# KIDS THESE DAYS: SOCIAL MEDIA, EVOLVING EXPECTATIONS OF PRIVACY, AND IMPLICATIONS FOR THE FOURTH AMENDMENT

*Lori A. Hoetger**

*While scholars have suggested social media and other digital communications are eroding expectations of privacy, there is minimal evidence supporting this concern. The present Article provides an important look into how expectations may be changing with two empirical studies examining whether age is related to expectations of privacy. Age could be related to privacy protections either because, (1) development of decision making affects how people view their privacy (Developmental Hypothesis) or (2) there are societal differences that shape privacy expectations that have changed over time (Generational Hypothesis). The first study compares prior research on adult expectations of privacy and court holdings with adolescents' expectations of privacy and finds that, while there are some similarities among these groups, adolescents' expectations do differ from adults' in several key aspects. The second study attempts to explain why there is this difference. By comparing expectations of privacy with age, experience with social media, and development of decision making capabilities, the second study finds limited support for both the Developmental and the Generational Hypotheses. The Article concludes with recommendations on ways courts can use empirical research to remain cognizant of evolving expectations of privacy in the digital age.*

* Assistant Professor of Law, University of Nebraska. Substantial work on this paper was completed while I was a Visiting Assistant Professor at the University of Illinois College of Law. I thank my amazing advisor, Eve Brank, her wonderful graduate students, Kate Hazen, Josh Haby, Emma Marshall, and Lindsey Wiley, and the undergraduate research assistants for their excellent assistance throughout my dissertation. I would also like to thank Eric Berger, Jeremey McClane, Bob Lawless, Andy Leipold, Jason Mazzone, Jennifer Robbennolt, Christopher Slobogin, Matthew Tokson, Lesley Wexler, and the University of Minnesota's law school faculty for providing helpful feedback and guidance in developing this paper. This research was supported by a National Science Foundation Law and Social Sciences Dissertation Enhancement Grant.

TABLE OF CONTENTS

## I. INTRODUCTION

During COVID-19 shutdowns, school districts developed a new way to spy on their students: school-provided computers like Chromebooks or laptops.[1] Many of these devices came equipped with monitoring software such as Gaggle, which alerts schools if students use the device for certain illicit purposes, including sending profanity or searching for nudity.[2] In addition to alerting schools of safety and security concerns, the software also revealed other sensitive information, such as students' sexual orientation, potentially outing students when they had kept their orientation a secret.[3] The software didn't stop there, though, as some schools reported learning of text messages composed of potential nudity sent outside of school hours on student-owned devices, when students would plug their phones in to their school-provided device to charge it and the device would automatically upload information stored on the phone.[4] And schools did not keep this information to themselves; 44% of teachers said that at least one of their students had law enforcement contact for some behavior flagged by the student monitoring software.[5]

While there is some apprehension about the rise in surveillance in recent years, privacy concerns are nothing new. In 1949, George Orwell published a book set in the (then) future year of 1984, depicting a government that constantly monitors its citizens through the use of two-way television screens in homes, screening of written correspondence, and undercover agents.[6] We are now four decades past the time period in which the book was set, and while not all of the book's government practices are actually used, numerous societal changes have impacted how much of our lives are on display. From an innocent Christmas toy keeping watch over young children to report their behavior to Santa Claus,[7] to the revelation of a widespread government surveillance program of citizens' metadata from cellular phones and internet usage,[8] societal developments have led scholars to express concern over the future of our privacy rights.[9]

Public figures' statements demonstrate potentially diminishing privacy expectations. A counselor to the United States president in 2017 expressed dismay over the ability to surveil individuals through phones, television sets, and

1. Pia Ceres, *Kids Are Back in Classrooms and Laptops Are Still Spying on Them*, WIRED (Aug. 3, 2022, 12:01 AM), https://www.wired.com/story/student-monitoring-software-privacy-in-schools/ [https://perma.cc/V7RZ-KQWQ].

2. *Id.*

3. *Id.*

4. *Id.*

5. *Id.*

6. *See generally* GEORGE ORWELL, 1984 (1949).

7. Laura Pinto & Selena Nemorin, *Who's the Boss? "The Elf on the Shelf" and the Normalization of Surveillance*, CAN. CTR. FOR POL'Y ALTS. (Dec. 1, 2014), https://policyalternatives.ca/publications/commentary/who%E2%80%99s-boss [https://perma.cc/7R6R-ZAGA].

8. *See generally* Sören Preibusch, *Privacy Behaviors After Snowden*, 58 COMMC'NS ASS'N FOR COMPUTING MACH. 48 (2015).

9. Mary Graw Leary, *Reasonable Expectations of Privacy for Youth in a Digital Age*, 80 MISS. L.J. 1035, 1037–38 (2011).

microwaves that all have camera capabilities.[10] Mark Zuckerberg, founder and CEO of one of the most popular social media sites—Facebook—declared there's a new "social norm" of sharing information with others, and the chief executive of Sun Microsystems—a former computer and software company—once quipped, "You have zero privacy anyway. Get over it."[11] Concern over the safety of our information may be well-founded: researchers pretending to be marketing a new product purchased large datasets of German citizens' internet browsing habits and were able to identify individual users to the point they uncovered a local judge's preference of pornography and the medication used by a German politician.[12]

In addition to expressions of diminished expectations of privacy, individuals sometimes exhibit behavior that seems completely contrary to any interest in privacy. Several communities have experienced so-called "sexting" scandals where youth share and circulate naked photographs of themselves or other adolescents—which not only can have personal and professional ramifications—but legal as well.[13] Twenty percent of adolescents aged thirteen to nineteen report sending or posting online nude or semi-nude photographs of themselves.[14] One possibility for this phenomenon is that adolescents have different expectations of privacy and this impacts their behaviors. This difference may be attributable to the development of risk-taking and decision making capabilities (the Developmental Hypothesis) or to a "generation gap" such that teens today view privacy very differently and will continue to do so even when they are adults (the Generational Hypothesis).

The Fourth Amendment only protects against government intrusions into spaces or information that receive a reasonable expectation of privacy—a subjective expectation of privacy that society is prepared to recognize as reasonable.[15] Scholars have expressed concern over the impact the ubiquity of electronic communications may have on our expectation of privacy[16] and on the potentially circular nature of the reasonable expectation of privacy test itself.[17] Additionally, judges are tasked with determining when a reasonable expectation of privacy

10. Michael A. Memoli, *Kellyanne Conway on Surveillance: We Have 'Microwaves That Turn into Cameras'*, L.A. TIMES (Mar. 13, 2017, 10:03 AM), http://www.latimes.com/politics/washington/la-na-essential-washington-updates-more-than-just-spying-microwaves-why-1489416182-htmlstory.html [https://perma.cc/93WK-5UQD].

11. Helen A.S. Popkin, *Privacy Is Dead on Facebook. Get over It.*, NBC NEWS (Jan. 13, 2010, 7:56 AM), https://www.nbcnews.com/id/wbna34825225 [https://perma.cc/E34J-2M4A].

12. Alex Hern, *'Anonymous' Browsing Data Can Be Easily Exposed, Researchers Reveal*, GUARDIAN (Aug. 1, 2017, 7:17 PM), https://www.theguardian.com/technology/2017/aug/01/data-browsing-habits-brokers [https://perma.cc/K2F9-A7CR].

13. Evan Millward, *Six Grant County Teens Charged After Sexting Scandal*, WCPO CIN. (May 16, 2017, 11:50 PM), https://www.wcpo.com/news/local-news/grant-county/six-grant-county-middle-schoolers-arrested-after-sexting-scandal [https://perma.cc/E6RQ-V36S].

14. KAITLIN LOUNSBURY, KIMBERLY J. MITCHELL & DAVID FINKELHOR, CRIMES AGAINST CHILD. RSCH. CTR., THE TRUE PREVALENCE OF "SEXTING" 1 (2011).

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

16. Leary, *supra* note 9, at 1035.

17. *See generally* Matthew B. Kugler & Lior Jacob Strahilevitz, *The Myth of Fourth Amendment Circularity*, 84 U. CHI. L. REV. 1747 (2017).

exists—but how can we expect judges to evaluate societal expectations of privacy with constantly new and emerging technologies that could, at least in theory, change societal expectations?

This Article addresses the question of whether electronic communication (particularly social media) is eroding societal expectations of privacy. The goal is to test the hypothesis posited by numerous scholars that use of digital communications and technology is eroding our sense of privacy and, in turn, will narrow the scope of the Fourth Amendment over time. Part II provides an overview of the Fourth Amendment reasonable expectation of privacy test. Part III details previous empirical research on lay people's expectations of privacy, and Part IV describes two empirical studies measuring expectations of privacy.[18] Age-related differences in expectations of privacy could be due to developmental differences in decision making (Developmental Hypothesis), experiences with social media (Generational Hypothesis), or both. The results show that as individuals get older, they tend to view electronic communications as more personal in nature and searches of such information as more intrusive; this difference is related to both frequency of social media use and at least one aspect of developmental decision making. This partially supports the Generational Hypothesis, but also indicates that development plays a role. Part V concludes that there is at least some empirical support for the claim that expectations of privacy are changing due to technology use, and empirical research can be an important tool for judges evaluating societal expectations of privacy.

## II. THE CHANGING NATURE OF THE FOURTH AMENDMENT?

The Fourth Amendment of the United States Constitution states that the right to be free from "unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause."[19] The first inquiry in any Fourth Amendment challenge of a state action is to determine whether a search occurred.[20] The United States Supreme Court has formulated an (allegedly) two-prong test to evaluate whether an individual's reasonable expectation of privacy was violated: (1) the individual claiming a violation of his or her Fourth Amendment right must have had a *subjective* expectation of privacy in the thing or place that was searched, and (2) that expectation of privacy must be one that society is willing to recognize as reasonable.[21] Thus, only challenged actions in which an individual's actual expectation of privacy, that society recognizes as reasonable, is violated would be a search under the Fourth Amendment.

18. All methods were approved by the University of Nebraska-Lincoln's Institutional Review Board. *See generally IRB/Human Subjects Research*, UNIV. NEBRASKA-LINCOLN OFF. RSCH. & ECON. DEV., https://research.unl.edu/researchcompliance/human-subjects-research/ [https://perma.cc/V46Z-H6GS] (last visited Mar. 20, 2024).

19. U.S. CONST. amend. IV.

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

21. *Id.*; Smith v. Maryland, 422 U.S. 735, 740 (1979).

In practice, however, courts often ignore claimed subjective expectations.[22] A review of 540 published cases evaluating expectations of privacy decided in 2012 found only 43% of the opinions even mentioned the subjective prong, and even fewer—only 12%—applied the subjective prong to evaluate whether the individual had a subjective expectation of privacy.[23] In contrast, 93% of the opinions mentioned the objective prong and 80% conducted an analysis *only* of whether a claimed expectation of privacy was objectively reasonable.[24] Thus, it appears courts are not concerned with whether an individual claiming a Fourth Amendment violation had an actual, subjective expectation of privacy, and focus more on whether any expectation of privacy, whether or not it exists, is one society is prepared to recognize as reasonable. But this focus has not led to a more straight-forward test.

Though courts tend to ignore the subjective prong, there has yet to be a consistent framework for determining societal, objective expectations, and it remains largely a mystery of how judges distinguish which expectations of privacy society is willing to recognize as reasonable from those society is not. For example, in some instances, courts have relied heavily on trespass[25] or federal regulations,[26] while explicitly excluding such factors from their consideration in other cases.[27] In part, this is a result of the reasonable expectation of privacy test being vague and requiring consideration of many factors.[28] Professor Kerr suggested four different models courts use in determining reasonable expectations of privacy: the probabilistic model, the private facts model, the positive law model, and the policy model.[29] Professor Tokson found courts analyze—at least implicitly—the intimacy of the information searched, the amount of information sought, and the cost of the surveillance, when ruling on reasonable expectations of privacy.[30] But courts are hesitant to adopt a specific model or set of factors to apply in all cases. Without such explicit reasoning, it appears judges rely on their own intuition—perhaps even their own subjective expectations—in reasoning which expectations society is willing to recognize as reasonable.

This struggle is especially apparent and troublesome when we consider the application of the reasonable expectation of privacy test to emerging technologies and electronic communications.

22. *See generally* Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113 (2015) (arguing that the "subjective expectation of privacy" test from *Katz v. United States* exists on paper but has no impact on outcomes).

23. *Id.* at 114.

24. *Id.* at 116–17.

25. *See generally* United States v. Jones, 565 U.S. 400 (2012).

26. *See generally* Florida v. Riley, 488 U.S. 445 (1989).

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

28. *See generally* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503 (2007).

29. *Id.* at 503.

30. Matthew Tokson, *The Emerging Principles of Fourth Amendment Privacy*, 88 GEO. WASH. L. REV. 1, 3 (2020).

### *A. Reasonable Expectations of Privacy and "New" Technologies*

Advances in technology can create problems for the Supreme Court analyzing reasonable expectations of privacy; the Ninth Circuit once called electronic communications such as e-mails and text messages a "new frontier in Fourth Amendment jurisprudence."[31] The Supreme Court has cautioned against determining reasonable expectations of privacy before a technological device's role in society becomes clear.[32] As new devices are developed and become popular, courts have to determine what types of searches the Fourth Amendment protects. This does not happen overnight; cases often take years to work their way to the Supreme Court, so by the time the Supreme Court evaluates expectations of privacy on a certain device, that type of device may be outdated. For example, the Supreme Court decided a case regarding expectations of privacy in text messaging beepers in 2010, long after beepers first became popular,[33] and did not decide a case involving cell phones until 2014, forty years after the first mobile phone call was made.[34]

Since adopting the *Katz* reasonable expectation of privacy test, the Court has seemingly inconsistently applied the test to new and emerging technologies, finding use of a thermoimaging device to measure heat activity in a home violated a reasonable expectation of privacy[35] but flying a helicopter over a backyard did not,[36] and use of an electronic device to monitor suspects' movements on public thoroughfares was not a search,[37] while use of a similar device to monitor movements between private residences and commercial storage units was a search.[38]

The Supreme Court first evaluated how society views cell phones in 2014 when it held that officers generally cannot search a suspect's cell phone incident to arrest without a warrant.[39] Chief Justice Roberts indicated, "cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person."[40] Though the Court did not explicitly address the issue of reasonable expectations of privacy in cellular devices, the opinion indicates the Court recognizes that individuals subjectively feel differently about information stored on their cell phones than they do about other types of information.[41]

The Court's most significant struggle with the Fourth Amendment and technology to date occurred in 2018, with its evaluation of reasonable

31. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904 (9th Cir. 2008).
32. City of Ontario v. Quon, 560 U.S. 746, 759 (2010).
33. *Id.* at 750.
34. Riley v. California, 573 U.S. 373, 378 (2014).
35. Kyllo v. United States, 533 U.S. 27, 40 (2001).
36. Florida v. Riley, 488 U.S. 445, 452 (1989).
37. United States v. Knotts, 460 U.S. 276, 287 (1983).
38. United States v. Karo, 468 U.S. 705, 721 (1984).
39. *Riley*, 573 U.S. at 385.
40. *Id.* at 393.
41. *Id.* at 400.

expectations of privacy in *Carpenter v. United States*.[42] There, the Court addressed a claim that law enforcement's use of a total of 127 days of historical Cell-Site Location Information ("CSLI")[43] violated a suspect's reasonable expectation of privacy. Chief Justice Roberts acknowledged the difficulty in evaluating reasonable expectations of privacy with electronic data collection methods.[44] Instead of strictly applying the third-party doctrine—which holds an individual does not have a reasonable expectation of privacy in information one shares with a third party—to CSLI, the Court focused on the level of intrusiveness in the information the government obtained and the private nature of location information.[45]

The question of whether *Carpenter* changed, augmented, or completely replaced the reasonable expectation of privacy test still remains.[46] In examining whether the collection of CSLI violated a reasonable expectation of privacy, the Chief Justice stated: "In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."[47] Scholars have pointed to this language in delineating factors that are now important to the evaluation of expectations of privacy, at least where it comes to digital information: (1) revealing nature of the information; (2) amount of information collected; (3) number of people affected by given surveillance practice; (4) inescapability of the data collection; (5) automatic nature of the disclosure; and (6) governmental cost of the surveillance.[48] An empirical examination of state and federal cases decided post-*Carpenter* revealed these factors do affect whether a court finds a reasonable expectation of privacy, especially the revealing nature of the data, amount of the data collected, and automatic nature of the data.[49]

The Court was clear to limit its holding to the facts before it, but *Carpenter* is almost certainly not the last time the Supreme Court will face surveillance using electronic data collection techniques, particularly as practices such as geofencing warrants and license plate readers become more common.[50] The First

42. *See generally* 585 U.S. 296 (2018).

