime & Intellectual Property Section of the United States Department of Justice (CCIPS) and some courts have cited the ability of some phones to receive "a kill command . . . that will cause the device to encrypt itself or overwrite data stored on the device."[214] However, the fact that this technology exists surely cannot always create an exigency.[215] On the other hand, what burden will be on law enforcement to determine whether this remote

on a remote server. Shari Claire Lewis, *Cloud Computing Brings New Legal Challenges*, LAW.COM (July 8, 2009), http://www.law.com/jsp/article.jsp?id=1202432062900. While the definition of cloud computing remains less defined, it "involves the sharing or storage by users of their own information on remote servers owned or operated by others and accessed through the Internet or other connections." ROBERT GELLMAN, THE WORLD PRIVACY FORUM, PRIVACY IN THE CLOUDS: RISKS TO PRIVACY AND CONFIDENTIALITY FROM CLOUD COMPUTING 4 (2009). Examples include video sites, photography sites, webmail such as Hotmail, Google Docs, etc. *Id.*; Alan Wernick, *A Legal Fog*, CHICAGO LAW., May 2009, at 49.

[213] *See*, *e.g.*, John Boudreau, *Get Ready for 3G: Apple Adds New Functions*, SAN JOSE MERCURY NEWS (July 7, 2008, 1:34 AM), http://chetansharma.com/blog/2008/07/07/iphone-3g-has-business-appeal.html (discussing how 3G iPhone supports "remote wipe" or the ability to instantly remove data remotely).

[214] U.S. DEPT. OF JUSTICE, *supra* note 197, at 30. United States v. Young, Nos. 5:05CR63-01-02, 2006 WL 1302667, at *13 (N.D. Wash. May 9, 2006) (exigent circumstances justified searching a cell phone for text messages where the cell phone had an option for auto deleting messages after one day); United States v. Valdez, No. 06-CR-336, 2008 WL 360548, at *3 (E.D. Wis. Feb. 8, 2008) (search of phone's address book and call history reasonable because, among other reasons, testimony from law enforcement indicated that the cellular provider enabled customers to remotely delete all of the information located on the cell phones); *see also* David C. Morrison, *Behind the Lines*, CONG. Q.: HOMELAND SECURITY, May 2010 (quoting CDNet, "A remote wipe feature on Blackberry and iPhone smartphones protects privacy but 'also allows the accomplices of criminals and terrorists captured by law enforcement remotely to erase all incriminating and intelligence-related data.").

[215] *See* United States v. David, 756 F. Supp. 1385, 1392 n.2 (D. Nev. 1991) (rejecting government argument that exigent circumstances support searching battery-operated computer because agent did not know how long batteries would last).

deletion ability is on the device in question?[216] To further complicate matters, some have noted that cell phones almost never have an exigency because cell phone providers keep records of calls and contents of text messages for at least a few weeks, which can be preserved and retrieved.[217]

While most of these cases have found at least a reasonable expectation of privacy in the phone, the Supreme Court has declined to rule directly. In this hypothetical, one could argue that S.S. did not have a reasonable expectation of privacy to the phone because she brought it to school aware of the school policy that if left on and in use, it could be confiscated by officials. She did not demonstrate a subjective expectation of privacy. However, pending threatened and actual litigation in analogous school searches (in which schools have seized cell phones due to the infraction of the cell phone policy and went on to search them) raises the question as to whether the knowledge of the policy to seize phones waives the right to protect them from search.[218]

Even if school officials could establish that S.S. lacked a reasonable expectation of privacy in the phone, the cases above demonstrate that what is searched matters significantly. Officials in our hypothetical reviewed incoming phone calls, con-

---

[216] United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009) (rejecting arguments that police must ascertain storage capacity of phone prior to searching it).

[217] *See, e.g.*, State v. Smith, 920 N.E.2d 949, 955-56 (Ohio 2009) (rejecting the argument that the possibility of permanent deletion of cell phone records yields exigency for a search: "even if one accepts the premise that the call records on Smith's phone were subject to imminent permanent deletion, the State failed to show that it would be unable to obtain call records from the cell phone service provider, which might possibly maintain such records as part of its normal operating procedures"); Mathew Orso, *Cellular Phones, Warrantless Searches, and New Frontier of American Jurisprudence*, 50 SANTA CLARA L. REV. 183, 199 (2010).

