UNC SCHOOL OF LAW

NORTH CAROLINA LAW REVIEW

Volume 97 | Number 6 Article 4

9-1-2019

# The Constant and Expanding Classroom: Surveillance in K-12 Public Schools

Barbara Fedders
*University of North Carolina School of Law*, fedders@email.unc.edu

# THE CONSTANT AND EXPANDING CLASSROOM: SURVEILLANCE IN K-12 PUBLIC SCHOOLS*

BARBARA FEDDERS**

*New technologies are expanding schools' ability to keep students under surveillance—inside and outside the classroom—during the school year and after it ends. Schools have moved quickly to adopt a dizzying array of new tools. These include digital learning products that capture and store student data; anonymous tip lines encouraging students to report on each other; and software that monitors students' emails and social media posts, even when they are written from home. Steadily growing numbers of police officers stationed in schools can access this information, compounding the technologies' power.*

*Advocates of these tools argue that they improve student safety and learning outcomes, but this Article reveals that the evidence for this argument is in fact quite thin. Moreover, policymakers have failed to consider important countervailing considerations—most notably, student privacy and its significance for child development; unequal impact, particularly for poor, Black, and LGBTQ youth; and potential liability for school administrators.*

*Using North Carolina's public schools as a case study, this Article makes three contributions to the burgeoning literature on the surveillance state. First, it provides a comprehensive typology that shows the full range of student surveillance. Second, it identifies key procedural and substantive objections to student surveillance that should be—but are not—taken into account by policymakers. Third, it proposes principles to guide the selection, implementation, and oversight of student surveillance.*



** Assistant Professor, University of North Carolina School of Law. I wish to thank Katie Becker, Anna Roberts, and Kathryn Sabbeth for their helpful comments and suggestions. Anne Klinefelter and Mark Weidemaier were especially generous in sharing their time and insights. I presented earlier versions of this Article at the Georgia State University College of Law, the Neighborhood Criminal Law Roundtable, and in Anne Klinefelter's "Current Issues in Privacy Law" seminar, where I received extremely useful feedback. Katie Becker, Kyle Compton, Rebecca Fisher, Anna Gillespie, Kisha Patel, and Lindsay Seventko provided excellent research assistance.

## INTRODUCTION[1]

Today's K-12 public-school students are under surveillance. Inside and outside the classroom, during the school year and summer, students' movements are tracked and their written words monitored. Schools capture enormous amounts of student data, for which the pertinent federal and state laws are insufficient to protect. Schools implement policies, which deputize students to report on each other for a broad range of suspected infractions. Moreover, they create codes of conduct that permit confiscation and, in some cases, exploration of students' cell phones. The number of police officers stationed in schools continues to grow.

1. This Article references various North Carolina public-school policies on electronic surveillance, cell phone use, and SRO usage. For a reference guide to these policies, please see the Resource Guide to North Carolina's Public Schools' Electronic Surveillance, Cell Phone Confiscation, and SRO Policies, which can be accessed at the *North Carolina Law Review's* website, https://www.northcarolinalawreview.org.

The twin justifications for student surveillance are safety and improved educational outcomes.[2] The companies developing these technologies market them against a backdrop of fear of violence, especially school shootings,[3] and anxiety about academic success. State lawmakers appear convinced by these justifications, passing legislation that mandates adoption of some technologies and allocates funds for the purchase of others.[4] Local school districts take advantage of increased state funding to hire school resource officers for kindergarten through the twelfth grade.[5] The various mechanisms of surveillance combine to make more information available about more students, for a longer period of time, and accessible to a greater number of actors than was possible before the digital age.[6]

North Carolina offers a case study of the mostly unexplored dangers of the emerging student surveillance regime: here, as elsewhere, education policymakers are adding, expanding, and enhancing surveillance methods at a rapid pace.[7] They are doing so, both at the state and the school-district level, without adequate consideration of significant competing substantive and procedural issues.[8]

These issues include, at a minimum, the following: first, the evidence for efficacy of many mechanisms of surveillance is thin.[9] Second, although children's growth and healthy development require protection of some age-appropriate degree of privacy[10]—including in a public school functioning *in loco parentis*[11]—students' privacy interests are undervalued by education policymakers.[12]

2. *See infra* Section I.B.

3. *See* Sasha Abramsky, *The School-Security Industry Is Cashing in Big on Fears of Mass Shootings*, THE NATION (Aug. 9, 2016), https://www.thenation.com/article/the-school-security-industry-is-cashing-in-big-on-public-fears-of-mass-shootings/ [https://perma.cc/MT9C-7Q9N] ("In the wake of the December 2012 Sandy Hook massacre in Newtown, Connecticut, one company after another has rushed to take advantage of the opportunities presented by the epidemic of fear that emerged in response to school violence, and to exploit the emotional vulnerabilities of terrified parents.").

4. *See infra* text accompanying notes 172–75.

5. *See infra* Section I.B.2.c.

6. *See generally* Julie E. Cohen, *Surveillance Versus Privacy: Effects and Implications*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE 455, 458–59 (David Gray & Stephen E. Henderson eds., 2017) [hereinafter Cohen, *Surveillance Versus Privacy*] (documenting "emergence of pervasive, networked surveillance").

7. *See infra* Section I.B.

8. *See infra* Part II.

9. *See infra* Section II.A.

10. *See* John Eekelaar, *The Emergence of Children's Rights*, 6 OXFORD J. LEGAL STUD. 161, 169–70 (1986).