43. Cell site location information consists of data collected by cell phone companies when cell phones "ping"—or connect to—nearby cell phone towers. This information can include a singular "ping" at one point in time, or data over a period of time that can be used to track a cell phone's movements. *See Cell Cite Location Information: A Guide for Criminal Defense Attorneys*, ELEC. FRONTIER FOUND., https://www.eff.org/files/2019/03/28/csli_one-pager.pdf [https://perma.cc/8N4E-PXRS] (last visited Mar. 20, 2024).

44. *Carpenter*, 585 U.S. at 313.

45. *Id.* at 315.

46. Tokson, *supra* note 30, at 31.

47. *Carpenter*, 585 U.S. at 319.

48. *See* Tokson, *supra* note 30, at 14 n.83.

49. *Id.* at 59–75.

50. *See, e.g.*, Johana Bhuiyan, *The New Warrant: How US Police Mine Google for Your Location and Search History*, GUARDIAN (Sept. 16, 2021, 7:11 PM), https://www.theguardian.com/us-news/2021/sep/16/geofence-warrants-reverse-search-warrants-police-google [https://perma.cc/NEV6-NN6K]; Jennifer Lynch, *Courts Issue Rulings in Two Cases Challenging Law Enforcement Searches of License Plate Databases*, ELEC. FRONTIER FOUND. (May 5, 2020), https://www.eff.org/deeplinks/2020/05/courts-issue-rulings-two-cases-challenging-law-enforcement-searches-license-plate [https://perma.cc/BDA7-BSPJ].

Circuit, post-*Carpenter*, en banc split evenly in deciding whether law enforcement access to long-term pole camera footage does not violate a reasonable expectation of privacy;[51] the Seventh Circuit has found access to this information never requires a warrant and the Supreme Court has—so far—declined the opportunity to weigh in.[52]

Following *Carpenter*, it appears the third party doctrine does not, by itself, prevent a reasonable expectation of privacy in digital information shared with others, at least where such sharing is automatic and not necessarily voluntary.[53] The question still remains, however, of what reasonable expectation of privacy individuals have in information they *willingly* share with other people—particularly—information that is *designed* to be shared with third parties such as social media.

### *B. Courts' Evaluations of Reasonable Expectations of Privacy in Social Media*

The use of social media—which attracts users with the promise of easily sharing information with a widespread audience—has been on the rise and presents new challenges for courts evaluating expectations of privacy.[54] While the Supreme Court has yet to weigh in, state courts have struggled with this issue with varying results. A Montana court addressed the issue of reasonable expectations of privacy in a Social Networking Site profile.[55] In finding the defendant had both a subjective and objective expectation of privacy in the information he posted on Facebook, the court compared the defendant's Facebook profile to a living room: the defendant's profile was like a living room where he was hosting a party with friends and family, and private messages were like the defendant pulling a friend into his bedroom and closing the door to have a private conversation.[56] The defendant maintained an expectation of privacy of the events that occurred in his living room even though he invited others inside (like "friending" someone on Facebook), and the defendant's expectation of privacy is even greater in the private conversation (like the instant message on Facebook) because he took further steps to keep that information private.[57] In addition, the court cited the widespread popularity of Facebook in reasoning that society recognizes the defendant's expectation of privacy as reasonable.[58] The court found the search was unreasonable.[59]

51. *See generally* United States v. Moore-Bush, 36 F.4th 320 (1st Cir. 2022) (en banc) (per curiam).

52. United States v. Tuggle, 4 F.4th 505, 516 (7th Cir. 2021), *cert denied*, 142 S. Ct. 1107 (Feb. 22, 2022).

53. Carpenter v. United States, 585 U.S. 296, 309 (2018).

54. Esteban Ortiz-Ospina, *The Rise of Social Media*, OUR WORLD IN DATA (Sept. 18, 2019), https://ourworldindata.org/rise-of-social-media [https://perma.cc/TQ66-9GUL].

55. Findings of Fact and Conclusions of Law Supporting January 29, 2015 Order Granting Defendant's Motion to Suppress and Dismiss at 36, Montana v. Windham (Mont. Feb. 5, 2015) (No. DC-13-118C).

56. *Id.* at 31.

57. *Id.*

58. *Id.* at 33.

59. *Id.* at 38–39.

The United States District Court for the District of Minnesota also found an expectation of privacy in private messages sent over Social Networking Sites.[60] Here, a school required a student to turn over her Facebook and email passwords after the school learned the student was having sexually explicit conversations with another student while off-campus.[61] The court held that Facebook messages, like emails, are inherently private and thus users have both a subjective and objective expectation of privacy.[62] Thus, without a warrant or other exception to the warrant requirement, the school could not search R.S.'s private messages or emails.[63]

The Delaware Supreme Court addressed the issue of whether misplaced trust in a "friend" on a social networking site is protected by the Fourth Amendment.[64] A Delaware detective created a fake Facebook profile with a fake name, picture, and other information, and used that page to monitor the defendant, Everett.[65] The Delaware court likened Everett's mistaken trust in accepting a fake profile's friend request to a defendant providing information to an undercover officer, a situation the Supreme Court determined was not a violation of Fourth Amendment privacy rights in *Hoffa v. United States*.[66] According to the Delaware court, individuals assume the risk that one of their social network friends may be an undercover officer or may share information with law enforcement.[67] Thus, at least in Delaware, users have no reasonable expectation of privacy in information willingly posted to social media and accessed by law enforcement, but courts have not established such a rule applicable to all users of social media in all circumstances. In each of these cases, judges have attempted to analogize to nondigital forms of communication or searches, analogies that prove imperfect and difficult to extend.

### *C. Can Judges Adequately Evaluate REP in Technology?*

A potential concern is that courts are not able to adequately gauge expectations of privacy—either subjective or objective—in electronic communication devices due to a lack of experience with new technology.[68] As discussed below, "digital natives" are those who were born into a world constantly connected to the internet and began using electronic communication devices from a young age.[69] The average age of federal judges is estimated at sixty-nine years,[70] and the average age of the current Supreme Court justices is approximately sixty-one

60. R.S. *ex rel.* S.S. v. Minnewaska Area Sch. Dist. No. 2149, 894 F. Supp. 2d 1128, 1142 (D. Minn. 2012).
61. *Id.* at 1133.
62. *Id.*
63. *Id.* at 1147.
64. Everett v. State, 186 A.3d 1224, 1225 (Del. 2018).
65. *Id.* at 1226.
66. *Id.* at 1232–33 (citing Hoffa v. United States, 385 U.S. 293, 302 (1966)).
67. *Id.* at 1237–38.
68. Mary Graw Leary, *The Supreme Digital Divide*, 48 TEX. TECH L. REV. 65, 70 (2015).
69. Marc Prensky, *Digital Natives, Digital Immigrants Part 1*, 9 ON THE HORIZON 1, 1 (2001).
70. Francis X. Shen, *Aging Judges*, 81 OHIO ST. L.J. 235, 237 (2020).

years.[71] According to recent census data, the median age of the United States population is 38 years old[72]—and a difference of thirty years can mean drastic differences in knowledge of and experience with electronic devices.

Questions and comments in oral arguments or to the media have highlighted this potential gap between Supreme Court Justices' and the average person's understanding of technology. For example, during oral arguments for a case examining Fourth Amendment interests in an employer-provided text messaging pager, Chief Justice Roberts questioned: "Maybe everybody else knows this, but what is the difference between the pager and the email?"[73] The Chief Justice—who is undeniably well-educated—also was unaware text messages are first sent to a service provider before being sent to the recipient, opining that he thought, "You push a button, it goes right to the other thing."[74] Justice Kennedy also wondered what happens if a text message is sent at the same time one is received, asking, "Does it say, 'Your call is important to us, and we will get back to you?'"[75] Chief Justice Roberts also appeared not to believe an attorney's assertion that there are many innocent reasons people would have multiple cell phones at the same time.[76] Justice Kagan has publicly admitted the justices are "basically clueless when it comes to technology."[77] The late Justice Scalia expressed his distaste for social media, calling it evidence of a "narcissistic society" that people want to put minute details of their life out there for everyone to see.[78]

At oral arguments in *Carpenter*, the Justices exhibited varying views on expectations of privacy in the digital age. Justice Elena Kagan noted technology, like the GPS tracking the Court evaluated in *United States v. Jones*, now allows law enforcement to conduct 24/7 surveillance of individuals with minimal effort.[79] Justice Sonya Sotomayor mused about the ubiquity of cell phones and analogized to the Court's prior determination that a tracking beeper inside someone's home was subject to Fourth Amendment protections: "I know people who take phones into public restrooms. They take them with them everywhere. It's an appendage now for some people."[80] Scholars have pointed to empirical work to provide a benchmark for judges who may want external information to confirm their intuitions regarding societal expectations of privacy.[81] The next Part

71. *Current Members*, SUP. CT. U.S., https://www.supremecourt.gov/about/biographies.aspx [https://perma.cc/5KYL-95EV] (last visited Mar. 22, 2024).

72. *Nation Continues to Age as it Becomes More Diverse*, U.S. CENSUS BUREAU (June 30, 2022), https://www.census.gov/newsroom/press-releases/2022/population-estimates-characteristics.html [https://perma.cc/8DQQ-6M7W].

73. Transcript of Oral Argument at 29, City of Ontario v. Quon, 560 U.S. 746 (2010) (No. 08-1332).

74. *Id.* at 48.

75. *Id.* at 44.

76. Transcript of Oral Argument at 49, United States v. Wurie, 573 U.S. 373 (2014) (No. 13-212).

77. Will Oremus, *Elena Kagan Admits Supreme Court Justices Haven't Quite Figured Out Email Yet*, SLATE (Aug. 20, 2013, 3:33 PM), https://slate.com/technology/2013/08/elena-kagan-supreme-court-justices-haven-t-gotten-to-email-use-paper-memos-instead.html [https://perma.cc/W42W-GUSB].

78. Jennifer Senior, *In Conversation: Antonin Scalia*, N.Y. MAG. (Oct. 4, 2013), https://nymag.com/news/features/antonin-scalia-2013-10/ [https://perma.cc/MJQ8-AZN4].

79. Transcript of Oral Argument at 47–48, Carpenter v. United States, 585 U.S. 296 (2018) (No. 16-402).

80. *Id.* at 43.

81. Kugler & Strahilevitz, *supra* note 17, at 1776–94.

reviews such research and theories explaining how expectations of privacy develop and may change over time.

## III. EMPIRICAL EVIDENCE OF SOCIETAL EXPECTATIONS OF PRIVACY AND WHY EXPECTATIONS MAY BE CHANGING

### *A. If Courts Don't, Why Should We Care About Measuring Expectations of Privacy?*

Judicial lack of experience and the changing nature of societal expectations highlight a potential issue with the reasonable expectation of privacy test: how can judges evaluate what expectations society is willing to recognize as reasonable when they do not fully understand the technology in the first place? Especially regarding social media, which is increasingly common but the Supreme Court has yet to address, the question of whether the federal judiciary is equipped to evaluate the expectation of privacy is apparent.[82] The purported target of the *Katz* reasonable expectation of privacy test is those subjective expectations society is willing to recognize as reasonable, but judges differ significantly from the general public in many factors, including age, personal experiences, and education. One potential solution is to turn to empirical studies of expectations of privacy to help inform courts. The problem, though, is that courts generally disregard subjective expectations of privacy, frequently failing to discuss that prong of the reasonable expectation of test altogether.[83] But empirical research on expectations of privacy can still inform courts for three reasons: first, judges may resort to their own subjective expectations of privacy which are prone to biases and may not be indicative of societal expectations; second, judges evaluate expectations of privacy from an after-the-fact, third party perspective, so objective evidence of expectations may be helpful to counteract this perspective; and third, empirical research can delineate those factors that are important in evaluating privacy.[84]

First, a significant difficulty with the reasonable expectation of privacy test is that judges are not often explicit in how they determine which expectations are

82. In February of 2021, 72% of American adults reported being a member of social media; that number is slightly less but still not insignificant at 59% when considering the population globally. *Social Media Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/social-media/ [https://perma.cc/Z9Y9-THCY]; Dave Chaffey, *Global Social Media Statistics Research Summary 2022*, SMART INSIGHTS https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research [https://perma.cc/DA5V-EHDV] (last visited Mar. 27, 2024). And social media usage varies by age—84% of Americans age 18–29 and 81% of those age 30-49 reported using social media, while 73% of those age 50-64 and only 45% of those age 65 and above (a group that includes much of the federal judiciary) report using a social media platform. *Social Media Fact Sheet*, *supra*.

83. Kerr, *supra* note 22, at 114.

84. *Id.* at 134; *see also* Dorothy K. Kagehiro, Ralph B. Taylor, William S. Laufer & Alan T. Harland, *Hindsight Bias and Third-Party Consentors to Warrantless Police Searches*, 15 LAW & HUM. BEHAV. 305, 306, 312 (1991); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings" Recognized and Permitted by Society*, 42 DUKE L.J. 727, 742–43 (1993).

reasonable. Though—as discussed above—most courts do not consider subjective expectations of privacy to be important, some judges may turn to their *own* subjective expectations. This notion has not gone unnoticed by the Court, as it was explicitly recognized by Justice Alito in his concurring opinion in *United States v. Jones*.[85] A fairly robust cognitive bias called the false consensus effect demonstrates how this may happen: individuals tend to view their own judgments as common and appropriate in a particular instance.[86] Because judges are not immune from such cognitive biases,[87] it remains possible—even likely—that judges tend to assume society would view those expectations the judge holds as reasonable. Empirical research can provide an important guidepost for judges to evaluate their own expectations of privacy.

Second, judges naturally review searches from an after-the-fact, third-party perspective. The hindsight bias, which is the cognitive bias where people tend to claim they accurately predicted an event after it already happened is at play in evaluations relevant to the Fourth Amendment, such as determining the level of consent granted to a search.[88] Professors Chao and colleagues found evidence that lay people suffer from outcome bias when evaluating whether a search violated a reasonable expectation of privacy: participants told a search uncovered incriminating evidence were more than two times less likely to feel the search violated a reasonable expectation of privacy than if they were told the target of the search was innocent.[89] The third-party perspective could play a role in judicial evaluations of privacy expectations as well, because a judge could first conclude whether an action constituted a search or not, then reason that of course society would (or would not) recognize that expectation as reasonable because the judge views themselves as a reasonable person.

Lay individuals, at least, rate searches presented in the first person perspective as more intrusive than those presented in the third person perspective, which demonstrates a "distancing effect" in evaluating expectations of privacy.[90] Previous research has found individuals find searches to be more intrusive and more violating of an expectation of privacy when presented in a first-person perspective rather than a third-person perspective.[91] Individuals could rate searches

85. United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring) (citing Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring)) ("[J]udges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person . . . .").

86. Lee Ross, David Greene & Pamela House, *The "False Consensus Effect": An Egocentric Bias in Social Perception and Attribution Processes*, 13 J. EXPERIMENTAL PSYCH. 279, 280 (1977).

87. Chris Guthrie, Jeffrey J. Rachlinski & Andrew J. Wistrich, *Judging by Heuristic: Cognitive Illusions in Judicial Decision Making*, 86 JUDICATURE 44, 45, 50 (2002).

88. Neal J. Roese & Kathleen D. Vohs, *Hindsight Bias*, 7 PERSPS. ON PSYCH. SCI. 411, 411 (2012); Kagehiro et al., *supra* note 84, at 306–07; *see also* Jonathan D. Casper, Kennette Benedict & Jo L. Perry, *Juror Decision Making, Attitudes, and the Hindsight Bias*, 13 LAW & HUM. BEHAV. 291, 293 (1989); Chris Guthrie, Jeffrey J. Rachlinski & Andrew J. Wistrich, *The "Hidden Judiciary": An Empirical Examination of Executive Branch Justice*, 58 DUKE L.J. 1477, 1512–15 (2009).

89. Bernard Chao, Catherine Durso, Ian Farrell & Christopher Robertson, *Why Courts Fail to Protect Privacy: Race, Age, Bias, and Technology*, 106 CALIF. L. REV. 263, 298 (2018).