[218] Scott Smith, *Cell Text Snooping Draws Ire: Linden School Changes Policy After Incident*, THERECORDNET.COM (Apr. 18, 2008, 12:00 AM), http://www.recordnet.com/apps/pbcs.dll/article?AID=/20080418/A_NEWS/804180326/-1/A_NEWS04 (school announces change in policy after teacher seized cell phone and then read three weeks worth of text messages and the ACLU challenged the policy); Sue Lindsay, *Boulder District OK's Cell Phone Search Limits*, DENVER ROCKY MOUNTAIN NEWS (Apr. 22, 2008, 12:05 AM), http://www.rockymountainnews.com/news/2008/apr/22/boulder-district-oks-cell-phone-search-limits.html (school reaches agreement with ACLU to not review contents of confiscated cell phones unless imminent risk to public safety).

tacts, and text messages. They also pressed one button to access S.S.'s social networking site.[219] The social networking site and email accounts presumably have passwords associated with them if accessed in a "normal" way from a computer. However, assume S.S., like many others, created an unimpeded shortcut to these accounts through one button on her phone. Typically the presence of a password can indicate a subjective expectation of privacy.[220] However, the government could argue that the creation of a one button method to bypass the password, combined with bringing the cell phone to a school setting knowing it could be accessed if seized, may be enough to establish a failure to exhibit an expectation of privacy.

This assumes the social networking site has limited access. However, privacy settings on such sites can be misleading and can cause youth to believe access is limited to con-

[219] Some smartphones provide mechanisms for accessing information on the Internet with the touch of an icon or button, circumventing a password.

[220] United States v. Gines-Perez, 214 F. Supp. 2d 205, 225-26 (D.P.R. 2002) (no reasonable expectation of privacy in photo on webpage "without taking any measures to protect the information"), *remanded on other grounds* 90 F. App'x 3 (1st Cir. 2004). *But cf.* Brown-Criscuolo v. Wolfe, 601 F. Supp. 2d 441, 449-50 (D. Conn. 2009) (concluding that a principal had a reasonable expectation of privacy in her personal email communication on her office computer, a prime rationale being that the computer was password-protected and no third parties had access to her computer); United States v. Rosario, 558 F. Supp. 2d 723, 727-27 (E.D. Ky. 2008) (no reasonable expectation of privacy when one takes no safeguards to protect the computer contents, such as utilizing a password shield restricting access to third parties); United States v. Heckencamp, 482 F.3d 1142, 1146-47 (9th Cir. 2007) (the government conceded that Heckencamp had a subjective expectation of privacy and the court held that an objectively reasonable expectation existed "in his personal computer, which was protected by a screensaver password, located in his dormitory room, and subject to no policy allowing the university actively to monitor or audit his computer usage"); United States v. Barrows, 481 F.3d 1246, 1248-49 (10th Cir. 2007) (giving great weight to fact that defendant did not "password protect his computer, turn it off, or take any other steps to prevent third-party use," thus rejecting a reasonable expectation of privacy claim); United States v. Ziegler, 474 F.3d 1184, 1189-90 (9th Cir. 2007) (password protected computers are sufficient for a finding of subjective expectation of privacy and a locked office in the workplace constituted a reasonable expectation in that space); Trulock v. Freeh, 27 F.3d 391, 403 (4th Cir. 2001) (a reasonable expectation of privacy in password-protected computer files is analogous to a locked footlocker, which cannot be searched without a warrant or consented to a search by a third party).

tacts.[221] Similarly, some courts have found no expectation of privacy in photos posted online.[222] These facts could indicate that the information obtained by school officials was publicly available. However, the fact that equivalent information can be obtained by other means does not make an unlawful search lawful.[223]

In the end, the traditional *Katz* analysis of privacy expectation creates more questions than answers. Although a cursory analysis suggests an expectation of privacy, deeper review of cell-phone-search case law combined with technological advancements allows litigants much leeway in arguing even that issue. This could result in exposing private information, even password protected information, to law enforcement review.