11. This common-law doctrine, as described in *Blackstone's Commentaries*, holds:

Third, surveillance does not always operate equitably.[13] The students most vulnerable to surveillance are from low-income families, and those most at risk of adverse outcomes from surveillance are Black and LGBTQ students.[14] Fourth, and finally, school administrators may incur unforeseen legal liability in hastily adopting surveillance practices that function in violation of statutes and judicial precedent that protect student privacy interests.[15]

This Article is the first in the legal literature to identify and analyze the full extent of K-12 student surveillance. Legal scholars have raised concerns about the negative privacy implications for students created by

> [The father] may also delegate part of his parental authority, during his life, to the tutor or schoolmaster of his child; who is then *in loco parentis*, and has such a portion of the power of the parent committed to his charge, *viz.* that of restraint and correction, as may be necessary to answer the purposes for which he is employed.

1 WILLIAM BLACKSTONE, COMMENTARIES, at *453. *See* State v. Pendergrass, 19 N.C. 365, 365 (1837) ("[T]he authority of the teacher is regarded as a delegation of parental authority."). Scholars have criticized the Supreme Court's application of the *in loco parentis* doctrine in cases involving Fourth Amendment challenges to a school's authority, arguing that the Court uses the doctrine only to shield schools from immunity as well as that the doctrine makes little sense as applied to contemporary public school matters since every child is required to go to school. *See, e.g.*, John C. Hogan & Mortimer D. Schwartz, In Loco Parentis *in the United States 1765–1985*, 8 J. LEGAL HIST. 260, 267–68 (1987); Susan Stuart, In Loco Parentis *in the Public Schools: Abused, Confused, and in Need of Change*, 78 U. CIN. L. REV. 969, 969 (2010) (describing how the doctrine is used by courts to "excuse violating student rights, particularly with degrading treatment in matters of search and seizure, but with little or no concomitant recognition of any responsibility to protect students from equally degrading treatment occasioned by sexual harassment and bullying"); Chelsea Lauren Chicosky, Article, *Restructuring the Modern Education System in the United States: A Look at the Value of Compulsory Education Laws*, 2015 BYU EDUC. & L.J. 1, 21–23 (2015) (describing compulsory attendance laws in every state). For a breakdown of each state's minimum and maximum ages of required attendance, see *State Education Reforms*, NAT'L CTR. FOR EDUC. STAT. (2017), https://nces.ed.gov/programs/statereform/tab5_1.asp [https://perma.cc/V6NT-8USB].

12. *See, e.g.*, *Technology Responsible Use*, DURHAM PUB. SCHS. BOARD EDUC., https://www.dpsnc.net/cms/lib/NC01911152/Centricity/domain/139/e-rate/Policy%20Technology%20Responsible%20Use.pdf [https://perma.cc/L6BT-V25A] ("Students and employees must understand the school system technological resources and strictly comply with these requirements and acknowledging awareness that the school system uses monitoring systems to monitor and detect inappropriate use of technological resources. . . . Students, employees, visitors, and other users *have no expectation of privacy in anything* they create, store, send, delete, receive, or display when using the school system's network, devices, Internet access email system, or other technological resources owned or issued by the school system, whether the resources are used at school or elsewhere." (emphasis added)); *see also infra* Section II.B.

13. *See* Elana Zeide, *Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPS*, 8 DREXEL L. REV. 339, 353 (2016) [hereinafter Zeide, *Student Privacy*].

14. *See infra* Section II.C.

15. *See infra* Section II.D.

the vast array of digital learning devices used in public schools.[16] They have also identified the costs and harms of school policing and punitive disciplinary practices.[17] Drawing from each of these bodies of scholarship,[18] this Article makes three principal contributions to the burgeoning legal literature on the surveillance state.[19] It uncovers, in Part I, a pervasive school surveillance regime, exploring the multiple mechanisms for monitoring and tracking students and explaining their heretofore unappreciated range and power. It analyzes, in Part II, the multiple procedural and substantive objections to student surveillance that should be—but largely are not—considered by school decisionmakers. Finally, it proposes, in Part III, principles that should guide the selection, implementation, and oversight of student surveillance mechanisms.

## I. THE STUDENT SURVEILLANCE REGIME

This part introduces the concept of student surveillance. After a working definition is given in Section A, Section B provides a typology that reveals the pervasiveness and power of contemporary student surveillance. Drawing on recent policymaking in North Carolina at the legislative and school-district level, Section B also demonstrates how surveillance regimes both deploy sophisticated technologies and rest on policy choices that prioritize and facilitate constant monitoring by administrators, school resource officers, and students themselves. Section B further illustrates how the aims of promoting safety and improved learning outcomes have accelerated surveillance's development.

16. *See, e.g.*, Susan P. Stuart, *Lex-Praxis of Education Informational Privacy for Public Schoolchildren*, 84 NEB. L. REV. 1158, 1159–62 (2006) (arguing that "[p]ublic schools are information-collection machines"); Zeide, *Student Privacy*, *supra* note 12, at 347–53.

17. *See, e.g.*, Barbara Fedders, *The Anti-Pipeline Collaborative*, 51 WAKE FOREST L. REV. 565, 566 (2016) (discussing how public school administrators increasingly borrow tactics and terminology from the criminal system and giving, as examples, the overuse of long out-of-school suspensions based on criminal-law concepts of retribution and deterrence, the stationing of school police in most public middle and high schools, and the use of juvenile courts to handle quotidian in-school misbehavior); *see also* Jason P. Nance, *Students, Security, and Race*, 63 EMORY L.J. 1, 3–7 (2013) [hereinafter Nance, *Students, Security, and Race*]; Jason P. Nance, *Student Surveillance, Racial Inequalities, and Implicit Racial Bias*, 66 EMORY L.J. 765, 767–73 (2017); Elizabeth A. Shaver & Janet R. Decker, *Handcuffing a Third Grader? Interactions Between School Resource Officers and Students with Disabilities*, 2017 UTAH L. REV. 229, 229–32.