90. Slobogin & Schumacher, *supra* note 84, at 760.

91. *Id.* at 759; Chao et al., *supra* note 89, at 298–99.

presenting the first person as more intrusive because they feel more personal and thus could relate more to the feeling of being intruded upon.[92] Courts, though, always evaluate searches from a neutral, third-party perspective, so they may *underestimate* privacy expectations compared to those who face actual invasions.

The third route of usefulness for such empirical research is to inform the various dimensions and factors of privacy. As discussed below, empirical research has been used to identify important dimensions of privacy, including perceived guilt and dangerousness, implied consent, personal nature of the item, and intrusiveness.[93] Research has explored those factors *judges* may be implicitly using in their evaluations, but it is also helpful to consider how lay people construct their views of privacy.[94]

Thus, the point of empirical research on privacy expectations is not to merely measure subjective expectations of privacy but instead to provide judges some statistical information on what expectations society is willing to recognize as reasonable. Research can also give courts insight into what factors or dimensions people use when crafting an expectation of privacy, which can help courts determine societal expectations when evaluating searches. It is important to keep that in mind when considering the results of empirical research such as the studies that follow.

### *B. The Current State of Empirical Research on Expectations of Privacy Provides an Important Starting Point for Judges*

Empirical evidence of privacy expectations—while not widespread—is certainly not new. Professors Slobogin and Schumacher compared undergraduate students', law students', and community members' expectations of privacy to determinations made by the Supreme Court and found lay people's expectations of privacy generally match Fourth Amendment protections the Court provides.[95] For example, participants rated searches such as a forced surgery of a suspect's shoulder to retrieve a bullet and a search of a suspect's bedroom as highly intrusive; these are both searches the Supreme Court held unreasonable under the Fourth Amendment.[96] Participants perceived searches like looking in foliage in a public park and shining a flashlight down a dark alley next to someone's home as not intrusive, and these are both searches the Supreme Court held did not violate the Fourth Amendment.[97] But, there were some key differences between Supreme Court rulings and participants' ratings of intrusiveness.[98] Participants viewed use of undercover agents and a dog sniff of a vehicle as fairly

92. *Id.* at 299.

93. Slobogin & Schumacher, *supra* note 84, at 765; Jeremy A. Blumenthal, Meera Adya & Jacqueline Mogle, *The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy,"* 11 J. CONST. L. 331, 345 (2009).

94. Tokson, *supra* note 30, at 4, 28–29.

95. Slobogin & Schumacher, *supra* note 84, at 737.

96. *Id.* at 739.

97. *Id.* at 738.

98. *Id.* at 740.

intrusive, while the Supreme Court has held that these searches do not violate reasonable expectations of privacy.[99]

Slobogin and Schumacher identified three aspects of searches that their lay participants used to evaluate intrusiveness: (1) guilt of person searched, (2) dangerousness of suspected activity, and (3) implied consent to the search.[100] Blumenthal, Adya, and Mogle extended these findings and determined lay individual use the personal nature of the search, the perceived level of intrusiveness of the search, permission granted, and the dangerousness of the suspected activity, when evaluating privacy expectations.[101] Similarly, people may identify various "zones" of privacy, such as personal space (bodily and territorial privacy), informational privacy, and communications privacy.[102]

Professors Chao, Farrell, Durso, and Robertson similarly extended the above research and found the vast majority of participants viewed searches of electronic information such as Google maps location data, email, documents saved on the cloud, and GPS location data, as highly intrusive and violating a reasonable expectation of privacy.[103] The ratings of these electronic searches were viewed similarly to physical searches such as a search of a bedroom or a physical pat-down search.[104]

Lay people tend to view the information stored on electronic communication devices as very private.[105] Adults in the United States rate searches of content on electronic communication devices, such as the content of emails or text messages, as nearly as intrusive as strip searches and body cavity searches, the type of searches the Supreme Court has found to have full Fourth Amendment protection.[106] In addition, searches of electronic content is rated as more intrusive, more revealing of private information, and more embarrassing than searches of content stored in physical property, such as papers held in a

99. *Id.*

100. *Id.* at 765–69.

101. Blumenthal et al., *supra* note 93, at 348.

102. Henry F. Fradella, Weston J. Morrow, Ryan G. Fischer & Connie Ireland, *Quantifying* Katz*: Empirically Measuring "Reasonable Expectations of Privacy" in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289, 333 (2010). In this study, participants indicated their level of agreement with various Supreme Court rulings. *Id.* at 347–48. The lay participants indicated greater expectations of privacy in informational and communications privacy than what Court rulings protect. *Id.* at 366–67. For example, 85.5% of participants indicated they disagreed with the Court holding in *United States v. Knotts* that the Fourth Amendment did not prevent state officials from using a tracking beeper to track the movements of a vehicle. *Id.* Fradella and colleagues included searches of students in a school setting. Participants largely disagreed with a prior Supreme Court ruling holding a school's drug testing policy did not violate students' expectations of privacy, indicating participants believed such policies did violate privacy rights. *Id.* at 363. While lay individuals report similar level of expectations of privacy that the Supreme Court protects in some court decisions, there are certain domains or types of privacy that individuals report higher expectations of privacy than the Court finds. *Id.* at 352–59. Though age was not related to agreement with Court opinions, this could be because their sample was limited to mostly young adults.

103. Chao et al., *supra* note 89, at 300–01.

104. *Id.*

105. Matthew B. Kugler, Comment, *The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study*, 81 U. CHI. L. REV. 1165, 1194–95 (2014).

106. *Id.* at 1197–98.

briefcase.[107] This suggests lay people have privacy expectations in electronic content comparable to their privacy expectations in their personal body.[108]

Instead of evaluating expectations of privacy, some scholars have focused on what procedures lay people believe should be required to make a search "reasonable." Professor McAllister found lay individuals support a warrant requirement for a GPS tracking device, regardless of the suspected guilt of the individual being tracked.[109] In a different study, the majority of participants reported they thought probable cause should be required for law enforcement to access location tracking data, social media profiles, cell phones, and email addresses.[110] This may differ with age—older adults reported more expectations of privacy in social media posts shared with friends, online purchase history, and online television shows watched than did younger adults, while younger adults reported more privacy expectations in GPS location data than did older adults.[111] Professors Smith, Madden, and Barton found that, consistent with court holdings in *Jones* and *Riley*, participants disapproved of police tracking suspects with a GPS tracking device or searching a cell phone.[112] And, perhaps prophetic to the Court's decision in *Carpenter*, participants were also disapproving of law enforcement tracking suspects via cell phone tower information.[113]

Overall, the available research indicates discrepancies between judges' and lay adults' expectations of privacy. A related—but different—concern is whether expectations of privacy are malleable and change in response to societal shifts.

107. *Id.*

108. *Id.* at 1195.

109. Marc McAllister, *GPS and Cell Phone Tracking: A Constitutional and Empirical Analysis*, 82 U. CIN. L. REV. 207, 238–39 (2014). This study focused on the probable cause requirement of the Fourth Amendment in asking participants whether they believed police should get a warrant before attaching a GPS tracking device to a vehicle. *Id.* at 242–43. Instead of varying the type of information searched, McCallister asked participants whether their view of the warrant requirement was different based on the identity of the person being tracked: an individual suspected of being a drug dealer, an individual suspected of being a serial killer, an individual suspected of being a terrorist, a convicted felon currently suspected of an unspecified crime, a person who had never been convicted of a crime but was currently suspected of an unspecified crime, a convicted felon who was not currently suspected of any crime, and a person who had never been convicted of a crime and was not currently suspected of committing any crime (a "true" innocent). *Id.* at 243. Participants supported the warrant requirement for a GPS tracking device, regardless of the suspected guilt of the individual being tracked. *Id.* at 246.

110. Christine S. Scott-Hayward, Henry F. Fradella & Ryan G. Fischer, *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 AM. J. CRIM. L. 19, 52–56 (2015). Professor Scott-Hayward and colleagues addressed lay individuals' opinions on the reasonableness of a search by asking American adults for their opinion on the burden of proof law enforcement should have to have before conducting certain types of searches of online information: no proof, gut instinct, reasonable suspicion, probable cause, or never. *Id.* at 53, 55.

111. *Id.* at 57 n.260.

112. Alisa Smith, Sean Madden & Robert P. Barton, *An Empirical Examination of Society Expectations of Privacy in the Digital Age of GPS, Cell Phone Towers, & Drones*, 26 ALB. L.J. SCI. & TECH. 111, 141 (2016).

113. *Id.*

### *C. Are We Losing Any Reasonable Expectation of Privacy?*

Many scholars have expressed dissatisfaction with the reasonable expectations of privacy test, even pointing out that under the test, "privacy is a legal fiction."[114] A major criticism of the reasonable expectations of privacy test is that it is inherently circular: legal pronunciations of what reasonable expectations of privacy people hold can impact actual expectations of privacy held by individuals, which in turn impact legal pronunciations of what reasonable expectations of privacy people hold.[115] Legal scholars[116] have expressed concern with this test because, as it is inherently circular, it is a subjective test and does not provide guidance on how to apply it to lower courts. But circularity might not be as big of a problem as some scholars suggest in light of the fact legal decisions determining Fourth Amendment rights are not well-known and, even if they are, do little to change public perceptions.[117]

As Justice Blackmun wrote in 1976, the government can easily eliminate any expectations of privacy by announcing a widespread "Big Brother" type of surveillance program.[118] In an early description of the reasonable expectations of privacy test, the Supreme Court opined that analyzing expectations would be inadequate to protect privacy rights "where an individual's subjective expectations had been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms," such as where "the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry."[119] As far-fetched as constant surveillance of private activities may seem, something not too far off was revealed in June 2013. A National Security Agency sub-contractor copied thousands of classified documents regarding a national global surveillance scheme.[120] One such program, PRISM, allowed the government to access citizens' Google and Yahoo accounts,[121] while

114. Adam R. Pearlon & Erick S. Lee, *National Security, Narcissism, Voyeurism, and* Kyllo: *How Intelligence Programs and Social Norms Are Affecting the Fourth Amendment*, 2 TEX. A&M L. REV. 719, 723 (2015).

115. Kugler & Strahilevitz, *supra* note 17, at 1749–50.

116. *Id.*

117. *Id.* at 1801. Professors Kugler and Strahilevitz surveyed American citizens just prior to, immediately after, one year after, and two years after the Supreme Court handed down a decision evaluating reasonable expectations of privacy in cell phones. *Id.* at 1776. Perceptions of intrusiveness in searches of cell phones increased directly after the *Riley v. California* decision, but were comparable to pre-*Riley* ratings one year and two years later. *Id.* at 1780–81. There was no difference in perceptions of intrusiveness pre- and post-*Riley* for different types of searches, such as a search of property. *Id.* at 1783. Those participants who had heard of the *Riley* decision had stronger expectations of privacy in their cell phones than did participants who had not heard of the *Riley* decision, which provides support for the claim that Fourth Amendment decisions impact expectations of privacy, but this difference had disappeared one year after the decision. *Id.* at 1788–90. Thus, any impact on expectations of privacy is short lived and likely does not do much to change the course of societal privacy expectations.

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

119. *Id.*

120. Glenn Greenwald, Ewen MacAskill & Laura Pointras, *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN (June 11, 2013, 9:00 AM), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance [https://perma.cc/XCA9-7T7W].

121. Timothy B. Lee, *Here's Everything We Know About PRISM to Date*, WASH. POST (June 12, 2013, 3:43 PM), https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/ [https://perma.cc/G2EV-ZRF4].

other programs included mass data collection of cell phone records such as location tracking data and phone numbers dialed. These leaks were widely reported in both America and abroad and have been cited as an example of a major event that could erode expectations of privacy.[122]

Data on online behavior does show a slight effect of the NSA surveillance programs. Search terms highly likely to get people in trouble with the United States government were searched less frequently after the mass surveillance programs were released, while those terms rated as unlikely to get people in trouble were searched more frequently.[123] A similar chilling effect was observed pre- and post-June 2013 in Wikipedia article visits.[124] Immediately after the NSA surveillance programs were revealed, the sensitive terms exhibited an almost 30% drop in number of visits.[125] And, while there was a slight increase both in searches related to the NSA and surveillance and use of privacy-protecting software such as Tor immediately after the program was revealed, the increases returned to baseline levels after a short period of time.[126]

Though the empirical data is inconclusive, it does appear government programs may change the actions individuals take to protect their privacy, at least in the short term. The same programs may also affect the expectations of privacy society is willing to recognize as reasonable: if most people voluntarily share information online, and most people know the government keeps track of the information they do share, can any expectation of privacy in online information be reasonable? If expectations of privacy change over time, this is evidence that big societal shifts—in usage of electronic communications and in government surveillance programs—do erode expectations of privacy.

### *D. Adolescents Differ from Adults in Experiences With and Views of Social Media*

One way to determine whether expectations of privacy are changing is to compare age groups' expectations, but we first must understand how adolescents are generally different from adults. Some developmental research has addressed the question of how adolescents' use of electronic communications differs from that of adults.'[127] Adolescents have a whole world open to them that was not available as recently as thirty years ago—the Internet. "Digital natives" are individuals who have grown up using digital communications and networked

122. Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. L. REV. 139, 182 (2016).

123. *Id.* at 198.

124. Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117, 147 (2016).

125. *Id.* An interrupted time series design tracking monthly visits both prior to and after the reveal demonstrated this drop was due to the leaks: prior to the leaks, the number of monthly views for the sensitive information was trending upwards, while after the leaks the number of monthly views sharply dropped and continued decreasing over time. *Id.* The same trend was not observed for articles relating to domestic security issues, infrastructure issues, or Wikipedia's most popular searches.

126. Sören Preibusch, *Privacy Behaviors After Snowden*, 58 COMMC'NS ACM 48, 51–54 (2015).

127. *See generally* studies discussed *infra* notes 133–39.

technologies;[128] these individuals are more familiar with using computers, sending information online, and living in a virtual "world." One issue with the influx of social networking sites is how these impact adolescents' expectations of privacy and willingness to share information with others.

Adolescents' online behaviors are often compared to adults' behaviors; adults are assumed to be more logical, and adolescents are perceived to use social media more often.[129] While some research has demonstrated older adults are less knowledgeable about online security than younger users[130] and adolescents feel more responsible and are more confident in their ability to manage their data online,[131] other research shows adolescents are more willing to take risks with their information, such as by sharing their passwords with others.[132]

Some evidence suggests adolescents are savvy social media users aware of privacy risks. As social media increases in popularity, adolescents become more cognizant of what types of information are appropriate to be posted online.[133] Contrary to concerns about eroding expectations of privacy, adolescents may be *less* willing than adults to share information online, possibly because adolescents are more accustomed to social media sites and more aware of the negative ramifications of posting information online.[134] This is evidence that adolescents do evaluate the risks and benefits of sharing information online and that this relates to disclosing information online.[135] Adolescents who perceive risks associated with publicly posting identifying information on a social media profile are less likely to provide such info.[136] Similarly, adolescents who perceive benefits associated with sharing information, such as peer acceptance, are more likely to publicly provide information.[137] Adolescents who report a greater need for popularity and less awareness of the consequences of disclosure are more likely to

128. *See generally* JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES (2008).

129. Monica Whitty, James Doodson, Sadie Creese & Duncan Hodges, *Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords*, 18 CYBERPSYCHOLOGY, BEHAV. & SOC. NETWORKING 3, 6 (2015).

130. Galen A. Grimes, Michelle G. Hough, Elizabeth Mazur & Margaret L. Signorella, *Older Adults' Knowledge of Internet Hazards*, 36 EDUC. GERONTOLOGY 173, 188 (2010).

131. Caroline Lancelot Miltgen & Dominique Peyrat-Guillard, *Cultural and Generational Influences on Privacy Concerns: A Qualitative Study in Seven European Countries*, 23 EUR. J. INFO. SYS. 103 (2014).

132. Whitty et al., *supra* note 129, at 6.

133. Justin W. Patchin & Sameer Hinduja, *Changes in Adolescent Online Social Networking Behaviors from 2006 to 2009*, 26 COMPUTS. HUM. BEHAV. 1818, 1820 (2010). This study of the once-popular Social Networking Site MySpace found that 85% of youth in 2009 chose to at least partially restrict access to their profile (this number was up from 39.1% just three years prior). *Id.* at 1819. Adolescents' MySpace profiles in 2009 were less likely to include pictures of the profile holder or friends in swimsuits or underwear and less likely to provide references to tobacco or alcohol use. *Id.*

134. Deborah M. Moscardelli & Richard Divine, *Adolescents' Concern for Privacy When Using the Internet: An Empirical Analysis of Predictors and Relationships with Privacy-Protecting Behaviors*, 35 FAM. & CONSUMER SCIS. RSCH. J. 232, 246 (2007).