b. Even If a Search, Under TLO's *and* Redding's *Decreased Standards, Significantly Little Protection For S.S. May Exist*

One could argue that the outcome of the above analysis is without significance because, while this is an unreasonable search of an adult, *T.L.O.* and *Redding* do little to protect students from such an intrusion. *T.L.O.* is an older case and *Redding* offered no significant alteration of *T.L.O.*'s standard. However, youths' sense of privacy may be altered more today than in the past not so much because of a weakening of legal protections post-*T.L.O.*, but because the amount of information available to a school official engaged in the lawful search has grown significantly. As Professor Kerr points out, the difference between the physical world and the digital world is that "physical environments generally limit the scale and location of evidence but digital environments normally do not."[224] Thus, the privacy invasion felt by T.L.O. and Redding was physically limited to what could be fit within the purse or backpack re-

---

[221] Grimmelmann, *supra* note 28, at 1160. ("The social dynamics of social network sites do more than just give people reason to use them notwithstanding the privacy risks. They also cause people to *misunderstand* those risks.") *Id.* at 1164; *see also supra* note 56 and accompanying text.

[222] *Gines-Perez*, 214 F. Supp. 2d at 225-26.

[223] Kyllo v. United States, 533 U.S. 27, 29-30, 35 n.2 (2001).

[224] Kerr, *supra* note 97, at 1012-15.

spectively.[225] Because these were limited by physical boundaries, the decreased privacy rights, decreased necessary suspicion, and lack of a warrant requirement can be seen as on balance with the compelling need of the school officials to maintain order and discipline. However, when these same decreased standards now allow access to a vast array of personal information, the unsatisfactory outcome of this standard becomes more apparent.

The first step in analyzing a student search under a traditional analysis is to determine if the examination of the phone was justified at its inception. This examination encompasses reviewing S.S.'s call history, text messages, address book, and her social networking site. To do so, officials must have a reasonable suspicion that these activities will yield evidence of violation of the law or school rule.[226] As phrased in *Redding,* a "moderate chance" must exist that such evidence will be found.[227] Given that there is credible information that within the hour students will be meeting and ingesting prescription medication, that S.S. was linked to this activity by two students (one of whom appears to both be friends with S.S. but also has a self-interest in inculpating S.S.), and that S.S. acknowledged ownership of the day planner and lending it to M.G., there appears a "moderate chance" that her cell phone, now repeatedly receiving calls or text messages just prior to the appointed distribution time, contains evidence of a violation of school policy. Similarly, the pattern of calls may also provide information about who else is involved, or may corroborate her relationship with the other two students.[228] Received texts and announcements on her social network site or wall posts all

[225] That is not to say the search of her person was not invasive because it also was limited to her person. Invasions of privacy in the physical world certainly can be severe. Such is why *Redding* noted that a strip search is in a unique category of its own due to its nature. Safford Unified Sch. Dist. #1 v. Redding, 129 S. Ct. 2633, 2641-42 (2009).

[226] New Jersey v. T.L.O., 469 U.S. 325, 342 n.8 (1985).

[227] *Redding*, 129 S. Ct. at 2639.

[228] *E.g.*, People v. Chho, No. CC822335, 2010 WL 1952659, at *5 (Cal. Ct. App. May 17, 2010) (probable cause to search cell phone existed in the totality of circumstances where presence of illegal drugs was coupled with continuous ringing of telephone).

have a moderate chance of yielding evidence as research indicates that this is a primary way in which youth communicate and arrange their social lives.[229] Consequently, such a low standard, combined with technological vulnerabilities and volume of information, may create the unintended consequence of a loss of protections for access to diaries, interpersonal communication with unrelated parties, and personal data and photographs.

The next step is to review whether the search was intrusive in light of the age or sex of the student.[230] Here age is most relevant. As has been demonstrated, some studies suggest that youth can be more liberal in sharing personal information by conceptualizing the risks to exposing such information differently. Therefore, what may be perceived as excessively intrusive to a digital immigrant may not to a younger person. Furthermore, research suggests the age of the student does matter as older students are more interactive on cell phones than younger students.[231] This could mean that in light of one's age, one's expectation of privacy is very different for youth and the actions appear less intrusive. It is this reality that could risk the demise of legally recognized privacy for youth as society knows it.