18. For the most part, scholars concerned about student informational privacy and those concerned about punitive discipline and student criminalization have remained distinct. For a notable counterexample, see Emily F. Suski, *Beyond the Schoolhouse Gates: The Unprecedented Expansion of School Surveillance Authority Under Cyberbullying Laws*, 65 CASE WESTERN RES. L. REV. 63, 63–64 (2014).

19. *See, e.g.*, Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 1–4 (2008) (describing and defining a "National Surveillance State" and asserting that "[t]he question is not whether we will have a surveillance state in the years to come, but what sort of surveillance state we will have").

### *A. Surveillance: What Is It?*

Sociologist David Lyon, a leading scholar of the interdisciplinary field of surveillance studies, defines surveillance as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection, or direction."[20] Foundational fictional[21] and film[22] treatments of surveillance focus on its use as a tool for nation-states to maintain control through the suppression of dissent. Contemporary surveillance, by contrast, is distinguished by its public-private hybridity[23] and its multiplicity of purpose.[24] Local, state, and federal social welfare, law enforcement, and counter-terrorism departments and agencies rely on information technologies created by private companies to collect, analyze, and aggregate data about individuals.[25] They use this data for many purposes: determining eligibility for government benefits; assessing the likelihood of future child abuse or neglect; predicting the location and source of criminal activity; and evaluating membership in organizations deemed hostile to U.S. interests, to name just a few.[26]

Of course, surveillance does not require technology. Before the digital age, social welfare agencies and police departments routinely placed people under surveillance, with the burden falling disproportionately on poor people, especially poor people of color.[27] Technology does, however,

20. DAVID LYON, SURVEILLANCE STUDIES: AN OVERVIEW 14 (2007).

21. GEORGE ORWELL, NINETEEN EIGHTY-FOUR 3–7 (1949).

22. THE LIVES OF OTHERS (Wiedemann & Berg 2006).

23. I am indebted to Melissa Jacoby for inspiring this insight. *See generally* Melissa Jacoby, *Corporate Bankruptcy Hybridity*, 166 U. PA. L. REV. 1715 (2018) (presenting a public-private bankruptcy model whereby bankruptcy responsibilities are allocated amongst private and public parties in part to "improve regulatory functioning").

24. *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1937 (2013) (describing surveillance as a routine part of the typical administrative apparatus with a wide variety of purposes).

25. *See* Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Richards*, 126 HARV. L. REV. F. 262, 262–65 (2013), https://harvardlawreview.org/2013/06/addressing-the-harm-of-total-surveillance-a-reply-to-professor-neil-richards/ [https://perma.cc/DS24-3EY6].

26. VIRGINIA EUBANKS, AUTOMATING INEQUALITY 178–83 (2017).

27. *See id.* at 11–12. Some scholars argue that the contemporary pro-privacy movement focuses too much on data privacy and does too little to acknowledge that the government historically has conducted extremely invasive surveillance of marginalized populations for a wide array of purposes, ranging from "maintaining public order to reinforcing the natural order." Mary Anne Franks, *Democratic Surveillance*, 30 HARV. J. L. & TECH. 425, 427–28 (2017). In *The Poverty of Privacy Rights*, Khiara Bridges draws from eighteen months of fieldwork conducted in a New York City medical center treating women in poverty to arrive at the sobering conclusion that for poor women, privacy rights are more aspirational than real. *See* KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS 34–35 (2017) (theorizing that these women are deprived of privacy rights because society presumes that they do not "possess the character that justifies recognizing the[se] rights in the first instance").

enable more comprehensive surveillance of marginalized people.[28] Technology also exposes a much broader swath of the population to surveillance[29]—particularly where, as in schools, it is deployed pursuant to, and in conjunction with, policies that emphasize monitoring and control.[30] The next section explores and analyzes surveillance technologies and policies in K-12 public schools.

### *B. Typology*

To fully appreciate the scope and power of contemporary student surveillance, consider the experiences of "Manuel," a fifteen-year-old public-school tenth grader.[31] One Saturday night, he posts a photo of himself and a group of male friends—all Latino—on Instagram, captioning it "Me and My Crew." The boys are making a variety of gestures with their hands—peace signs, thumbs-up signs, and other gestures of indeterminate meaning. His school, which owns a third-party social media-scanning software program, is alerted by the company that makes the program due to what its algorithm identifies as suspicious activity. On Monday, the assistant principal directs the school resource officer ("SRO") to question him about the Instagram post. Manuel explains that the photograph simply shows him and his friends having fun. Not satisfied with that explanation, the SRO trails him at every class exchange. The SRO also asks for and reviews footage from the school's video cameras from the past week. The assistant principal alerts Manuel's teachers that he suspects Manuel of possible gang involvement. When Manuel sneaks a look at his cell phone during math class, his teacher confiscates it, referencing the student code of conduct prohibiting students from having their phones out in class. Later Monday night, on the school-issued laptop he uses because his parents cannot afford to buy him his own, Manuel takes a break from his homework and emails a friend to confide that he is depressed, anxious about the SRO, and angry at a mutual friend, Jose. Within an hour, a

28. *See* EUBANKS, *supra* note 26, at 11.