135. Seounmi Youn, *Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk-Benefit Appraisal Approach*, 49 J. BROAD. & ELEC. MEDIA 86, 86 (2005).

136. *Id.* at 100–01.

137. *Id.*

disclose personally identifying information.[138] Adolescents who were less willing to provide information publicly engaged in coping behaviors such as providing inaccurate or incomplete information.[139] But adolescents are not adults, and one way the age groups differ is in brain development and decision making.

### *E. An Alternative Explanation to Adolescents' Differing Expectations: Dual Systems Model of Adolescent Risk-taking*

One explanation for the difference in adolescents' use of media is that they are, quite simply, worse at making decisions than are adults. The Dual Systems Model of Adolescent Risk-Taking differentiates between two systems in the brain: the incentive processing system and the cognitive control system.[140] The incentive processing system involves the valuation and prediction of rewards and punishments.[141] This theory is based on developmental neuroscience research that identified two separate systems at work in adolescent risk-taking.[142]

Steinberg connected adolescent risk-taking behaviors to an increase in dopamine activity in the socioemotional system beginning around puberty.[143] This leads to an increased attentiveness to rewards, increased sensation seeking, and heightened emotional arousal.[144] When this system is at its peak, adolescents may focus more on short term rewards and ignore long term consequences.[145] In contrast, the cognitive control system involves impulse control, foresight, and future planning.[146] This system matures gradually throughout adolescence, unlike the abrupt increase and then drop off seen with the incentive processing system.[147] Around age sixteen, the incentive processing system is at its most active point, while the cognitive control system is not yet fully matured.[148] So

138. Emily Christofides, Amy Muise & Serge Desmarais, *Hey Mom, What's on Your Facebook? Comparing Facebook Disclosure and Privacy in Adolescents and Adults*, 3 SOC. PSYCH. & PERSONALITY SCI. 1, 6 (2012).

139. Youn, *supra* note 135, at 99.

140. Laurence Steinberg, *A Dual Systems Model of Adolescent Risk-Taking*, 52 DEV. PSYCHOBIOLOGY 216, 216 (2010).

141. *Id.*

142. B.J. Casey, Sarah Getz & Adriana Galvan, *The Adolescent Brain*, 28 DEV. REV. 62, 62 (2008); Laurence Steinberg, *A Social Neuroscience Perspective on Adolescent Risk-Taking*, 28 DEV. REV. 78, 83 (2008). The "socioemotional" system (or incentive processing system) is located in the limbic and paralimbic brain areas and involves the amygdala, ventral striatum, orbitofrontal cortex, medial prefrontal cortex, and superior temporal sulcus. *Id.* at 83–93. The "cognitive control" system consists of the prefrontal and parietal cortices and related parts of anterior cingulate cortex. *Id.* at 93–99.

143. Steinberg, *supra* note 140, at 217.

144. *Id.*

145. *See id.* at 216–17.

146. *Id.* at 216.

147. *Id.* at 217.

148. *See id.* Steinberg identifies a temporal gap between the incentive processing system, which develops early in adolescence, and the cognitive control system, which fully matures much later, that makes adolescence a particularly vulnerable time for risk-taking behaviors. *Id.* at 216. This period of vulnerability coincides with an increase of risk-taking behaviors such as delinquency and reckless driving; these behaviors then decrease in early adulthood. Subsequent research has demonstrated a link between reward seeking, cognitive control, and sexual behaviors in adolescence, and an association with the gap between sensation seeking, impulsivity, and juvenile deviant behaviors.

adolescents may focus on the immediately rewarding nature of social media (*e.g.*, the dopamine hint from getting "likes" or adds from other users) and not the potential long term consequences of sharing sensitive information online. The Court is familiar with such research, as it has referenced these and similar findings in other areas of the law, such as the constitutionality of the death penalty and mandatory life without parole statutory schemes for juveniles.[149]

### *F. Generational Divide in Social Media, Developmental Decision Making, or Both?*

Thus, adolescents' expectations of privacy may differ from those of adults for two potential reasons. The Generational Hypothesis reasons that current adolescents' expectations of privacy have developed in the "Digital Age," where digital communications and sharing of information are almost second nature.[150] Current adolescents are growing up aware of governmental privacy intrusions; for example, in 2013, the controversial National Security Agency policy of collecting mass amounts of online and cellular data was revealed.[151] Private policies and practices may also impact development of expectations of privacy. For instance, commentators have suggested that the popular Elf on a Shelf fairy tale may lessen expectations of privacy.[152] Today's youth are surrounded by technology, such as Amazon's Alexa or iPhone's Siri, that is constantly watching, listening, and purporting to make lives easier.[153] Schools have routine surveillance and security screening, both at school and for electronic devices.[154]

On the other hand, according to the Developmental Hypothesis, privacy expectations may differ by age because adolescents' decision-making capacities are still developing. Adolescents differ from adults in incentive processing and sensation seeking, and this may impact how they evaluate expectations of privacy, especially where their cognitive control system is not yet fully developed, supporting the Developmental Hypothesis.[155] Thus, adolescents differ from adults both in development and in experiences, and both of these factors may lead to differences in expectations of privacy.

149. *See* Roper v. Simmons, 543 U.S. 551, 569 (2005); Miller v. Alabama, 567 U.S. 460, 471 (2012).

150. *See supra* notes 132–35 and accompanying text.

151. Glenn Greenwald, Ewnen MacAskill & Laura Poitras, *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, GUARDIAN (June 11, 2013), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance [https://perma.cc/XCA9-7T7W].

152. Pinto & Nemorin, *supra* note 7. Elf on a Shelf is a holiday practice where parents place a small toy elf in their home and tell their children the elf is there to observe their actions and report back each night to Santa Claus in the North Pole. *Id.* Pinto and Nemorin argue that this accustoms children to surveillance from third parties, which will translate to accepting surveillance and privacy intrusions from the government.

153. *See, e.g.*, Jamey Tucker, *Voice Assistants Like Alexa, Siri Are ALWAYS Listening*, LOCAL 3 NEWS (Dec. 1, 2021), https://www.local3news.com/voice-assistants-like-alexa-siri-are-always-listening/article_7183d0a9-194f-5899-833f-8739ef3e4c67.html [https://perma.cc/H35V-GN2Q].

154. *Fast Facts: School Safety and Security Measures*, NAT'L CTR. FOR EDUC. STATS., https://nces.ed.gov/fastfacts/display.asp?id=334 [https://perma.cc/R75T-TNRV] (last visited Feb. 20, 2024); Ceres, *supra* note 1.

155. *See supra* notes 141–49 and accompanying text.

Such differences may have important implications for the development of Fourth Amendment jurisprudence. The reasonable expectation of privacy standard theoretically allows for Fourth Amendment protections to change over time as those expectations that society is willing to recognize as reasonable evolve. If adolescents' expectations of privacy differ from those of adults due to generational differences, eventually the types of searches that are currently protected under the Fourth Amendment will change. But, if adolescents' expectations differ more so because of developmental differences in decision making, as adolescents develop their expectations will look more like those of adults, and the current Fourth Amendment protections will arguably not need to evolve. The following studies began to answer the question of whether expectations of privacy are changing due to generational differences in the use of electronic communications.

## IV. ARE EXPECTATIONS OF PRIVACY CHANGING? TWO STUDIES TO EXAMINE WHETHER, AND WHY, ADOLESCENTS' EXPECTATIONS DIFFER FROM ADULTS'

The concern over the adequacy of the reasonable expectation of privacy test in light of the changing ways we share information is highlighted by the struggle of applying the test to new and emerging technologies. A question currently unanswered by empirical data is whether expectations are changing due to use of electronic communications. There are many ways to study this—ideally a longitudinal study examining the same population over years to measure how expectations of privacy change and correlating that with electronic communication use. Unfortunately, due to the changing nature of technology and the length of time required to track expectations, such an approach would be nearly impossible to complete in a timely manner. Another approach is a cross-sectional design examining different subsets of the population at one point in time, though this is also certainly not without its faults. Primarily, at least with respect to age or generational differences, the cross-sectional design leaves open the question of whether any differences between groups are permanent or whether current adolescents evolve to look more like current adults (for example). But with the help of measuring proxy variables, we can at least begin the examination of the question of whether increased use of electronic communications changes our expectations of privacy.

### *A. Study 1: Adolescents' Expectations of Privacy and Fourth Amendment Case Law*[156]

The first step in asking whether expectations of privacy are changing is to describe adolescents' expectations of privacy and compare them to a group for which we already have data: judges in judicial opinions. Study 1 extends the

156. *See* Appendix A for a full list of all variables included in this study.

research of previous scholars[157] by comparing adolescents' expectations of privacy with court rulings on reasonable expectations of privacy.

Ninety-five adolescents aged 12 through 17 completed a survey regarding expectations of privacy. The mean age of participants was 14.8 with a median of 16. After obtaining parental consent via email, adolescents completed an online survey consisting of a series of short vignettes describing searches from already-decided appellate and Supreme Court cases. To address the question of whether perspective of the search matters,[158] participants evaluated each search from two different perspectives: a first-person perspective (*e.g.*, the school principal searches *your* bag) and a third-person perspective (*e.g.*, the school principal searches *a student's* bag). The twenty-four search descriptions were presented in random order.

Adolescents' Ratings of Searches[159]

Adolescents rated each search on three domains of privacy: intrusiveness, personal nature, and permission granted for the search. Adolescents rated the intrusiveness of a bodily search—a pat down in a school setting—as the most intrusive,[160] most personal in nature,[161] and conducted with a low level of permission.[162] Additionally, adolescents consistently rated searches of information, including electronic tracking devices,[163] cell phones,[164] and social media sites,[165] near or above the midpoint on both intrusiveness and personal nature. In fact, adolescents rated a search of a cell phone by police officers and school officials as personal in nature as a pat-down search by school officials. Participants also rated a search of cell phones nearly as intrusive as a physical pat-down search, indicating adolescents could view cell phones similarly to the privacy they expect in their physical body.

Table 1 compares adolescent participants' ratings of intrusiveness of the searches with Slobogin and Schumacher's adult participants' ratings and court

157. Slobogin & Schumacher, *supra* note 84, at 728; Blumenthal et al., *supra* note 93, at 333; Fradella et al., *supra* note 102, at 293–94.

158. This manipulation replicated Slobogin and Schumacher's first vs. third person variable, to determine whether adolescents, like the lay adults in Slobogin and Schumacher's study, viewed searches presented in the first person as more intrusive than those presented in the third person. *See* Slobogin & Schumacher, *supra* note 84, at 759.

159. Because courts view searches from a third-party perspective, only the ratings of searches presented in that perspective are included in the following results.

160. Average intrusiveness rating of a pat-down search in a school setting was 4.33. *See infra* Table 1.

161. Average personal nature rating of a pat-down search in a school setting was 4.23. *See infra* Table 2.

162. Average permission granted rating of a pat-down search in a school setting was 1.53. *See infra* Table 2.

163. Average intrusiveness rating of an electronic tracking device was 3.49 and average personal nature rating was 3.38. *See infra* Table 1; Table 2.

164. Average intrusiveness rating of a cell phone search by police officers was 3.94 and average personal nature rating was 4.23. *See infra* Table 1; Table 2. Average intrusiveness rating of a cell phone search by school officials was 4.00 and the personal nature rating of that search was 4.22. *See infra* Table 1; Table 2.

165. Average intrusiveness rating of a social networking site search was 3.01 and average personal nature rating was 2.92. *See infra* Table 1; Table 2.

rulings.[166] These comparisons must be interpreted with caution, as there is nearly twenty-five years between the two studies and many differences in the samples beyond age. One major difference that is apparent is how participants rated a pat-down search by a school official. Participants in the current study rated a pat-down search as the most intrusive search presented to them, while adult participants in Slobogin and Schumacher's study rated the search thirtieth out of fifty searches presented.[167] Conversely, adult participants in Slobogin and Shumacher's study considered a stop and talk as relatively more intrusive (ranked as the fifteenth most intrusive out of the fifty searches presented)[168] than did adolescent participants in the current study (ranked as the twentieth most intrusive out of the twenty-three searches presented).[169] Perhaps adolescents are accustomed to being routinely questioned by adults and thus do not view a brief conversation with police as being all that invasive.

On the other hand, adults in Slobogin and Schumacher's study viewed some searches as similarly intrusive to adolescents in the current study. Both a flashlight search through a car window and airport security were ranked as relatively unintrusive in both studies, while reading a private diary ranked as relatively very intrusive.[170]

Like in Slobogin and Schumacher's study, current adolescent participants' ratings of intrusiveness can be compared to how courts ruled on the same search. Notably, the three searches adolescent participants in the current study rated as most intrusive—pat-down search, school official search of a cell phone, and police officer search of a cell phone—were all determined to be an unreasonable search by the courts that evaluated them.[171] The fourth-ranked most intrusive search (diary) would also be an unreasonable search, but an analogous Supreme Court case determined a search of private papers was not a Fourth Amendment violation because the search was conducted by a private actor.[172]

On the other end of the intrusiveness spectrum, the seven searches ranked as least intrusive were all ruled by courts to be not unreasonable searches in violation of the Fourth Amendment. But, the current participants did not always agree with courts. While courts have ruled both a school official's search of a student's backpack with reasonable suspicion[173] and a school official's search of pictures on a student's cell phone[174] do not violate the Fourth Amendment, current participants saw these searches as fairly intrusive (ranked at fifth and sixth

166. Slobogin & Schumacher, *supra* note 84, at 738–39 tbl. 1.

167. *Id.*

168. *Id.*

169. *See infra* Table 1.

170. *Id.*; Slobogin & Schumacher, *supra* note 84, at 738–39 tbl.1.

171. Safford Unified Sch. Dist. #1 v. Redding, 557 U.S. 364, 378–79 (2009); Klump v. Nazareth Area Sch. Dist., 425 F. Supp. 2d 622, 641 (2006); Riley v. California, 573 U.S. 373, 402 (2014).

172. Burdeau v. McDowell, 256 U.S. 465, 475 (1921). While the facts of the case in *Burdeau* largely involved business papers, the defendant's private papers were included also. *Id.* at 473–74.

173. New Jersey v. T. L.O., 469 U.S. 325, 346 (1985).

174. J.W. v. Desoto Cnty. Sch. Dist., No. 2:09-cv-00155-MPM-DAS, 2010 WL 4394059, at *12 (N.D. Miss. Nov. 1, 2010).

most intrusive, respectively). Thus, similar to Slobogin and Schumacher's comparison of adult lay individuals to court rulings, while there seems to be agreement between adolescents and courts on the extreme ends of the intrusiveness spectrum, in the middle there is more disagreement.[175] It is in these "gray area" cases that courts' rulings differ the most from adolescents' opinions.

TABLE 1: PERCEPTIONS OF THIRD-PERSON SEARCHES RANKED BY INTRUSIVENESS: COMPARISON TO SLOBOGIN & SCHUMACHER AND COURT RULINGS

| Search | Intrusiveness | Current Rank | Rank in S&S | Court Ruling |
|---|---|---|---|---|
| Pat down (school) | 4.33 | 1 | 30/50 | Unreasonable |
| Cell phone (school) | 4.00 | 2 | -- | Unreasonable |
| Cell phone (police) | 3.94 | 3 | -- | Unreasonable |
| Diary | 3.90 | 4 | 3/50 | Unreasonable |
| Backpack (school) | 3.87 | 5 | 10/50 | Reasonable[176] |
| Cell phone pictures | 3.74 | 6 | -- | Unreasonable |
| Instant Messages (school) | 3.60 | 7 | -- | Unreasonable |
| Bus passenger's bag | 3.58 | 8 | 7/50 | Unreasonable |
| Bedroom with parental consent | 3.54 | 9 | 4/50[177] | Reasonable |
| Blood draw | 3.52 | 10 | 5/50 | Unreasonable |
| Electronic tracking device on car | 3.49 | 11 | 33/50 | Unreasonable |
| Plain view | 3.41 | 12 | 41/50 | Reasonable |
| Fingerprinting student (police) | 3.26 | 13 | -- | Unreasonable |
| Dog sniff (police) | 3.20 | 14 | 28/50 | Reasonable |
| Dog sniff (school) | 3.18 | 15 | -- | Reasonable |
| Random drug test (extra-curricular) | 3.09 | 16 | -- | Reasonable |

175. Slobogin & Schumacher, *supra* note 84, at 739–40.

176. The Supreme Court determined a school official's examination of the contents of a student's backpack is a search, but due to a student's lessened expectation of privacy in their property at school, a standard lesser than probable cause is required to satisfy the Fourth Amendment. *T.L.O.*, 469 U.S. at 330–33.