The answer to the intrusiveness question is very much connected to exactly what was searched. One published opinion involving a school search of a cell phone, whose holding was limited to denying the school district summary judgment in a civil suit, held that the search exceeded the allowable scope. In *Klump v. Nazareth School District*,[232] school officials seized a student's cell phone when he was observed with it in violation

---

[229] AMANDA LENHART & MARY MADDEN, PEW INTERNET & AMERICAN LIFE PROJECT, TEENS, PRIVACY & ONLINE SOCIAL NETWORKS 6 (2007), *available at* http://www.pewtrusts.org/uploadedFiles/wwwpewtrustsorg/Reports/Society_and_the_Internet/PIP_Teens_Privacy_SNS_Report_Final.pdf (detailing the frequency of Internet use by teenagers and noting that social network sites as a communication tool is the primary reason for joining).

[230] While sex seems less relevant than in the context of the actual case, research indicates that girls Redding's age are more likely to post information online and communicate with others. *See supra* note 43.

[231] *See* MCQUADE & SAMPAT, *supra* note 23, at 32.

[232] 425 F. Supp. 2d 622 (E.D. Pa. 2006).

of the school policy.[233] School officials then accessed the phone's directory to obtain numbers of other students and called them to determine whether they would violate school policy by answering their cell phones on campus.[234] As if that were not enough, officials then accessed voicemail and text messaging functions, at one point conversing with Klump's brother without properly identifying themselves.[235] At some point a text arrived on the phone indicating possible drug activity, but the parties disputed when that occurred.[236] At the summary judgment stage, the court was bound to view the facts in favor of Klump.[237] As such, the court found that the seizure of the phone was justifiable.[238] However, accessing the directory and the calls were not justifiable under *T.L.O.* because such activity was designed to find evidence of other students' misconduct for which they had no reasonable belief was occurring.[239]

In contrast, in this hypothetical an argument may be made that the calls within the last hour could lead to evidence of a violation. However, searching older text messages or call logs may exceed what is necessary. Similarly, searching all of S.S.'s contacts may also be excessive in scope. Finally, access to social networking may at first seem intrusive. However, when one recalls the research that girls are most likely to create content online, that youth are less likely to protect it from public view, and that social networking sites are a primary method of scheduling and tracking contacts, the scope may not be excessive. Finally, given that S.S.'s phone is a smartphone, the police may be able to establish an exigency to do a more intrusive search for fear of the "kill order."

While the result of such a motion may be unclear under a traditional analysis, it would seem that the combination of the low standard in *T.L.O.* combined with the decreased privacy rights and understandings of privacy for these youth, may

---

233 *Id.* at 630.
234 *Id.*
235 *Id.*
236 *Id.* at 631, 639.
237 *Id.*
238 *Id.* at 640.
239 *Id.*

combine to allow access to vast amounts of personal data and diminish a privacy expectation for a large class of people.

2. Justice Harlan's Fundamental Approach

Justice Harlan recognized the acceptance of his two-part test. He cautioned, however, against a "substitution of words for analysis."[240] Therefore, he felt the law should translate not only rules and customs, but also "values," thus forcing the Court to not only recite expectations, but ultimately to examine "the desirability of saddling [burdens] upon society."[241]

For Justice Harlan, his inquiry would begin with the threshold question of whether under the Constitution and system of government, society should impose upon students the risks of invasion into their cell phones or other digital media without procedural protections.[242] This is determined by (1) assessing the nature of the practice; (2) assessing its likely impact on the individual's sense of security; and (3) balancing that against the utility of the conduct.[243]

The nature of the practice must be broken into the different examinations. In this hypothetical, the nature of school officials examining the outside of the phone and incoming calls is distinct from pressing at least one button to further examine the call log, taking an additional step to review text messages, or pressing an icon to gain access to a social networking site. Each of these practices can be considered a step further into the suspect's private phone.[244] While the Court has recognized the special nature of the school's relationship with students and the "substantial interest" in maintaining discipline on school grounds,[245] one might find the nature of this practice of examining phones for information of impending drug consumption on school property inherently reasonable. However, as the school official accesses additional information stored in the

---

[240] United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

[241] *Id.*

[242] *Id.*

[243] *Id.*

[244] Gershowitz, *supra* note 97, at 45-57.