29. *See, e.g.*, I. Bennett Capers, *Crime, Surveillance, and Communities*, 40 FORDHAM URB. L.J. 959, 960–62 (2013) (describing dramatic growth in the number of surveillance cameras in New York City over a forty-year period and diffusion from high-crime areas to most parts of the city).

30. *See infra* Section I.B.2.

31. "Manuel" is not a real child. His experiences are a composite of those of students I am aware of from my work directing the University of North Carolina School of Law Youth Justice Clinic as well as accounts published by companies that make software for monitoring students. His surveillance experience is not meant to be representative of any one student's forty-eight-hour experience; rather, the hypothetical is intended to illustrate the range, power, and impact of contemporary student surveillance technologies and policies.

different SRO is at his home, alerting his parents that he is conducting a "wellness check" because of concerns over Manuel's email.

### 1. Technologies for Watching

Lyon's definition of surveillance[32]—what it is comprised of and its multiplicity of uses—offers a useful way to think about how schools watch students in the digital age. The following subsections explain how digital learning devices, student monitoring software, and video cameras work as surveillance mechanisms. Additionally, each subsection explains the key financial and legislative underpinnings for the development of these technologies as well as the justifications often offered for their adoption or expansion.

#### *a. Digital Learning and Data Capture*

Digital learning refers to "any instructional practice that effectively uses technology to strengthen a student's learning experience."[33] While the most extreme version is the so-called "cyber school,"[34] brick-and-mortar schools also use a variety of digital learning devices and technologies to supplement traditional methods of teaching and learning.[35]

Digital learning has exploded in the last decade. While schools with limited financial resources may rely on "bring-your-own-device" policies, which permit students to bring in their own devices,[36] schools increasingly

32. *See* LYON, *supra* note 20, at 14.

33. Elementary and Secondary Education Act § 4102, 20 U.S.C. § 7112(3) (Supp. V 2017).

34. Amelia A. DeGory, Note, *The Jurisdictional Difficulties of Defining Charter-School Teachers Unions Under Current Labor Law*, 66 DUKE L.J. 379, 420 (2016) (describing that "cyber school" includes students reporting to a computer lab monitored by teachers as well as students attending classes from computers in their own home).

35. *See* § 7112(3). Digital learning

> encompasses a wide spectrum of tools and practices, including—(A) interactive learning resources, digital learning content (which may include openly licensed content), software, or simulations, that engage students in academic content; (B) access to online databases and other primary source documents; (C) the use of data and information to personalize learning and provide targeted supplementary instruction; (D) online and computer-based assessments; (E) learning environments that allow for rich collabo-ration and communication, which may include student collaboration with content experts and peers; (F) hybrid or blended learning, which occurs under direct instructor supervision at a school or other location away from home and, at least in part, through online delivery of instruction with some element of student control over time, place, path, or pace; and (G) access to online course opportunities for students.

*Id.*

36. *See* Karen J. McLean, *The Implementation of Bring Your Own Device (BYOD) in Primary Schools*, FRONTIERS PSYCHOL., Nov. 2016, at 1, 1; Emma Chadband, *Should Schools Embrace "Bring Your Own Device"?*, NEATODAY (July 19, 2012), http://neatoday.org/2012/07/19/should-schools-embrace-bring-your-own-device/ [https://perma.cc/3477-SDLN].

provide their students with laptops, tablet computers, or other mobile-computing devices. Students can use them in school and sometimes at home, accessing such instructional material as e-textbooks and online tutoring.[37] In addition, teachers and administrators encourage parents to supplement the school curriculum with material provided on myriad third-party educational applications available for no financial cost.[38]

Digital learning proponents argue that the devices make teaching more efficient and effective, learning more personalized, and communication among parties quicker and easier. Teachers can access products that clarify and streamline instruction and curricular development, monitor student work for plagiarism, and assist with classroom management.[39] Students' use of personalized learning technologies provides their teachers with significant amounts of information about their performance—going beyond

37. *See, e.g.*, Mike Desmond, *District Providing All Buffalo School Students with Tablets, Laptops*, WBFO (Mar. 11, 2019), https://news.wbfo.org/post/district-providing-all-buffalo-school-students-tablets-laptops [https://perma.cc/VU2Z-AQ6F] (detailing Buffalo Public Schools' provision of laptops and tablets to students, some of whom may take the devices home); T. Keung Hui, *Wake County Distributing 52,000 New Laptops and Tablets to Schools*, NEWS & OBSERVER (Oct. 19, 2016), https://www.newsobserver.com/news/local/education/wake-ed-blog/article109160952.html [https://perma.cc/YAD4-5DFS] (detailing Wake County's distribution of devices and participation in Bring Your Own Device programs). While one-to-one programs are believed essential to level the playing field for low-income students who cannot afford to purchase their own laptops or tablets, the implementation of digital learning technologies in school means that students must have reliable access to the internet out of school—something that many students do not have. When schools increasingly rely on digital learning materials to deliver material, the need for students to access the internet increases as well. When low-income students do not have regular and reliable access to the internet, the use of digital learning technologies can exacerbate rather than ameliorate wealth-based learning gaps. *See* Rachel Monahan, *What Happens When Kids Don't Have Internet Access at Home?*, THE ATLANTIC (Dec. 12, 2014), https://www.theatlantic.com/education/archive/2014/12/what-happens-when-kids-dont-have-internet-at-home/383680/ [https://perma.cc/PU8U-ZBVN] (quoting a Washington Public Schools Assistant Superintendent as saying "[o]nce you've converted the curriculum, the material, it's more project-based learning. You kind of need the Internet for all those pieces to work well. If you're not able to provide that last level of connectivity, you've now widened the gap in terms of what kids can do, not to mention the expectation around that").