177. Slobogin and Schumacher's search scenarios did not include parental consent, which may explain the difference with our results.

| | | | | |
|---|---|---|---|---|
| Social Networking Site (school) | 3.01 | 17 | -- | Reasonable |
| Property around a home | 2.98 | 18 | 30/50 | Reasonable |
| Random drug test (sports) | 2.84 | 19 | -- | Reasonable |
| Stop and Talk | 2.70 | 20 | 15/50 | Reasonable |
| Flashlight through car window | 2.51 | 21 | 47/50 | Reasonable |
| Garbage | 2.18 | 22 | 38/50 | Reasonable |
| Airport Security | 2.17 | 23 | 49/50 | Reasonable |

TABLE 2: PERSONAL NATURE OF ITEM SEARCHED AND PERMISSION GRANTED RATINGS FOR THIRD-PARTY SEARCH VIGNETTES
(0 = NOT AT ALL; 5 = EXTREMELY)

| **Search** | **Personal Nature** | **Permission Granted** |
|---|---|---|
| *Physical Searches* | | |
| Pat-down (school) | 4.23 | 1.53 |
| Backpack (school) | 4.00 | 1.36 |
| Bus passenger's bag | 3.52 | 1.65 |
| Bedroom with parental consent | 3.75 | 2.16 |
| Blood draw | 3.54 | 1.93 |
| Plain view | 3.38 | 1.40 |
| Fingerprint student (police) | 3.31 | 1.39 |
| Drug sniff (police) | 3.23 | 1.68 |
| Drug sniff (school) | 3.09 | 1.58 |
| Random drug test (extra-curricular) | 3.20 | 2.10 |
| Property around a home | 2.93 | 1.52 |
| Random drug test (sports) | 2.96 | 1.94 |
| Stop and talk | 2.46 | 1.82 |
| Flashlight through car window | 2.48 | 1.16 |
| Garbage | 2.11 | 1.18 |
| Airport security | 2.49 | 2.39 |
| *Information Searches* | | |
| Cell phone (school) | 4.22 | 1.48 |
| Cell phone (police) | 4.23 | 1.46 |
| Diary | 3.93 | 1.40 |
| Cell phone pictures | 3.88 | 1.55 |
| Instant messages (school) | 3.72 | 1.52 |
| Electronic tracking device on car | 3.38 | 1.63 |
| Social Networking Site (school) | 2.92 | 1.49 |

Adolescents also rated each search on privacy domains. Some average ratings are obvious based on the description of the search; for example, the search rated highest in bodily privacy was a pat-down search.[178] But adolescents also rated a cell phone search by a school official as violating bodily privacy and privacy of a person's space[179]—ratings comparable to the average ratings for a school official search of a backpack[180] and a drug sniff at school.[181] Searches of a cell phone were rated the highest in violating privacy of information and privacy of communications.[182]

TABLE 3: PERCEPTIONS OF THIRD-PARTY SEARCH VIGNETTES BY PRIVACY DOMAIN (0 = NOT AT ALL PRIVATE; 5 = EXTREMELY PRIVATE)

| **Search** | **Body** | **Personal Space** | **Informational** | **Communications** |
|---|---|---|---|---|
| *Physical Searches* | | | | |
| Pat down (school) | 4.29 | 4.33 | 3.73 | 3.13 |
| Backpack (school) | 3.07 | 3.68 | 3.58 | 2.86 |
| Bus passenger's bag | 2.80 | 3.58 | 3.29 | 2.81 |
| Bedroom with parental consent | 3.01 | 3.78 | 3.46 | 2.89 |
| Blood draw | 3.45 | 3.23 | 3.17 | 2.70 |
| Plain view | 2.71 | 3.38 | 3.27 | 2.71 |
| Fingerprint student (police) | 3.17 | 3.07 | 2.90 | 2.35 |
| Drug sniff (police) | 3.16 | 3.12 | 2.88 | 2.56 |
| Drug sniff (school) | 3.00 | 3.14 | 2.65 | 2.45 |
| Random drug test (extra-curricular) | 2.86 | 2.85 | 2.53 | 2.23 |
| Property around a home | 2.09 | 3.12 | 2.59 | 2.31 |
| Random drug test (sports) | 2.57 | 2.45 | 2.38 | 2.10 |
| Stop and talk | 2.13 | 2.29 | 2.60 | 2.39 |
| Flashlight through car window | 2.21 | 2.50 | 2.28 | 2.03 |
| Garbage | 2.00 | 2.11 | 2.25 | 1.90 |
| Airport security | 2.04 | 2.05 | 1.89 | 1.78 |
| *Information Searches* | | | | |
| Cell phone (school) | 3.04 | 3.77 | 4.10 | 4.08 |

178. Average bodily privacy rating for a pat-down search was 4.29. *See infra* Table 3.

179. Average bodily privacy rating of a cell phone search by a school official was 3.04 and personal space rating was 3.77. *See infra* Table 3.

180. Average bodily privacy rating for school official search of a backpack was 3.07 and 3.68 for personal space privacy. *See infra* Table 3.

181. Average bodily privacy rating for a dog sniff at school was 3.00 and 3.14 for personal space privacy. *See infra* Table 3.

182. For a police officer search of a cell phone, the average rating was 4.00 for informational privacy and 4.10 for communications privacy. For a school official search of a cell phone, the average rating was 4.10 for informational privacy and 4.08 for communications privacy. *See infra* Table 3.

| | | | | |
|---|---|---|---|---|
| Cell phone (police) | 2.96 | 3.65 | 4.00 | 4.10 |
| Diary | 2.86 | 3.49 | 3.94 | 3.33 |
| Cell phone pictures | 2.81 | 3.56 | 3.72 | 3.65 |
| Instant messages (school) | 2.74 | 3.51 | 3.65 | 3.75 |
| Electronic tracking device on car | 2.81 | 3.32 | 3.41 | 3.04 |
| Social Networking Site (school) | 2.61 | 2.77 | 2.90 | 2.81 |

Three searches were rated as the most violating of privacy: school official pat-down,[183] school official cell phone search,[184] and police officer cell phone search.[185] Airport security[186] and a search of garbage left at the curb[187] were the least violating of privacy. The same pattern was found for ratings of expectations of privacy.

TABLE 4: RATINGS OF PRIVACY EXPECTATIONS AND VIOLATIONS OF PRIVACY OF THIRD-PARTY SEARCH VIGNETTES
(0 = NOT AT ALL VIOLATED; 5 = EXTREMELY VIOLATED)

| **Search** | **Expectation of Privacy** | **Violation of Privacy** |
|---|---|---|
| *Physical Searches* | | |
| Pat-down (school) | 4.22 | 4.16 |
| Backpack (school) | 3.67 | 3.68 |
| Bus passenger's bag | 3.35 | 3.42 |
| Bedroom with parental consent | 3.78 | 3.65 |
| Blood draw | 3.33 | 3.33 |
| Plain view | 3.31 | 3.39 |
| Fingerprint student (police) | 3.09 | 3.16 |
| Drug sniff (police) | 3.09 | 3.12 |
| Drug sniff (school) | 3.04 | 2.92 |
| Random drug test (extra-curricular) | 2.83 | 2.67 |
| Property around a home | 2.98 | 2.98 |
| Random drug test (sports) | 2.64 | 2.63 |
| Stop and talk | 2.36 | 2.51 |
| Flashlight through car window | 2.49 | 2.49 |
| Garbage | 2.27 | 2.22 |
| Airport security | 2.13 | 2.15 |

183. Average rating of a school official pat-down search for violating an expectation of privacy was 4.16. *See infra* Table 4.

184. Average rating for a school official cell phone search violating an expectation of privacy was 4.14. *See infra* Table 4.

185. Average rating for a police officer cell phone search violating an expectation of privacy was 4.00. *See infra* Table 4.

186. Average rating for an airport security search violating an expectation of privacy was 2.15. *See infra* Table 4.

187. Average rating for a search of garbage left at the curb was 2.22. *See infra* Table 4.

| | | |
|---|---|---|
| *Information Searches* | | |
| Cell phone (school) | 4.10 | 4.14 |
| Cell phone (police) | 4.00 | 4.00 |
| Diary | 3.75 | 3.70 |
| Cell phone pictures | 3.75 | 3.86 |
| Instant messages (school) | 3.82 | 3.67 |
| Electronic tracking device on car | 3.31 | 3.45 |
| Social Networking Site (school) | 2.90 | 2.82 |

Search Perspective: Third vs. First Person Searches

An interesting social experiment out of Oregon demonstrates why the perspective of the search might matter in the real world. After Portland, Oregon, public officials openly claimed individuals give up all expectation of privacy in garbage placed at the curb for trash pick-up, two journalists set out "to turn the tables on three of [the] esteemed public officials" and "embarked on an unauthorized sightseeing tour of their garbage."[188] The journalists visited the homes of the local district attorney, police chief, and mayor, and collected items from their garbage, including: a receipt with a complete credit card number, an investment summary, a print-out of a private work-related email, and a newsletter from the Christian conservative organization Focus on the Family.[189] The mayor issued a press release calling the journalists' actions "potentially illegal" and requested a meeting with the journalists and their attorney.[190] Despite the public officials' prior stance on the lack of a privacy interest in garbage, they all reacted negatively to being the subject of such a search.[191] In short, the officials did not seem to think something was a privacy invasion until it happened to them. Slobogin and Shumacher and Chao and colleagues both presented lay adults with searches in both the first and third person to examine whether individuals are susceptible to a similar bias of finding searches as less intrusive when they happen to someone else.[192] Using first person descriptors could be a (admittedly, very, very weak) way to simulate actual privacy invasions.

Like this previous research, this study asked participants to evaluate searches in both a first person perspective and third person perspective.[193] Multilevel modeling ("MLM") was used to examine whether adolescents' ratings of searches presented in the first person differed from the ratings of searches

188. Chris Lydgate & Nick Budnick, *Rubbish! Portland's Top Brass Said It Was OK to Swipe Your Garbage—So We Grabbed Theirs*, WILLAMETTE WEEK (Dec. 23, 2002, 4:00 PM), https://www.wweek.com/portland/article-1616-rubbish.html-2 [https://perma.cc/YW5T-KRUT].

189. *Id.*

190. *Id.*

191. *Id.*

192. Slobogin & Schumacher, *supra* note 84, at 735.

193. This condition was a within-subject variable, meaning each participant was exposed to each scenario twice—once in the first person (*e.g.*, a search of *your* backpack) and once in the third person (*e.g.*, a search of *a student's* bag).

presented in the third person.[194] Separate models were tested for each of the following individual outcome variables: intrusiveness, violations of privacy, and expectations of privacy. But adolescents' ratings of the searches did not vary based on the perspective of the search.[195]

Variables That Predict Privacy Perceptions

To determine whether variables identified by previous research accurately describe the variables adolescents use to determine whether a search violates privacy, two different models were analyzed using MLM.[196] As adolescents' perceptions of the personal nature of the search increased, and as their perceptions of how intrusive the search increased, adolescents viewed the search as more violative of privacy, providing support that adolescents—similar to lay adults in Slobogin and Shumacher's study—use these two dimensions when evaluating

194. MLM is appropriate to use for repeated measures within individual participants to account for the nested structure of the vignettes and to test both within-subject and between-subject differences. *See* Heather Woltman, Andrea Feldstain, J. Christine Mackay & Meredith Rocchi, *An Introduction to Hierarchical Linear Modeling*, 8 TUTORIAL QUANTITATIVE METHODS FOR PSYCH. 52, 52 (2012). MLM accounts for the interdependence of ratings of vignettes within each participant. Further, within-subject variable vignette characteristics (first person vs. third person) are appropriately examined as predictors of outcome ratings. *Id.* at 53. The model was specified as followed:

**Level 1:** $Y_{ij}$ (outcome rating) = $\beta_{0j}$ + $\beta_{1j}$ (vignette characteristic) + $r_{ij}$
**Level 2:** $\beta_{0j} = \gamma_{00} + \mu_{0j}$
$\beta_{1j} = \gamma_{10} + \mu_{1j}$

where $Y_{ij}$ represents scores on the outcome variable for vignette *i* by respondent *j*; $\beta_{0j}$ represents the intercept of respondent *j* (*i.e.*, the average rating across vignettes); $\beta_{1j}$ represents the degree to which ratings vary as a function of vignette characteristic (first-person=0, third-person=1); and $r_{ij}$ represents random error for individual j. Coefficients can be understood as functionally similar to unstandardized regression coefficients, and they represent the degree of association between two variables. All Level 1 parameters include a constant and a unique error term (at Level 2). *Id.* at 58.

195. Contrary to this hypothesis, perspective of vignette was not significantly associated with intrusiveness ratings, $t(3421) = .7$, $p = .48$, ratings of personal nature of item searched, $t(3325) = .49$, $p = .623$, ratings of permission granted for the search, $t(3325) = .68$, $p = .49$, ratings of privacy of the item searched, $t(3325) = -.22$, $p = .83$, ratings of how much the search violated privacy, $t(3325) = -.24$, $p = .81$, ratings of how upset the participant thought they would be, $t(3325) = .53$, $p = .60$, or ratings of how upset the participant thought the average person their age would be, $t(3325) = 1.4$, $p = .16$. These results indicate adolescents do not rate searches presented in the first person differently than those presented in the third person on any of the measured dimensions.

196. The models were specified as followed:

**Level 1:** $Y_{ij}$ (outcome rating) = $\beta_{0j}$ + $\beta_{1j}$ (vignette characteristic) + $r_{ij}$
**Level 2:** $\beta_{0j} = \gamma_{00} + \mu_{0j}$
$\beta_{1j} = \gamma_{10} + \mu_{1j}$

where $Y_{ij}$ represents scores on the outcome variable for vignette *i* by respondent *j*; $\beta_{0j}$ represents the intercept of respondent *j* (*i.e.*, the average rating across vignettes); $\beta_{1j}$ represents the degree to which ratings vary as a function of vignette characteristic (personal nature, consent given, bodily privacy, territorial privacy, communications privacy, and informational privacy); and $r_{ij}$ represents random error for individual j. Separate models were tested for each vignette characteristic and for each of the three outcomes (intrusiveness, violation of privacy, and expectation of privacy). A significant $\beta_{1j}$ coefficient for a given model will provide evidence that an outcome varies as a function of a particular vignette characteristic (*e.g.*, vignettes of a more personal nature will be rated significantly higher with regard to intrusiveness).

The first model includes variables Slobogin and Schumacher identified—personal nature of item searched, intrusiveness of the search, and consent (extent to which permission was granted for the search)—as Level 1 predictors of ratings of how much the search violated privacy.

privacy expectations. But participants were also asked to rate how *consensual* the activity in each description was, and these perceptions of consent provided for the search were *not* related to how much the search violated one's privacy.[197]

Implications from Study 1

One implication from Study 1 is that adolescents view searches of cell phones—either conducted by school officials or police officers—as highly violating privacy, as much as a pat-down search. The Supreme Court indicated a search such as a pat-down is highly intrusive and requires a level of suspicion in a school setting.[198] In light of this research, courts may want to consider that individuals view searches of cell phones similarly to the physical pat-down. Professor Slobogin argues that courts should rethink allowing a lower standard of cause for searches like a Terry stop-and-frisk, even though previous opinions assumed a low level of invasion in a limited, over-the-clothes search.[199] The findings here support Slobogin's contention that may courts should rethink just how invasive a search like a stop-and-frisk may be—if we consider a search of a cell phone as violating an expectation of privacy, so should a stop-and-frisk.