[245] New Jersey v. T.L.O., 469 U.S. 325, 339-40 (1985).

phone, and then on S.S.'s social networking site, the intrusion becomes more attenuated from the valid interest in maintaining a learning environment in the school.

As to the second prong, the presence of a school policy affects the impact these different examinations have on the individual. If a youth has advance notice as to the likelihood of her cell phone being searched on school property, then she is afforded the opportunity to avoid the possibility of such an intrusion by avoiding the use of a cell phone on campus. However, if, such as in *Klump*, the policy is only for cell phone use (here arguably S.S. was not using her phone; others were leaving her messages), and allows only for seizure of the phone and not its search, it is likely that there is a significant impact on S.S.'s sense of security. This impact may or may not grow as to the social networking examination. If she has put in place password protections or limited access to this site, the impact on her sense of security is great. However, if the information on that site is available for the public to see, query whether the fact that her phone was used to gain access to publically available information creates a privacy expectation that did not otherwise exist.

These fact-driven concerns must be balanced against the third prong: the utility of this conduct. Here an argument can be made to support all sides. School officials correctly point out that some students facilitate violations of school regulations and laws through social networking sites. They plausibly argue they would be remiss in failing to recognize that and, thus, explore such sites in their effort to maintain a safe learning environment. In the S.S. example, presented with the possibility that several students will soon be ingesting prescription medication, one could argue that perhaps there is utility is searching the phone and text traffic directly preceding the event. On the other hand, S.S. could reasonably argue that the sudden burst of calls was prompted by her removal from class and that her presence in the vice principal's office is more likely the source of this traffic. She could further argue that because the information officials seek can be obtained by a warrant to her cell phone company, there is no utility in this practice. This

argument would have more force if there were no impending event.

Justice Harlan's approach does not lead to a decisive answer. It is as fact-driven as the traditional analysis but a better approach because it asks the right questions, i.e., whether this *should* be done. Furthermore, it increases protections for a compromised class by examining the fairness and propriety of an invasion of privacy without a warrant. Such an approach, while imperfect, does offer a more reasoned analysis of the implications of "saddling" youth with such a security challenge.

3. Justice Blackmun's Normative Approach

A majority of the Court in *Smith v. Maryland* recognized that circumstances can occur in which an individual's subjective expectation "has been 'conditioned' by influences alien to well recognized Fourth Amendment freedoms" and that when such occurs, the subjective expectations should have little or no role in ascertaining the scope of Fourth Amendment protections.[246] According to Justice Blackmun, when such a situation arises, the Court should engage in a "normative inquiry" to determine the validity of the governmental action.

The apparent simplicity of this solution is belied by the necessary inquiry. As a threshold matter, one must determine if this is such a situation where expectations have been conditioned in such a way as Justice Blackmun describes. To reach Blackmun's analysis, our hypothetical assumes that S.S. has no subjective expectation of privacy because she came to school with a cell phone displayed and lacking password protection, and the information placed on her social networking site is available to at least some third parties.[247] However, that would not end the inquiry. Has she been conditioned to think in this way? One might argue that she has been so conditioned, based on her youth and her status as a digital native for whom tech-

[246] Smith v. Maryland, 442 U.S. 735, 741 n.5 (1979).

[247] That is not to say this is the correct conclusion. This is merely assumed to allow examination of Blackmun's approach in situations where *Katz* fails.

nological sharing of information—sometimes at her own risk—is the natural order.

Unlike the situation that Justice Blackmun warned against—that the government could reduce subjective expectations merely by announcing its intent, and then exploit those reduced expectations by acting on its announced intention[248]—S.S.'s "conditioning," assuming it exists, was not directly caused by the government. Rather, she and her age cohort, through their differing conceptions of privacy, have arguably conditioned themselves to forego some traditional privacy protections. Or, one could argue they have been conditioned in this regard by the companies who collect and sell their information.[249] Either way, they have done so despite warnings from teachers and other public employees to *limit* their exposure online.[250] Consequently, just as the defendant in *Smith*, youth arguably choose to utilize the Internet and manage their privacy in ways that produce known privacy compromises.