38. *See* Curtiss Streitelmeier, *Make Parents Comfortable with Tech for a Successful 1:1 Program*, EDTECH MAG. (July 30, 2018), https://edtechmagazine.com/k12/article/2018/07/make-parents-comfortable-tech-successful-11-program [https://perma.cc/FU8E-DHJJ]; *Top Educational Apps for Kids*, TALKING PARENTS (Feb. 27, 2019), https://talkingparents.com/blog/march-2019/top-educational-apps-for-kids [https://perma.cc/9A66-P7KK]. While these applications may not have a financial cost, they may impose actual and potential harms on students through their data collection and sharing practices. *See, e.g.*, *In re* Google, Inc. Privacy Policy Litig., No. C-12-01382-PSG, 2013 WL 6248499, at *1 (N.D. Cal. Dec. 3, 2013) (describing Google's business model and noting that "[w]ith little or no revenue from its users, Google still manages to turn a healthy profit by selling advertisements within its products that rely in substantial part on users' personal identification information . . . [and] in this model, the users are the real product"); *see also infra* Section II.A.

39. Zeide, *Student Privacy*, *supra* note 13, at 345–48.

just seeing a student's performance on a particular assignment to include metadata. A teacher can ascertain whether a student struggled to answer a question not only by the answer provided but also by the number of times a student logged into a system and how long she spent on a particular task.[40] Armed with this information, teachers can then presumably differentiate their instruction by providing additional and advanced material to students who can manage it as well as tailoring specific resources for students working at a slower pace so that they can practice and gain mastery.[41] The North Carolina School Superintendent of Public Instruction has argued that personalized learning technology can lessen if not eliminate the need for many summative assessments.[42] Finally, web-based record-keeping platforms make accessing and communicating about grades and disciplinary incidents easier for students, their parents, and teachers.[43] Overall, educators appear enthusiastic about digital learning.[44]

While perhaps not adopted by schools for surveillance purposes, digital learning technologies nonetheless allow for capture of significant amounts of student data by private companies.[45] Along with educational information, a young person's use of digital technology has the potential to

40. Elana Zeide, *The Limits of Education Purpose Limitations*, 71 U. MIAMI L. REV. 494, 505 (2017) [hereinafter Zeide, *Limits of Education*].

41. *See, e.g.*, Heather Elliott, *The Importance of Education Technology in Our Changing World*, SMARTTECH (Sept. 28, 2016), http://edblog.smarttech.com/2016/09/importance-education-technology-changing-world/ [https://perma.cc/XSC7-5JBJ]. *But see* James B. Levy, *Teaching the Digital Caveman: Rethinking the Use of Classroom Technology in Law School*, 19 CHAP. L. REV. 241, 249 (2016) (expressing skepticism about educational technology generally and specifically citing research showing a "'remarkably consistent' pattern extending over time in which classroom technology is both 'oversold and underused'" and finding a "similar pattern with respect to teaching practices that [can be characterized as] 'change amidst constancy,' meaning that even when teachers adopt new technologies, they tend to do so in ways that reinforce established classroom practices rather than change them"(quoting LARRY CUBAN, OVERSOLD AND UNDERUSED: COMPUTERS IN THE CLASSROOM 130, 137, 171, 195 (2001))).

42. Email from Mark Johnson, North Carolina Superintendent of Public Instruction, to North Carolina parents and caregivers of public-school students (Jan. 6, 2019) (on file with the North Carolina Law Review).

43. *See, e.g.*, *Power School*, HOMEBASE: ENGAGE, CONNECT, SUPPORT, https: homebase.ncpublicschools.gov/applications/powerschool [https://perma.cc/YT7K-F3UF] (noting that PowerSchool is the "official student information system used statewide by the public and charter schools of North Carolina for Storing and managing student data"); *see also* Jessica Lahey, *I Will Not Check My Son's Grades Online Five Times a Day*, THE ATLANTIC (Sept. 6, 2013), https://www.theatlantic.com/national/archive/2013/09/i-will-not-check-my-sons-grades-online-five-times-a-day/279385/ [https://perma.cc/NR23-98MN] (noting that seventy to eighty percent of the schools that use PowerSchool implement the parent portal).

44. J. WILLIAM TUCKER & AMELIA VANCE, SCHOOL SURVEILLANCE: THE CONSEQUENCES FOR EQUITY AND PRIVACY 3 (2016), http://www.nasbe.org/wp-content/uploads/Tucker_Vance-Surveillance-Final.pdf [https://perma.cc/J6F9-FWDZ] (citing studies showing educator enthusiasm for digital and online learning).

45. *See infra* notes 49–63 and accompanying text.

leave a data trail that can be available either while a child is a student or later, allowing private interests to mine this data to facilitate the creation of advertising and marketing profiles.[46] One CEO of an educational technology company describes education as the "world's most data-mineable industry, by far."[47] The educational technology industry thus has financial incentives to continue to offer discounted or free devices to schools.[48]

While the federal and state education policy permits and encourages digital learning,[49] regulators have not prioritized protecting student data available to private companies after students use digital learning technologies.[50] The Family Educational Rights and Privacy Act ("FERPA") is the main federal statute that governs the privacy of student data.[51] The law protects student data and regulates access to and use of education records; it gives students and parents the right to review their education records and to challenge misleading or inaccurate information.[52] However, the statute is not sufficiently protective of student information given technological advances. For example, it is unclear whether information about students obtained pursuant to school surveillance technologies is part of their education records.[53] In addition, privacy advocates argue that school districts can circumvent FERPA's requirements that student data not

46. FAITH BONINGER & ALEX MOLNAR, NAT'L EDUC. POL'Y. CTR., LEARNING TO BE WATCHED: SURVEILLANCE CULTURE AT SCHOOL 14 (2016), https://nepc.colorado.edu/sites/default/files/publications/RB%20Boninger-Molnar%20Trends.pdf [https://perma.cc/F98H-LBXA].