The Supreme Court may agree with adolescents that searches of cell phones are highly invasive, while disagreeing about Terry stop-and-frisks.[200] This reflects another finding from Study 1—while adolescents' ratings of intrusiveness agree with court rulings on searches deemed to be either highly intrusive or not at all intrusive, there is still a "gray area" where adolescents and courts view searches differently. This finding is consistent with Slobogin and Shumacher's comparison of adult ratings to court rulings.[201] This may be because there are some searches that are so intrusive (*e.g.*, search of cell phones) or so not intrusive (*e.g.*, search of garbage placed at a curb) that the vast majority of people, regardless of age or profession, agree on the privacy implications. These findings do not support either the Developmental or the Generational Hypotheses because, indeed, maybe adolescents' privacy expectations are not all that different at all.

Contrary to Slobogin and Shumacher's and Chao and colleagues' findings, adolescents in the current study did not rate searches presented in the first person differently than those presented in the third person. This may be due to a phenomenon referred to as the egocentric bias, in which people fail to consider situations from others' perspective.[202] One form of this bias is the emotional egocentricity bias: when individuals consider others' emotions, they are highly

197. These relationships were not significantly associated with the participant's age, $t(92) = -1.32$, $p = .19$.

198. Safford Unified Sch. Dist. #1 v. Redding, 557 U.S. 364, 364 (2009).

199. Christopher Slobogin, *Equality in the Streets: Using Proportionality Analysis to Regulate Street Policing*, 2 AM. J.L. & EQUAL. 36, 36 (2022).

200. Riley v. California, 573 U.S. 373, 453 (2014).

201. Slobogin & Schumacher, *supra* note 84, at 746.

202. Anthony G. Greenwald, *The Totalitarian Ego: Fabrication and Revision of Personal History*, 35 AM. PSYCH. 603, 604 (1980).

influenced by their own emotions.[203] This bias is enhanced in adolescents compared to adults. Thus, adolescents' ratings of first- and third-person searches may not differ because adolescents are highly likely to consider the third-person searches from their own, first-person perspective.

The current study also examined the privacy domains identified by Fradella and colleagues—bodily, territorial, informational, and communications privacy—and how adolescents' ratings of these domains predicted whether adolescents thought a search violated privacy. All four of the domains were significant predictors of ratings of privacy violations. And while it may be predicted from Professor Fradella and colleagues and adolescents' increased use of electronic communications that ratings of informational and communications privacy may be more predictive of ratings of privacy violations, that was not the case in the current study. This may be because adolescents view searches of property highly connected with information and communications (*e.g.*, a cell phone search) as also violating bodily and personal space privacy. Cell phones are so important to adolescents that they view the phones as part of their personal space, potentially as part of their identity.

Study 1 only examined adolescents' perceptions of searches that courts had already confronted. While the results could be compared to prior research and court rulings, direct comparisons of different age groups were not possible due to different measures and dependent variables. Study 2 seeks to expand the results of Study 1 by including participants across the lifespan to allow for direct comparisons among age groups at one point in time. In addition, Study 2 includes more individual difference variables to empirically evaluate the Generational and Developmental Hypotheses. Because searches of digital communications, such as cell phones and social media sites, are just now reaching the courts, and due to generational differences in the use of these types of communications, Study 2 focused on these types of searches.

### *B. Study 2: Measuring Age Differences in Expectations of Privacy: Social Media Use, Decision Making Capabilities, or Both?*

Study 1 establishes that current adolescents' expectations of privacy have some differences from court rulings on searches, but overall do not differ widely, which somewhat refutes the premise that expectations of privacy are changing.[204] But it is not a direct comparison, as we only looked at data comparing adolescents to court opinions. Study 2 took this inquiry a step further and directly compared expectations of privacy across the lifespan: adolescents, young adults, and adults. To zero in on evolving expectations of privacy in new and emerging technology, this study focused the search scenarios on mainly digital communications.

203. Federica Riva, Chantal Triscoli, Claus Lamm, Andrea Carnaghi & Giorgia Silani, *Emotional Egocentricity Bias Across the Life-Span*, 8 FRONTIERS AGING NEUROSCIENCE 74 (2016).

204. This is assuming court's evaluations of what expectations of privacy society is willing to recognize as reasonable mirror actual societal expectations.

A total of 341 participants completed the second study. The average age of all participants was 33.4 years, encompassing 43 adolescent participants ages 12-17 with an average age of 12.9 years, 129 young adult participants with an average age of 20.3 years, and 169 adults with an average age of 48.6 years.

Participants answered questions regarding their expectations of privacy online from government actors.[205] To crudely measure whether they thought a subjective expectation of privacy is reasonable or not, participants rated how *reasonable* they think it is for government actors to access each piece of information. In addition, participants completed the Barratt Impulsiveness Scale[206] and six items from the Sensation Seeking Scale[207] to measure developmental trajectories of decision making to evaluate the Developmental Hypothesis.[208] Previous research has used these scales to measure the incentive processing system of adolescents.[209]

### Social Media Usage

The majority of participants (94.5%) were a member of at least one social media site. The most popular social media platform was Facebook; 91.4% of participants who are a member of at least one social media site reporting they had a profile on that platform. Approximately 60% of participants who are a member of at least one social media site reported they used Facebook more than any other social media platform. The average number of hours participants spent each day on social media was 1.71, and as participants' age increased, the time they reported they spent on social media decreased.[210]

### Perceptions of Searches for All Age Groups Combined

In an attempt to measure expectations of privacy without using the word privacy, participants were asked how *upset* they would be if law enforcement conducted the search on them. Participants predicted they would be the most

205. Study 2 examined more variables than presented here. Appendix B includes a full list of measures included in Study 2 and a full list of the vignettes and questions that are presented in the current article.

206. *See generally* Jim H. Patton, Matthew S. Stanford & Ernest S. Barratt, *Factor Structure of the Barratt Impulsiveness Scale*, 51 J. CLINICAL PSYCH. 768 (1995).

207. *See generally* Marvin Zuckerman, Sybil Eysenck & H. J. Eysenck, *Sensation Seeking in England and America: Cross-Cultural, Age, and Sex Comparisons*, 46 J. CONSULTING & CLINICAL PSYCH. 139 (1978).

208. The Barratt Impulsiveness Scale (Version 11) is a 30-item self-report measure; participants rate how often they do certain things on a scale of 1 (*almost never/never*) to 4 (*almost always/always*). Higher scores indicate more impulsiveness. The Barratt Impulsiveness Scale Version 11 has been found to be an internally consistent measure of impulsiveness, see Patton et al., *supra* note 206, at 768, and suitable for measuring impulsiveness among adolescents, see Steinberg, *supra* note 140, at 217. The Sensation Seeking Scale is a 19-item true/false measure. The original Sensation Seeking Scale includes four sub-scales: thrill and adventure seeking, disinhibition, experience seeking, and boredom susceptibility. Steinberg only included six items from the original Sensation Seeking Scale because the other items measured impulsivity, not sensation seeking. *Id.* at 219. Both the entire Sensation Seeking Scale and the subset of six items has adequate internal reliability. *See* Zuckerman et al., *supra* note 207, at 146; Steinberg *supra* note 140, at 219.

209. Steinberg, *supra* note 142, at 91.

210. Statistical analysis revealed this relationship was significant ($r = -.22$, $p < .05$).

upset if police officers searched their text messages[211] or private messages,[212] while they would be the least upset if their anonymous social media posts were searched.[213] To get a similar proxy of objective expectations, participants were asked how *upset the average person their age* would be if law enforcement conducted the search on them. Participants predicted the average person their age would be the most upset at a police officer search of their text messages stored on their phone,[214] text messages stored by their cell phone provider,[215] and private messages.[216] Participants predicted the average person their age would be least upset at a police officer search of their anonymous social media posts.[217] Interestingly, participants predicted the average person their age would be *more* upset than the participant would be for each search presented, indicating participants in our study thought they might be more "reasonable" than the average person their age.

Participants also rated searches on the two perceived privacy domains—personal nature and intrusiveness—found in Study 1 to be related to privacy expectations. Text messages[218] and audio of phone calls[219] were rated the most personal, while anonymous social media posts were rated the least personal.[220] Similarly, participants rated searches of text messages, either stored on their cell phone[221] or cell service provider[222] as the most intrusive. Searches of anonymous posts on social media were rated the least intrusive.[223]

Age and Perception of Searches

An important first question is whether (and, if so, how) age is related to views of searches.[224] Age was significantly associated with ratings of intrusiveness and personal nature of item searched; as age of the participant increased, so

211. Average rating of level of upset at a police officer search of text messages was 4.34.

212. Average rating of level of upset at a police officer search of social media private messages was 4.25.

213. Average rating of level of upset at a search of anonymous social media posts was 2.45.

214. Average rating of level of upset of the average person at a search of text messages stored on their cell phone was 5.05.

215. Average rating of level of upset of the average person at a search of text messages stored by the cell phone provider was 4.90.

216. Average rating of level of upset of the average person at a search of social media private messages was 4.89.

217. Average rating of level of upset of the average person at a search of anonymous social media posts was 3.15.

218. Average personal nature rating of text messages was 5.57.

219. Average personal nature rating of the audio of phone calls was 5.31.

220. Average personal nature rating of anonymous social media posts was 2.94.

221. Average intrusiveness ratings of a search of text messages stored on their cell phone was 5.66.

222. Average intrusiveness ratings of a search of text messages stored by their cell phone provider was 5.50.

223. Average intrusiveness ratings of a search of anonymous social media posts was 3.23.

224. Same as the prior analyses, MLM was used for this hypothesis. Level 1 of the model included each vignette and Level 2 was scores on the three risk-taking capacity measures: the Barratt Impulsiveness Scale, the Sensation Seeking Scale, and the self-reported risk-taking behaviors. A separate MLM was conducted for each outcome variable of interest.

did their perception of how intrusive and personal the search was.[225] The next step was to address the question of whether this relationship is due to experience with social media, development of decision making, or both.

Experience with Social Media and Perceptions of Searches

As discussed previously some scholars have posited that use of social media is eroding expectations of privacy, what I deem the Generational Hypothesis of age-related changes in privacy perceptions. I used MLM, like in Study 1, to address the question of whether more experience with social media was associated with privacy ratings.[226] In this model, experience with social media was defined as the length of time participants have used social media and the number of hours per day participants use social media. Consistent with scholars' hypothesis that use of social media is affecting privacy expectations, both years spent on social media and reported hours per day spent using social media were related to participants' ratings of intrusiveness and the personal nature of the item searched.[227] As participants reported they had been using social media for longer, they were more likely to see the searches as intrusive and personal in nature. Hours spent per day on social media had the opposite relationship; as participants spent more time per day using social media, they viewed searches as *less* intrusive and *less* personal in nature.[228]

Development and Search Perceptions

But as discussed above, social media usage (at least hours spent per day) is also related to age. To evaluate the Developmental Hypothesis, privacy expectations were also compared to developmental decision-making variables. Sensation seeking was related to perceptions of searches[229]—as participants increased in sensation seeking, they viewed searches as *less* intrusive and *less* personal in

225. Statistical analyses revealed the relationship between age and intrusiveness was significant ($t(264) = 2.30$, $p < .05$), as was the relationship between age and the personal nature of the item searched ($t(264) = 2.81$, $p < .01$).

226. The following model was tested:

**Level 1:** $Y_{ij}$ (outcome rating) $= \beta_{0j} + r_{ij}$

**Level 2:** $\beta_{0j} = \gamma_{00} + \mu_{0j}$

$\beta_{1j} = \gamma_{10} + \gamma_{11}$ (experience with SNS) $+ \mu_{1j}$

Level 2 predictors include: (a) number of years the participant has used SNS and (b) the number of hours the participant spends on a SNS each day. A separate MLM was conducted for each outcome variable (intrusiveness, violation of privacy, and expectation of privacy).

227. Years spent using social media was significantly associated with ratings of intrusiveness ($t(317) = 2.68$, $p < .001$) and the personal nature of the item searched ($t(317) = 2.80$, $p < .001$).

228. These relationships were also statistically significant—both the association between hours spent daily on social media and intrusiveness ratings ($t(317) = -.250$, $p < .05$) and the association between hours spent daily on social media and personal nature ratings ($t(317) = -2.48$, $p < .05$) were significant.

229. The association between sensation seeking and intrusiveness ratings reached statistical significance ($t(264) = -2.31$, $p < .05$), as did the association between sensation seeking and personal nature ratings ($t(264) = -3.11$, $p < .01$).

nature—but impulsivity was not related to these ratings.[230] This indicates that while development of decision-making capabilities provides *some* explanation for the relationship between age and perceptions of searches, it does not provide the whole story.

Implications from Study 2

Study 2 extended the results of Study 1 by including participants across the age span and adding measures of impulsivity, sensation seeking, and experience with social media to further explore what variables may affect how individuals view searches of online information. This research provides important evidence that expectations of privacy are, in fact, changing over time. Overall, as participants got older, they viewed searches as being more intrusive and more personal in nature. This was both due to a desensitization effect of social media and the lessening role of sensation seeking as individuals' brains develop. In other words, these data provide support for both the Developmental and the Generational Hypotheses.

This has potential implications for the Court's application of the third-party doctrine. The Court has ruled that users do not necessarily surrender all expectations of privacy in their cell phone records just because records are stored by a cell phone provider.[231] In examining participants' ratings of the searches, participants view searches of text message as highly intrusive and upsetting. This is true whether the text messages are stored on a cell phone or stored by a cell phone service provider. While all three age groups rated text messages stored on a cell phone as more personal in nature than those stored by a provider, and rated a search of cell phone text messages as more intrusive than a search of messages stored by a provider (which provides at least some empirical support for a societal acceptance of the third-party doctrine), a search of text messages stored by a provider was rated the second-most intrusive search and the third-most personal in nature overall.

One type of search that participants do not view as very intrusive or personal in nature, in contrast, is a search of anonymous social media posts.[232] The search scenario presented here asked participants how intrusive they thought a state actor merely viewing their anonymous posts would be. Several social media sites, such as Whisper and YikYak, allow users to post anonymously on various topics. Perhaps because these posts—on their face—cannot be associated with any individualizing information, participants were not concerned with potential searches of such information. But this feeling of "safety" in posting information anonymously may not be warranted. Anonymous applications often allow law

230. The association between impulsivity and ratings of intrusiveness and personal nature failed to reach statistical significance at the .05 level.

231. *See generally* Carpenter v. United States, 585 U.S. 296 (2018).

232. The question of anonymous social media posts (those that are not attributed to a single user) is distinct from the question of social media posts attributed to a user under a pseudonym. Further research should explore societal expectations of these types of communications, and if the act of a state actor identifying the author of the post is seen as intrusive.

enforcement to subpoena or get a warrant for identifying information such as IP addresses and location information, and users have been able to create fully automated software that can identify the location of posts with accuracy up to 100 meters.[233] Anonymous posts are likely not as anonymous as users believe, and further research should also inquire into the perceptions of state action by further investigating these posts, such as by obtaining records to identify the poster.

Assumed anonymity may lead posters to do things they would not otherwise do. In 2015, students at both Emory University and Virginia Tech University were arrested for anonymous posts on YikYak stating the user was going to perpetrate a school shooting.[234] Scholars have professed concern over anonymity leading to increased rates of cyberbullying.[235] The same factor that make users less concerned with privacy online—lack of individualizing information—may also make users more likely to make negative comments or even commit crimes. The anonymity may provide a false sense of security for posters to stalk, harass, or bully other users, but the website and law enforcement are still able to track down the poster. Courts may need to take into account the dichotomy between what users *understand* to be the information shared with others and what information *actually* can be accessed by posting online when evaluating expectations of privacy.

## V. SO IS SOCIAL MEDIA ERODING ANY EXPECTATION OF PRIVACY?

The majority of Americans—approximately 72%—use social media, a number that is up from 50% ten years prior and only 5% in 2005.[236] The purpose of these platforms is to share information with other users, but once something is on the Internet, its reach and influence is impossible to curtail. Courts now face the difficult task of determining what expectations of privacy remain reasonable in an age where information is constantly shared, whether the user is aware of the sharing or not. The current studies identified expectations of privacy in today's digital age and how privacy may evolve along with technology. A variety of individual factors may shape privacy expectations; these studies focused on age, development, and experience with social media. Age may affect privacy expectations because, according to the Generational Hypothesis, younger generations have grown up with digital communications and will never know a world that is not constantly connected. But according to the Developmental Hypothesis, development may affect privacy expectations because of enhanced impulsivity and sensation seeking in adolescence. Experience may affect privacy

233. Minhui Xue et al., *You Can Yak But You Can't Hide: Localizing Anonymous Social Network Users*, PROCS. OF THE 2016 INTERNET MEASUREMENT CONF. 26, 26 (Nov. 2016), https://dl.acm.org/doi/pdf/10.1145/2987443.2987449 [https://perma.cc/T46S-3FJ4].