Even assuming that this conditioning of youth sufficiently compromises their subjective expectation of privacy, the next step, this normative inquiry, is not without challenges.[251] First, whose normative should be used? The fundamental problem society may be facing is not the isolated diminished expectation of privacy of an individual, but that of an entire class of people. For an individual, one can more easily examine what general social norms are. Regarding a class, however, it is unclear whose normative applies. It is nearly impossible to isolate or justify the norms of one class as the measure. For example, it is difficult to imagine the propriety of a different privacy standard between the wealthy and poor; professional and laborer; or young and old. A second approach is to attempt to measure broader societal norms. Doing so could lead to minimizing

---

[248] *Smith*, 442 U.S. at 741 n.5 (offering examples such as the government announcing that all homes will be subject to warrantless entry or that a refugee from a totalitarian country assumes the government continuously monitors him).

[249] *See supra* note 56 and accompanying text.

[250] *See generally Protecting Youths in an Online World: Hearing before the S. Subcomm. on Consumer Protection and the Comm. On Commerce, Science, and Transportation*, 111th Cong. (2010) (statement of Chairman John D. Rockefeller IV).

[251] See *supra* note 109 for a discussion about "normative."

youth's norms from that calculus. With youth's actual experiences excluded from the process, the analysis creates a false sense of what "society" is willing to accept. In essence it would be excluding from an alleged normative analysis what the majority of users online expect.

The final problem with such an approach is that there seems to be no general understanding today of cell phone, text message, and social networking privacy. Americans have occupied houses with yards for generations, giving courts a firm basis on which to assess societal expectations of privacy in connection with them in *Ciraolo* or sealed letters in *Jackson*.[252] However, courts have struggled with exactly what society is willing to recognize when it comes to electronic media as it is now, before societal expectations have been established. Furthermore, in 2010 the Supreme Court declined to make any broad judgments regarding expectations of privacy in text messages because the issue reached the Court "before its [the emerging technology] role in society has become clear."[253] This lack of clarity is aggravated by the fact that society is trying to come to terms with a moving target of much more rapidly developing technology. "Rapid changes in the dynamics of communication and information transmission are evident not just in technology itself, but in what society accepts as proper behavior. . . . At present it is uncertain how . . . norms, and the law's treatment of them, will evolve."[254] Therefore, Blackmun's appraisal has significant shortcomings.

CONCLUSION

Society, with this rapid technological development, finds itself in an unexpected place. The Court sought to guard against an erosion of privacy, among other values, caused by the government. Today, however, a situation unanticipated by the Court has developed where there is an erosion of privacy, but a conditioned erosion driven by a combination of youthful

---

[252] *Ex parte* Jackson, 96 U.S. 727 (1877).

[253] City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010).

[254] *Id.* at 2629-30.

viewpoint and exuberance and rapid technological advances. This development challenges traditional notions of privacy expectations. Of the options discussed, Justice Harlan once again poses the most viable solution. While the resolution of "what if Savana Redding had a cell phone?" may not be any easier to reach through his alternative balancing test, the strongest answer is not always the easiest. Justice Harlan's test, while no simpler, may be the truer. It asks the right questions: in its most basic form, *should* youth be saddled with risking such an invasion of their privacy simply because of their age and technological savvy? Harlan's formula allows courts to examine the actual practice at issue with that question in the background. It also allows room for the reality that the school setting may indeed require "some easing of the restrictions" on searches for the safety of the suspect and others.[255]

Expectations of privacy are evolving and technology's advancement warns against tying social norms and subjective expectations to current technological capabilities. Therefore, the Court's assumption-of-risk approach may become a sterile self-fulfilling exercise unless a more fundamental value-laden analysis is made to determine whether the invasion at issue should occur with or without protection from the Fourth Amendment, and if so, then what degree of protection the Amendment should afford.

[255] New Jersey v. T.L.O., 469 U.S. 325, 340 (1985).