47. *Id.* (noting a CEO of an education technology company who boasted, "[w]e literally have more data about our students than any company has about anybody else about anything . . . [a]nd it's not even close").

48. *See* Meriem El-Khattabi, *Mining for Success: Have Student Data Privacy and Educational Data Mining Created a Legislative War Zone?*, 2017 U. ILL. J.L. TECH. & POL'Y 511, 511 (noting that in 2016, one in five students had access to a school-issued Google computing device); Zeide, *Limits of Education*, *supra* note 40, at 511–14 (discussing the value private organizations find in collecting data from educational tools).

49. *See, e.g.*, U.S. DEP'T OF EDUC., TOWARD A NEW GOLDEN AGE IN AMERICAN EDUCATION 11 (2004), https://files.eric.ed.gov/fulltext/ED484046.pdf [https://perma.cc/W5SN-W9CQ] (discussing the implementation of a national education technology plan that acknowledges the significant role technology plays in American education).

50. *See, e.g.*, BONINGER & MOLNAR, *supra* note 46, at 17 (noting that the California student privacy law, generally considered the most student-privacy protective law in the country, does not apply to Google applications that are not explicitly part of the Google Applications for Education suite).

51. Jennifer C. Wasson, Recent Development, *FERPA in the Age of Computer Logging: School Discretion at the Cost of Student Privacy?*, 81 N.C. L. REV. 1348, 1353 (2003).

52. *Id.* at 1353–54.

53. TUCKER & VANCE, *supra* note 44, at 13.

be shared with third parties by "characterizing ed[ucation] tech[nology] companies as 'school officials.'"[54]

Another federal law aimed at protecting minors is the Children's Online Privacy Protection Act ("COPPA"),[55] which proscribes the collection of personal information from a child under the age of thirteen without parental consent.[56] COPPA applies to websites or online services directed at children and any operator of these products with actual knowledge that it is collecting personal information from a child.[57] The statute requires operators of children's websites to post privacy policies outlining "what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information."[58] COPPA, too, has key weaknesses in terms of privacy protection. For one, it only covers students under thirteen. In addition, no private rights of action are available under this statute; instead, the Federal Trade Commission enforces the law.[59]

Some states have enacted data protection laws aimed at filling in gaps left by FERPA and COPPA. California's law, for example—considered the most protective of student privacy—prohibits educational technology companies from knowingly selling student data or using it to create a profile of the student for non-educational purposes.[60] However, even this more robust law cannot guard against redisclosure of student data in the event of purchases, mergers, or other acquisitions.[61] Moreover, privacy scholars and advocates warn that even the most privacy-protective laws do

54. *See, e.g.*, Frida Alim et al., *Spying on Students: School-Issued Devices and Student Privacy*, ELECTRONIC FRONTIER FOUND. 26 (Apr. 13, 2017), https://www.eff.org/files/2017/04/13/student-privacy-report.pdf [https://perma.cc/CE2P-TXL8] (noting that student privacy laws do not apply to Google applications that are not explicitly part of the Google Applications for Education suite).

55. Pub. L. No. 105-277, §§ 1301–1308, 112 Stat. 2681-728, 2681-728 to -735 (1998) (codified as amended at 15 U.S.C. §§ 6501–6506 (2012)).

56. 15 U.S.C. § 6502(b)(1)(A)(ii) (2012).

57. *Id.* § 6502(b)(1)(A).

58. *Id.* § 6502(b)(1)(A)(i).

59. *See, e.g.*, Press Release, Fed. Trade Comm'n, Xanga.com to Pay $1 Million for Violating Children's Online Privacy Protection Rule (Sept. 7, 2006), https://www.ftc.gov/news-events/press-releases/2006/09/xangacom-pay-1-million-violating-childrens-online-privacy [https://perma.cc/DYH7-WLKB] (finding that social network website allowed and had actual knowledge that children under thirteen were creating profiles, resulting in a settlement with the Federal Trade Commission for $1 million).

60. *The State Student Privacy Report Card*, PARENT COALITION FOR STUDENT PRIVACY 9 (Jan. 2019), https://www.studentprivacymatters.org/wp-content/uploads/2019/01/The-2019-State-Student-Privacy-Report-Card.pdf [https://perma.cc/9PZ7-WQ2H].

61. *Id.* at 8.

not address new technologies such as Gaggle.[62] Finally, the possibility of widespread data breaches for students is a real one.[63]

In sum, given the current inadequate regulatory regime, digital learning technologies expose students' personal information to a host of public and private entities that potentially can use this data for non-educational purposes.

*b. Student Monitoring Software*

As the use of digital learning technologies has become more widespread,[64] policymakers have sought to oversee and control the online activity of minors.[65] For example, at the federal level, the Children's Internet Protection Act ("CIPA") requires that schools receiving federal funding adopt an internet security policy that keeps students from accessing obscene visual depictions, child pornography, or images "harmful to minors."[66] Despite the breadth of the material that CIPA restricts—the "harmful to minors" category is quite broad[67]—the statute survived[68] a First Amendment free speech challenge filed by the American Library Association.[69] In some school districts, these statutorily required filters

62. Taylor Armerding, *Schools Keep Track of Students' Online Behavior, but Do Parents Even Know?*, CSO ONLINE (Nov. 4, 2014, 4:16 AM), https://www.csoonline.com/article/2841969/big-data-security/schools-keep-track-of-students-online-behavior-but-do-parents-even-know.html [https://perma.cc/89XT-6DTF]; *see infra* Section I.B.1.b.i.