234. T. Rees Shapiro, *Emory University Student Arrested for Shooting Threat Posted on Yik Yak*, WASH. POST (Oct. 13, 2015, 11:18 PM), https://www.washingtonpost.com/news/grade-point/wp/2015/10/13/emory-university-student-arrested-for-shooting-threat-posted-on-yik-yak/ [https://perma.cc/B98H-6GYK].

235. Erin Peebles, *Cyberbullying: Hiding Behind the Screen*, 19 PEDIATRICS & CHILD HEALTH 527, 527 (2014).

236. *Social Media Fact Sheet*, *supra* note 82.

expectations because the more we use social media and other technology that requires sharing information, we may view privacy differently. These studies examined the interplay between the various factors that affect privacy expectations.

The question, then, is what does this mean for the Fourth Amendment? This part will briefly summarize the important findings of the empirical studies discussed above and their direct implications for the Fourth Amendment. Then, the part will review recommendations for replacing or adapting the reasonable expectation of privacy test and argue these replacements do not adequately protect privacy. Finally, this article concludes with a recommendation that courts identify specific factors relevant to societal expectations of privacy, informed by theory and research, that can help guide law enforcement, policymakers, and lower courts as they address new technologies.

### *A. Expectations of Privacy May Be Eroding with Social Media Usage*

Across both studies, a consistent pattern emerged: individuals of all ages view information shared on digital communications such as cell phones as highly private and searches of that information as highly intrusive. In Study 1, adolescents rated searches of cell phones as intrusive as a search of a private diary and nearly as intrusive as a physical pat down. In Study 2, all age groups viewed text messages and private messages sent via social media as the most personal in nature and a search of such communications as highly intrusive; all age groups viewed these types of searches similar to a search of audio recording of phone conversations. It seems that there is something different or special about private communications, even those that are sent via electronic communications.

The participants in Study 2 ranged in age from 12 to older than 60 and, predictably, had equally ranging experiences with social media. As a participant's age increased, they, on average, viewed searches of electronic communication devices as more intrusive. Similarly, as the number of years a participant had been a member of a social media site increased, their average ratings of intrusiveness and personal nature of the item searched also tended to increase. Older participants—even those who are not digital natives—have more years they could be using social media, so it makes sense the results mirror one another.

The other proxy measure of experience with social media, the number of hours per day a user spends on a social media site, had the opposite relationship with perception of searches: as the self-reported number of hours per day on social media increased, average ratings of intrusiveness and personal nature of information *decreased*. Users who spend more time on social media each day view searches of private communications as less intrusive and view sharing this type of information as less personal in nature. This is evidence of a desensitization to the privacy risks associated with electronic communication devices, which supports the Generational Hypothesis. As a user incorporates social media into their daily life, to the point they are logged on to a site for upwards of ten hours a day (as some participants here reported), they may become used to constantly sharing information with others, and less concerned about an unintended party viewing their information.

The results also partially supported the Developmental Hypothesis. While one measure of development of decision making—impulsivity—had no relationship to perceptions of searches, sensation seeking did. As sensation seeking increased, the average ratings of intrusiveness and personal nature decreased. Participants higher in sensation seeking viewed searches of electronic communication devices, on average, as less intrusive and the information as less personal in nature. These participants who scored high in sensation-seeking may focus on the rewards associated with sharing information—positive attention from others—and may view searches of their information as a potentially good thing. Sensation seeking may mediate the relationship between age and perceptions of intrusiveness and be one explanation for why older individuals (because sensation seeking tends to decrease with age) viewed searches as less intrusive.

Aside from individual differences, people may view governmental intrusions of privacy differently depending on the type of information sought. Fradella and colleagues explored how lay perceptions of searches differed by the type of privacy interest implicated, but further research can explore how privacy interests differ depending on the type of information revealed by the search. Fourth Amendment jurisprudence generally ignores the type of information or evidence revealed by a search, focusing instead on the act of the search itself.[237] But if lay individuals view governmental intrusions differently depending on the domain intruded upon, scholars may need to consider the implications for Fourth Amendment case law. It may be that certain searches likely to reveal information in a domain that is considered private (*e.g.*, the type of information you would send as an instant message to a friend on a social media site) are considered more intrusive. While the current studies focused on the medium of communication that was searched, future studies can explore whether lay individuals view intrusions of privacy differently depending on domains.

The relationship between age, development, experience, and privacy is complicated. But what can be determined from the current results is that social media usage is changing views of privacy. Scholars have mused for years that the nature of privacy is likely changing due to our reliance on wired communications, and these results, in general, support that hypothesis.[238] So what should we do with this information?

### *B. If Expectations of Privacy Are Eroding, Should the Fourth Amendment Scope Shrink to Recognize That?*

Much ink has been spilled lamenting the circular nature of the *Katz* reasonable expectation of privacy test and how expectations can be conditioned or eroded over time.[239] But if people stop caring about whether others have access to their personal information, should the Fourth Amendment reflect that in

237. *See, e.g.*, Kagehiro et al., *supra* note 84, at 307.

238. For a summary of the circularity hypothesis and data to suggest it may just be a myth, see Kugler & Strahilevitz, *supra* note 17, at 1761.

239. Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979); Leary, *supra* note 68, at 67–68.

limiting the definition of a search? If we truly tie the scope of the Fourth Amendment to societal expectations, the end result would be fewer actions are considered a search as expectations of privacy erode. But this is not the correct way to define Fourth Amendment searches, for several reasons. For one, relying solely on evolving expectations of privacy would work against the interest in the stability of judicial decisions. Second, if we go back to the historical purpose of the Fourth Amendment—to prevent government overreach—a shrinking Fourth Amendment scope is still of concern. And, finally, merely acknowledging that expectations of privacy are eroding fails to account for the automatic nature and vast amounts of data that private companies collect.

One concern regarding allowing fluctuating expectations of privacy to determine the scope of the Fourth Amendment is stability in court judgments. Hypothetically, if expectations of privacy drastically change over time, a government action that was once declared a search in violation of a reasonable expectation of privacy could later be ruled *not* such a violation. As an example, the Supreme Court reasoned the use of a thermoimaging device to view heat emanating from a home was a violation of expectations of privacy because it was a device not in general public usage.[240] There could be a world, though, where eventually such a device is available to and used by the public (say, if thermoimaging devices become available on Amazon).[241] If a law enforcement agency decides to resume use of this type of device without a warrant, and this use is challenged in court, should the court rule that the device no longer violates a reasonable expectation of privacy, overturning a precedent that is only 20 years old?[242] A strict application of the text of *Kyllo* and may end with that result.[243] Thus, courts need to do more to account for the changing nature of expectations in their analysis of the *Katz* test to further the interest in stability of court rulings.

The second concern with relying solely on societal expectations of privacy to determine the scope of the Fourth Amendment is that it does not reflect the original purpose of the Fourth Amendment: government overreach. The Fourth Amendment was drafted in response to government use of general warrants in the British colonies, primarily by customs officials to search homes and businesses.[244] The concern behind the amendment is not solely privacy but to prevent the government from obtaining too much power.

240. Kyllo v. United States, 533 U.S. 27, 34–35 (2001).

241. In fact, Amazon does sell a number of thermoimaging cameras and other tools. *See Results for Thermoimaging*, AMAZON, https://www.amazon.com/s?k=thermoimaging&crid=2QNBDO4M5B70&sprefix=thermoimaging%2Caps%2C75&ref=nb_sb_noss_2 [https://perma.cc/8HC3-TWGR] (last visited Feb. 6, 2024).

242. Professor Slobogin dubbed a similar consideration the "Walmart test": "If the item is available at Walmart, it is likely to be affordable to and accessible by a large segment of the public." Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo*'s Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393, 1403 (2002).

243. The majority opinion in *Kyllo* did not conduct a reasonable expectation of privacy evaluation, instead constructing a test that "[w]here, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." *Kyllo*, 533 U.S. at 40.

244. Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1193–94 (2016).

One way courts address this purpose of the Fourth Amendment is through equilibrium adjustment.[245] Professor Kerr posits courts (either explicitly or implicitly) adjust the strength of Fourth Amendment powers in response to changes in the balance of power between the government and private citizens.[246] As the government gains more power, either through advancements in technological surveillance or otherwise, courts increase Fourth Amendment protections to reassert the balance that was established at the time of the passage of the Fourth Amendment.[247] When government power decreases, though, courts loosen Fourth Amendment protections to regain that balance.[248] This equilibrium adjustment approach could also be used to counteract changing expectations of privacy: as expectations of privacy lessen, courts can look to other sources of privacy rights to return the balance of power.

The final reason not to rely solely on lessening expectations of privacy is that technology and electronic communications are a different type of animal when it comes to data collection and dissemination, and people may not fully understand the ramifications of this large amount of information. In other words, what people do not know may actually hurt them.[249]

### *C. Applying the Third-Party Doctrine to Electronic Communications*

The Court addressed a similar concern in *Carpenter*, when it decided not to strictly apply the third-party doctrine to CSLI. In the 1970's, the Court reasoned that an individual must assume responsibility for the risk of sharing information with a third party, such as a bank teller or a telephone operator.[250] The Court grounded this doctrine in reasonable expectations of privacy: users do not have any legitimate expectation of privacy in information they knowingly and willingly share with a third party.[251] But the information the Court dealt with in *Miller* and *Smith* was limited to bank records and telephone numbers dialed, respectively.[252] Electronic communication devices today, however, collect and transmit an incredible amount of data. Cell phone towers track our movements while we actively make phone calls or passively receive automated alerts from the applications on our phones.[253] Social media sites collect our likes and dislikes and the identity of our friends and family.[254] Fitness trackers store information

245. Orin Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 478 (2011).

246. *Id.*

247. *Id.*

248. *Id.*

249. Eric Johnson, Note, *Lost in the Cloud: Cloud Storage, Privacy, and Suggestions for Protecting Users' Data*, 69 STAN. L. REV. 867, 892 (2017).

250. United States v. Miller, 425 U.S. 435, 444 (1976); Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

251. *Smith*, 442 U.S. at 743.

252. *Miller*, 425 U.S. at 436; *Smith*, 442 U.S. at 737.

253. Brief for Empirical Fourth Amendment Scholars as Amici Curiae Supporting Petitioners at 2–3, United States v. Carpenter, 585 U.S. 296 (2018) (No. 16-402).

254. Jill Lehmann, *How Social Media Algorithms Work*, RISE MKT. GRP. (Mar. 29, 2023), https://risemkg.com/how-social-media-algorithms-work/ [https://perma.cc/3L2H-DNDL].

about our heart rate and activity level (and may even be able to tell when a user is pregnant before she realizes it herself, or whether a plaintiff is faking an injury).[255]

In addition to the amount of information technology collects, users do not always make the explicit choice to share information with a third party. It is likely that in the 1970's users were aware they were sharing their bank records with the bank teller when they handed over the ledger and aware they were sharing a phone number dialed with the telephone operator. Today, though, technology users do not hand over information to another person. Cell service providers and application platforms automatically collect much of the information without an explicit exchange of data, or the language describing the sharing of information is buried in hundreds of pages of terms and conditions.[256] The data users provide is, in a way, an unlisted price of using the technology.

Facebook, for example, sold massive amounts of user data to advertisers and political firms.[257] Applications users installed on the Facebook site collected information on user identities, personal networks, and "likes." The firms then used this information to target specific advertisements to specific users.[258] While there was a public outcry over this alleged data breach, all user information that the application collected was collected with consent, though some applications did collect data on users' friends without those friends' explicit consent.[259]

A strict application of the third-party doctrine would hold that almost all electronically shared data is not protected by the Fourth Amendment. Thus, the government would not need to have probable cause to search Facebook's data because users have no reasonable expectation of privacy in that information. While this interpretation of the third-party doctrine may be in question after the Court's analysis in *Carpenter*, courts are still finding the third-party doctrine applies to information voluntarily shared online.[260] In light of the results of the current research, that users of all ages view private messages sent via text or social media as secret as a personal diary, this would be contrary to societal expectations of privacy.

Courts developed the third-party doctrine over four decades ago, long before the amount of information society shares online was even imaginable. Society's experience with digital communications then looked very different than that experience does now. Courts struggle with how to apply the reasonable

255. Alex Hern, *Your Fitness Tracker Knows You're Pregnant Before You Do*, GUARDIAN (Feb. 8, 2016, 6:24 AM), https://www.theguardian.com/technology/2016/feb/08/fitness-tracker-pregnant-fitbit [https://perma.cc/97AT-ZVMY].

256. Caroline Cakebread, *You're Not Alone, No One Reads Terms of Service Agreements*, BUS. INSIDER (Nov. 15, 2017, 6:30 AM), https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11 [https://perma.cc/JHE3-HNMM].

257. Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html [https://perma.cc/27FB-YLNX].

258. *Id.*

259. *Id.* At least, with consent to participate in research included in the application's terms of service; it is not clear whether users actually read those terms or understood them to mean their data would be collected.

260. *See supra* notes 53–67 and accompanying text.

expectation of privacy test to technology that changes must faster than does the law. Added to that, judges differ demographically from the general public and may have less experience with new technology, and so they may be unable to adequately evaluate expectations of privacy. A strict application of the reasonable expectation of privacy test and particularly the third-party doctrine could lead to a complete loss of the right to privacy protected by the Fourth Amendment because individuals share so much information. Should courts, then, change the reasonable expectation of privacy test or abandon it altogether and replace it with a new test?

### *D. Recommendations for Replacing or Adapting the Reasonable Expectation of Privacy Test*

Many legal scholars have proposed answers to the problem of determining reasonable expectations of privacy, mostly revolving around either adapting the reasonable expectation of privacy test or doing away with it altogether.[261] Approaches suggested by other scholars include looking to legislation or other sources of law, retaining the reasonable expectation of privacy test but comparing digital and electronic information to physical searches, or adapting the reasonable expectation of privacy test for a normative or regulatory approach.

One option would be to forgo the examination of reasonable expectations of privacy and instead look to positive law, which encompasses not only legislation but also common law, administrative regulations, and other sources.[262] Professors Baude and Stern argue this approach is more consistent with the underlying purpose of the Fourth Amendment to prevent against government overreach, moving the focus from privacy to power.[263] Professor Leonetti similarly suggest courts look to other sources of law, particularly property principles such as trespass, nuisance, and theft, to determine what types of property should be protected by the Fourth Amendment.[264] This approach is reminiscent of—but not the same as—the physical intrusion model of the Fourth Amendment, espoused in early twentieth century cases and later returned to in *Jones*.[265] But turning solely to legislation and other sources of law will not fully protect privacy rights. For one, legislation directly on privacy is relatively rare, with the United States currently lacking a federal comprehensive scheme. Additionally, legislation is subject to the whims of the current Congress and can easily change. Relying on legislation and other sources of law will create uncertainty, especially when considering different states are free to experiment with various statutory schemes that could greatly change how the Fourth Amendment is implemented

261. Orin Kerr, *The Misunderstood "Reasonable Expectation of Privacy" Test*, VOLOKH CONSPIRACY (Feb. 9, 2010, 8:54 PM), http://volokh.com/2010/02/09/the-misunderstood-reasonable-expectation-of-privacy-test/ [https://perma.cc/76HS-8VBZ].

262. William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1823 (2016).

263. *Id.* at 1827–28.

264. Carrie Leonetti, *A Grand Compromise for the Fourth Amendment*, 12 J. BUS. & TECH. L. 1, 11 (2016).

265. Olmstead v. United States, 277 U.S. 438, 467 (1928); United States v. Jones, 565 U.S. 400 (2012).

in each jurisdiction. And even if we turn to legislation for privacy rights, it is important we still have the Constitution to provide a floor for individual rights.