63. *See generally* JOSEPHINE WOLFF, YOU'LL SEE THIS MESSAGE WHEN IT IS TOO LATE: THE LEGAL AND ECONOMIC AFTERMATH OF CYBERSECURITY BREACHES (2018) (discussing the frequency and ease of electronic data breaches). One North Carolina commentator notes, referring to student data stored online, "[t]hey always say this stuff is protected, but probably a student could hack it." Telephone Interview by Katie Becker with Janine Murphy, Representative, N.C. Sch. Bd. Ass'n (Feb. 20, 2019).

64. *See supra* Section I.B.1.a.

65. *See* Enrique Dans, *Surveillance in Schools: Where is This Taking Us?*, FORBES (Aug. 23, 2018), https://www.forbes.com/sites/enriquedans/2018/08/23/surveillance-in-schools-where-is-this-taking-us/ [https://perma.cc/K4ZE-L57H] (surveying legislative developments and concluding that "[s]igns are, we're headed toward a scenario where students will be permanently under surveillance by cameras, algorithms and all kinds of technologies designed to not only to [sic] monitor their movements, but what they're thinking").

66. 20 U.S.C. § 9134 (f)(1)(a) (2012).

67. *See generally* JUDITH LEVINE, HARMFUL TO MINORS: THE PERILS OF PROTECTING CHILDREN FROM SEX 3–19 (2002) (arguing that "harmful to minors" nomenclature typically constitutes an umbrella term for censorship).

68. United States v. Am. Library Ass'n, 539 U.S. 194, 214 (2003) ("Because public libraries' use of Internet filtering software does not violate their patrons' First Amendment rights, CIPA does not induce libraries to violate the Constitution, and is a valid exercise of Congress' spending power."). Shielding students from "indecent, lewd," or "sexually suggestive speech" was found to be within schools' constitutionally permissible activities because schools' mission is to "inculcat[e] fundamental values necessary to the maintenance of a democratic political system." Bethel Sch. Dist. No. 403 v. Fraser, 478 U.S. 675, 678, 681, 694 (1986).

69. *See* Judith F. Krug, *The Aftermath of the Children's Internet Protection Act*, INSIGHTS ON L. & SOC'Y, Winter 2004, at 1 (noting that the American Library Association had opposed

travel with students when they bring their school-issued computers home, thus broadening the geographical scope of the school's control of students' online activity.[70]

Another example of policymakers' preoccupation with internet oversight can be found at the school-district level. Many districts have policies advising that all work on the internet and with digital devices is subject to school monitoring, whether or not the work is done in school.[71] One district's policy is sweeping both in terms of what it covers and to whom it applies:

> Students and employees must understand the school system technological resources and strictly comply with these requirements and acknowledging awareness that the school system uses monitoring systems to monitor and detect inappropriate use of technological resources . . . . Students, employees, visitors, and other users have no expectation of privacy in anything they create, store, send, delete, receive, or display when using the school system's network, devices, Internet access email system, or other technological resources owned or issued by the school system, whether the resources are used at school or elsewhere, and even if the use is for personal purposes.[72]

In addition to CIPA and district-level policies that provide for monitoring students in their use of technology, third-party software packages permit school districts to move beyond merely protecting students from online material deemed to be harmful.[73] Districts that opt to use these software packages can gain access to a wide swath of student-created content, covering an expanded amount of time.[74] The following sections discuss two such products.

CIPA because it viewed filters as over- and under-inclusive to the stated goals of the act and because of the equity implications of the Act—the millions of low-income people who must rely on a library for Internet access miss much of what is available to people who can afford to pay).

70. Audrey Watters, *When Schools' Internet Filters Follow You Home*, HACKED EDUC. (May 7, 2012), https://hackeducation.com/2012/05/07/when-school-internet-filters-follow-you-home-cipa [https://perma.cc/6F65-RZQK].

71. *See, e.g.*, *supra* note 12 and accompanying text.

72. *Technology Responsible Use*, *supra* note 12; *see also CHCCS Policy Code: 3225 Computer, Network, and Internet Usage*, CHAPEL HILL-CARRBORO CITY SCHS. (2010), https://sites.google.com/site/educationcollaboration/guidelines/chccs [https://perma.cc/V8SQ-XUU8] ("[T]here is no privacy. Schools can monitor, check, and capture student input.").

73. *See infra* Section I.B.1.b.

74. *See infra* Section I.B.1.b; *see also* LYON, *supra* note 20, at 14 (noting that surveillance is "not random, occasional, or spontaneous").

### i. Safety Management Platforms

Schools that wish to easily and efficiently monitor student-created content on school-issued computers and transmitted over school internet servers have the option of using so-called safety management platforms. These programs use natural-language processing to sift through the millions of words typed by students.[75] One such platform is Gaggle; schools that purchase this product obtain the software along with access to a team of off-site "security specialists" trained to look for an unspecified group of words deemed troubling.[76] When, as in the case of Manuel, they are alerted that students have typed such words, company representatives contact the school, and, in some cases, law enforcement.[77] School officials and law enforcement can, and do, in turn notify the student's parents and sometimes visit the student's home in-person.[78]

Schools may justify the use of safety management platforms by referencing the need to detect any or all of the following: signs of intent to commit self-harm, indications of intent to commit violence, and verbal harassment that rises to the level of cyberbullying.