Still other scholars claim changing the doctrine will not do enough to protect privacy and we need broader societal changes in its place. Former Ninth Circuit Chief Judge Kozinski and Professor Nguyen point out the increasing use of sharing information online does not necessarily mean individuals are willingly giving up privacy, because many people are unaware of how their information is stored and shared.[266] They argue an educational campaign, along with government regulation of information disclosures and courts adapting the reasonable expectation of privacy test, can help protect privacy interests.[267] Professor Leary calls on Fourth Amendment litigants to provide courts with better evidence of technological capabilities and privacy expectations, and on legislatures to pass laws to protect privacy interests.[268] Orin Kerr similarly describes legislation and case law as independent and parallel systems that can help protect privacy interests.[269] Professor Scott expresses concern the Fourth Amendment cannot adequately protect privacy interests and society needs better community oversight to fill the gap.[270] While these suggestions are laudable, there is little progress towards protecting privacy rights on a federal level and little to no evidence that educating individuals would improve matters.[271]

Some scholars attempt to analogize to other Fourth Amendment case law to provide a framework for analyzing electronic communication privacy expectations outside of the third-party doctrine. Professor Ferguson would incorporate into the reasonable expectation of privacy test a concept of digital curtilage.[272] Findlay compares social networking sites to a home, the type of property that has traditionally received the fullest Fourth Amendment protections.[273] Professor Kerr proposes a distinction between coding and content information that would

266. Alex Kozinski & Eric S. Nguyen, *Has Technology Killed the Fourth Amendment?*, CATO SUP. CT. REV. 15, 16 (2011).

267. *Id.*

268. Leary, *supra* note 68, at 94–95.

269. Orin Kerr, *An Economic Understanding of Search and Seizure Law*, 164 PA. L. REV. 591, 594 (2016).

270. Jeramie D. Scott, *Social Media and Government Surveillance: The Case for Better Privacy Protections for Our Newest Public Space*, 12 J. BUS. & TECH. L. 151, 157, 161 (2017).

271. The European Union has addressed privacy rights with the General Data Protection Regulation (GDPR) that went into effect in 2018. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016 J.O. (L 119) 1–2, 13. The stated purpose of the measure is to give users more control over their data. To do this, the GDPR enhanced the requirements regarding consent to collect and use information, including requiring consent language to be clear and prevent companies from combining consent to lots of different data collection into one document. Under the GDPR, users must be able to withdraw their consent at any time and to access their data if they so desire. The GDPR grants users the "right to be forgotten"—to ask the website to erase all their data and to prevent any third party the site provided the data from using the data going forward. This type of policy puts the decision whether to share information firmly in the hands of the user, but attempts to guide the user by placing more control over private data in the hands of the consumer. H.R. 8152, 117th Cong. (2022).

272. Andrew G. Ferguson, *The "Smart" Fourth Amendment*, 3 CORNELL L. REV. 547, 553 (2017).

273. Daniel Findlay, Note, *Tag! Now You're Really "It:" What Photographs on Social Networking Sites Mean for the Fourth Amendment*, 10 N.C. J.L. & TECH. 171 (2008). This new doctrine would recognize a reasonable expectation of privacy in all stored data and communications that are closely associated with the device, marked as secure from other users, and implicate a personal or family-use interest. *Id.* at 193–200.

protect all information that is the "content" of a communication, but the addressing or coding information such as the email address or phone number to which the message is sent is not protected.[274] Kerr sees similarities between this approach and the more traditional approach used for physical property: there is a reasonable expectation of privacy in anything located "inside" physical property (such as property inside of a home), but not in anything that is "outside."[275] This approach is familiar to judges but new(ish) types of data do not fit neatly into physical search boxes. For example, whether the subject field for emails is coding or content is up for discussion, as is the URL of a website visited, as both can provide extensive information about the content of the item but are both, technically, part of the addressing or coding information.

Finally, some scholars call for a complete abandonment of the reasonable expectation of privacy test in exchange for a normative or regulatory approach.[276] Professor Gardner would restate the standing requirement for Fourth Amendment searches as whether society *should* allow law enforcement officers to conduct such a search.[277] This would involve a balancing between the impact of the search conduct on society's sense of security with the utility of the conduct as a law enforcement technique. This approach, though, fails for many of the same reasons an examination of expectations of privacy does. Judges are not policymakers, and it is not clear they would be good at making policy decisions on new technology when, demographically, the judicial branch is likely to have less experience with the new technology than the greater population.

274. The results of Study 2 demonstrate how this distinction may not work for electronic communications. Searches of "coding" information, such as phone numbers dialed or cell phone contacts, were not rated as highly intrusive or highly personal in nature, while searches of "content" information, such as text messages, audio of phone calls, and documents, were rated as highly intrusive and personal in nature. This finding supports the distinction courts have made between information regarding the intended address of a recipient, which by its nature is necessarily shared with a third party, and the content of a message. Even in the digital age, where all information sent via digital communication is shared with a third party, individuals view content information as more private than coding information. Differing expectations in addressing information and content information did not hold true, however, for posts and pictures shared on social media. These types of searches were rated as not very intrusive and not very personal in nature. This is possibly because the purpose of these types of posts is to share information with many other people. Users posting a message on another user's profile intend that user, and the user's friends, to be able to read that message. In that way, social media posts are more like coding information that is necessarily shared with others and not meant to be kept private. Courts evaluating searches of social media posts may be able to analogize to coding information when determining whether the Fourth Amendment protects such searches. Another difficulty for the coding vs. content distinction is websites. The URL of a website a user visits could be seen as coding information because the user must type in the address in order to visit that particular site. On the other hand, the URL—which frequently includes a descriptive title of the website—can provide information about the content included on the website, which in turn can provide information about the user. But participants in the current study did not rate searches of websites visited as highly intrusive or personal in nature, and considered such searches fairly reasonable. This may be because participants see such information like coding information that must be shared with a third party. Alternatively, participants may be accustomed to third parties tracking the websites they visit—employers and schools regularly restrict and monitor Internet traffic—that such searches are now routine.

275. Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1020 (2009).

276. *Id.* at 1016.

277. Martin R. Gardner, *Rediscovering Trespass: Towards a Regulatory Approach to Defining Fourth Amendment Scope in a World of Advancing Technology*, 62 BUFF. L. REV. 1027, 1073 (2014).

Another option is viable, though, and that is to utilize empirical research on expectations of privacy, not just to inform courts of subjective expectations of privacy but also to provide theory and structure to the factors courts should consider when evaluating whether a government act was a search.[278]

### *E. Empirically and Theoretically Defining Expectations of Privacy: A Case for Privacy Theory and Research*

Instead of reformulating the reasonable expectations of privacy test—or, perhaps, in addition to reformulating the test—courts may best be able to protect privacy by utilizing empirical research on expectations of privacy. Scholars have published research on empirical expectations of privacy and can continue to do so as technology evolves. "[E]mpirical research findings lend legitimacy to the Court's role as a decider of privacy," but empirical findings can go further than that to help guide judicial rulings.[279] Empirical research can provide a benchmark against which judges can evaluate their own subjective expectations of privacy and provide a theoretical framework for factors to consider in new cases. Professors Hazel and Slobogin advocate for the use of survey results in Fourth Amendment analyses because, for instance, these results can be relevant to societal acceptance of privacy expectations and because societal mores (which influence privacy) can best be determined through empirical evidence.[280]

Empirical research can be useful by providing a benchmark of how judges' expectations compare to those of lay individuals. As discussed above, judges are not always explicit in how they evaluate societal expectations of privacy. In the absence of clear guidance, some judges may implicitly turn to their subjective expectations to rule. But judges may be influenced by cognitive biases like the hindsight bias or a third-person perspective, and due to generational and/or developmental differences judges may feel very differently than do other segments of society. Empirical research can provide a check on this type of reasoning, so judges can better evaluate those expectations society is willing to recognize as reasonable.

Of course, empirical findings alone cannot be the answer. Empirical research is time consuming and rarely tailored to the specific fact pattern before the court. To be helpful to courts, researchers would have to constantly update studies as new technologies are developed and to include a representative sample of society in their studies. As a result, the law would still lag behind technology because technology will move faster than the empirical studies can. But the law quite often moves even more slowly, and the knowledge that will be added as a result of these studies will help craft a more complete Fourth Amendment. Research such as the current study can also be valuable to identify those domains

278. The use of empirical evidence to help guide judicial evaluations of expectations of privacy has previously been espoused by other scholars. *See* James W. Hazel & Christopher Slobogin, *"A World of Difference"? Law Enforcement, Genetic Data, and the Fourth Amendment*, 70 DUKE L.J. 705, 706 (2021).

279. Smith et al., *supra* note 112, at 140.

280. Hazel & Slobogin, *supra* note 278, at 761–62.

or factors that relate to expectations of privacy, which can then be used by courts to analogize to pending cases.

Research has explored those factors *courts* consider when ruling whether an action was a search,[281] but research can also be valuable in explaining those factors that *lay people* find important. Factors such as privacy zones, intrusiveness of the search action, and personal nature of the item searched all appear to be important to lay people and thus should also be considered by courts. Psychological, cognitive, and communications theories can all help provide the basis for examining certain factors to determine whether lay people use these factors in evaluating privacy interests.

Empirical evidence is one tool to help courts evaluate expectations of privacy, and one courts have used in the past.[282] Courts have been exposed to research in Fourth Amendment cases; empirical legal researchers filed an *amicus* brief in *Carpenter* arguing empirical research demonstrates individuals are not aware cell phone companies track their location using cell site location information and people do retain an expectation of privacy in both cell site location information and GPS coordinates.[283] While it's not clear whether this brief influenced the Court's ultimate decision, such briefs can provide valuable information to courts evaluating expectations of privacy.

Privacy expectations are a result of a number of factors, including age, development, and experience with social networking sites. As generations continue to grow up with constantly new and changing technology, privacy expectations will also evolve and change. To adapt alongside technology, courts can turn to empirical studies to help guide them. The current Article is a first step in providing an understanding of what factors shape expectations of privacy and how expectations of privacy may evolve alongside technology.

281. Tokson, *supra* note 30, at 30–43.

282. The Supreme Court has utilized empirical research in other areas of the law such as sentencing schemes for adolescent offenders. *See* Roper v. Simmons, 543 U.S. 551, 564–68 (2005); Miller v. Alabama, 567 U.S. 460, 494–95 (2012).

283. Brief for Empirical Fourth Amendment Scholars as Amici Curiae Supporting Petitioners at 1–2, United States v. Carpenter, 585 U.S. 296 (2018) (No. 16-402).

## APPENDIX A: MEASURES FOR STUDY 1

**Perceptions of searches.**

For each of the following searches, participants rated on a scale from 0 (not at all) to 5 (extremely):

How personal was the thing that was searched

How much did the search interfere with property or a person

How intrusive was the search

How much permission the individual searched gave for this search

How much does this search violate privacy of a person's body

How much does this search violate privacy of a person's space

How much does this search violate privacy of information

How much does this search violate privacy of communications

Do you expect this type of thing to be kept private?

**Searches** (the case that evaluated whether a similar action fell within the Fourth Amendment is in parentheses and was not included in the questionnaire presented to the participants). Searches were presented in both a first person and third person tense to each participant (*e.g.*, "A police officer draws blood" vs. "A police officer draws *your* blood") in random order.

Searches followed by an asterisk were included in previous research

1. A police officer draws blood to test the blood for alcohol (*Schmerber v. California*, 384 U.S. 757 (1966))*
2. A school principal asks a student for permission to search her purse for evidence of smoking cigarettes in school. The student says no, but the principal searches her purse anyway (*New Jersey v. TLO*, 469 U.S. 325 (1985))*
3. A school principal suspects a student of having drugs. She pats down the student's outer clothing and asks the student to strip down to her bra and underwear. The principal asks the student to shake out the bands of her bra and underwear to see if there are drugs inside (*Safford Unified Sch. Dist. #1 v. Redding*, 557 U.S. 362 (2009))*
4. A school has a policy of randomly drug testing any student who participates in extra-curricular activities, including sports, band, and clubs (*Bd. of Educ. v. Earls*, 536 U.S. 822 (2002))*
5. A school has a policy of randomly drug testing and student who participates in sports at the school (*Vernonia Sch. Dist. v. Acton*, 515 U.S. 646 (1995))*
6. Police officers see evidence of a crime sitting out in plain view, and enter a home to take that evidence (*Payton v. New York*, 445 U.S. 573 (1980))*
7. Police officers search the area around a person's home (*Oliver v. United States*, 466 U.S. 170 (1984))*
8. Police officers place an electronic tracking device on a car. The officers track the car's movement (*United States v. Jones*, 564 U.S. 400 (2023))

9. Everyone flying at an airport must go through a metal detector and their bags go through an X-ray machine before they can get to their gate (*United States v. Davis*, 370 U.S. 65 (1962)*
10. A police officer pulls over a driver. While the police officer is questioning the driver, the officer shines his flashlight in the backseat to observe what the passengers are doing (*Texas v. Brown*, 460 U.S. 730 (1983))*
11. Police officers bring a trained drug-sniffing dog to a school and ask students to line up in the hallway. The dog walks up to and sniffs each student (*Doran v. Contoocook Valley Sch. Dist.*, 616 F. Supp. 2d 184 (D.N.H. 2009))
12. A school principal brings a trained drug-sniffing dog to school and asks students to line up in the hallway. The dog walks up to and sniffs each student (*Doe v. Renfrow*, 631 F.2d 91 (7th Cir. 1980))
13. A police officer comes to a teenager's house when the teenager is not there. The teenager's mom lets the police officer search the teenager's bedroom (*Georgia v. Randolph*, 547 U.S. 103 (2006))*
14. A police officer takes a teenager's cell phone. The police officer looks through the teenager's text messages, phone calls, and what websites the teenager has visited (*Riley v. California*, 573 U.S. 373 (2014))
15. A teacher takes a student's cell phone. The teacher looks through the student's text messages, phone calls, and what websites the student has visited (*G.C. v. Owensboro Pub. Schs.*, 711 F.3d 623 (6th Cir. 2013))
16. A police officer stops a teenager on a public sidewalk. The police officer asks the teenager questions for about 10 minutes (pre-frisk facts of *Terry v. Ohio*, 382 U.S. 1 (1968))*
17. Two police officers get on a bus at a scheduled stop. The police officers ask to search the passenger's bags (*Florida v. Bostick*, 501 U.S. 429 (1991))
18. Police officers read a private diary to find evidence of breaking the law (non-state actor facts analogous to *Burdeau v. McDowell*, 256 U.S. 465 (1921))*
19. Police officers go through garbage that has been put on the curb (*California v. Greenwood*, 486 U.S. 35 (1988))*
20. Police officers search a teenager's cell phone and use pictures on there as evidence of a crime (*Texas v. Granville*, 423 S.W.3d 399 (Texas Ct. Crim. App. 2014))[284]

284. This case was decided prior to *Riley v. California*, 573 U.S. 373 (2014), which held that a search of the contents of an arrestee's cell phone could not be justified by the search incident to arrest exception to the warrant requirement. *Id.* at 403. But because *Texas v. Granville* dealt precisely with a juvenile, as opposed to *Riley* which addressed the constitutionality of a search of an adult incident to arrest, I have labeled this search "reasonable" as it was determined by the Texas court. A court may likely come to a different conclusion in light of the *Riley* decision, however.

21. Police officers come to a school and pull a student out of a classroom. The officers fingerprint the student (*Texas v. Lanes*, 767 S.W.2d 789 (Tex. 1989))
22. Teacher accesses a student's Social Networking Site profile (*R.S. ex rel. S.S. v. Minnewaska Area Sch. Dist. No. 2149*, 894 F. Supp. 2d 1128 (D. Minn. 2012))
23. Teacher accesses a student's instant messages that the student privately sent to a friend on a Social Networking Site (*R.S. v. Minnewaska Area Sch. Dist. No 2149*, 894 F. Supp. 2d 1128 (D. Minn. 2012)

## APPENDIX B: VIGNETTES FOR STUDY 2

**Vignettes**

For each of the following searches, participants rated on a scale from 0 (not at all) to 5 (extremely): (1) how likely it is that government actors will access the type of information; (2) how reasonable it is for government actors to access the type of information; (3) how upset they would be in the government actor accessed their information; (4) how upset the average person their age would be if a government actor accessed their information; (5) how personal in nature the information is; and (6) how intrusive it is if a government actor views this information.

1. A cellular phone, including all text messages, phone numbers dialed, and websites accessed.
2. Emails saved on a computer
3. Emails saved on a cellular phone
4. Private messages sent to another user on a social networking site
5. Text messages saved by a cellular phone company
6. A user's post on their own profile of a social networking site
7. Pictures a user posts on their social networking site
8. An anonymous post a user posted on a website
9. An audio recording of a telephone call
10. A computer, including all documents stored on the computer and websites accessed on the computer.