Consider first the argument about the need to detect student intent to commit self-harm.[79] Rates of depression and anxiety among young people have soared in recent years,[80] as has the number of students engaging in

75. *See* Simone Stolzoff, *Schools are Using AI to Track What Students Write on Their Computers*, QUARTZ (Aug. 19, 2018), https://qz.com/1318758/schools-are-using-ai-to-track-what-students-write-on-their-computers/ [https://perma.cc/5F7R-BTHG]; *see also* Dans, *supra* note 65 (describing development of artificial intelligence methods to track what students are doing and predictive algorithms to analyze the probability of negative student outcomes, including dropping out, and noting that these developments are "driven by policies that support the virtually unlimited collection of student data from the earliest stages").

76. Corey Tutewiler, *Discipline vs. Teachable Moments: Defined*, GAGGLE, https://www.gaggle.net/speaks/discipline-vs-teachable-moments-defined/ [https://perma.cc/M7F5-HMWG].

77. *Id.*

78. *See* Press Release, Educ. Writers Ass'n, A Growing Number of Districts are Selecting Gaggle's School Safety Solutions to Protect Their Students (Feb. 6, 2019), https://www.ewa.org/press-release/growing-number-districts-are-selecting-gaggles-school-safety-solutions-protect-their [https://perma.cc/U524-UL5J] (describing the notification process by which Gaggle notifies administrators and parents when student activity is flagged); *Wassau School District: The Priceless Value of a Student's Life*, GAGGLE, https://www.gaggle.net/success-stories/wausau-school-district [https://perma.cc/M8BX-TWXG] (discussing suicide-prevention tactics of performing home "wellness checks" on students whose online communications are flagged).

79. *See* Press Release, Educ. Writers Ass'n, *supra* note 78 (describing how Gaggle helped to prevent student suicide in the schools where it is used and listing "partner districts" from around the country).

80. *See, e.g.*, Laurence Steinberg, *Anxiety and Depression in Adolescence*, CHILDMIND INST. (2017), https://childmind.org/report/2017-childrens-mental-health-report/anxiety-depression-adolescence [https://perma.cc/E4YJ-39LG] (noting that anxiety and depression are on

self-harm that results in a hospital visit.[81] Between 2007 and 2014, the suicide rate among middle-school youth doubled.[82]

Along with concern about the potentially self-harming student herself, educators might justify the purchase and use of Gaggle by pointing to evidence that a self-harm history correlates with violent acts against others; one study showed that sixty-one percent of school assailants had a history of suicide attempts.[83]

While school shootings are extremely rare,[84] they dominate school safety planning.[85] Along with contracting with security companies for the installation of "hard target" mechanisms—bullet-proof glass, door locks, metal detectors, and the like[86]—school violence prevention efforts also often include so-called "threat assessments" of students. These are undertaken *after* a student has committed a serious or violent infraction in order to help the school determine the appropriate response and

the rise and that high school students have more anxiety symptoms and are twice as likely to see a mental health professional as teens in the 1980s).

81. Melissa C. Mercado et al., *Trends in Emergency Department Visits for Nonfatal Self-Inflicted Injuries Among Youth*, 318 JAMA 1931, 1931 (2017). Girls and transgender youth are particularly vulnerable. *Id.*; *see* Claire M. Peterson et al., *Suicidality, Self-Harm, and Body Dissatisfaction in Transgender Adolescents and Emerging Adults with Gender Dysphoria*, 47 SUICIDE & LIFE-THREATENING BEHAV. 475, 475 (2017) (noting a study showing that approximately thirty percent of transgender youth report a history of at least one suicide attempt, and nearly forty-two percent report a history of self-injury, such as cutting).

82. Centers for Disease Control and Prevention, *QuickStats: Death Rates for Motor Vehicle Traffic Injury, Suicide, and Homicide Among Children and Adolescents Aged 10–14 Years—United States, 1999–2014*, MORBIDITY & MORTALITY WEEKLY REP. (Nov. 4, 2016), https://www.cdc.gov/mmwr/volumes/65/wr/mm6543a8.htm?s_cid=mm6543a8_w [https://perma.cc/83A8-2FPG].

83. *See* Allison Paolini, *School Shootings and Student Mental Health: Role of the School Counselor in Mitigating Violence*, VISTAS ONLINE, 1, 3 (2015), https://www.counseling.org/docs/default-source/vistas/school-shootings-and-student-mental-health.pdf?sfvrsn=f2db432c_6 [https://perma.cc/CW7Y-TJQC].

84. *See* Elizabeth S. Scott, Miller v. Alabama *and the (Past and) Future Regulation of Juvenile Crime*, 31 LAW & INEQ. 535, 541 (2013) (noting that "children face a greater risk of being struck by lightning" than being shot in school); *see also* Abramsky, *supra* note 2 (discussing the rarity of school violence).

85. Matthew T. Theriot, *School Resource Officers and the Criminalization of Student Behavior*, 37 J. CRIM. JUST. 280, 280 (2009) ("Though contrary to statistics showing that school crime nationally was declining, relatively rare, and usually nonviolent, school shootings fed growing public fear of juvenile and school crime." (citation omitted)); *see also* Kate Stringer, *American Schools Are Safer Than Ever, but Annual Education Poll Reveals 1 in 3 Parents Now Fear That Their Children are in Danger on Daily Basis*, 74 MILLION (July 17, 2018), https://www.the74million.org/article/american-schools-are-safer-than-ever-but-annual-education-poll-reveals-one-in-three-parents-now-fear-their-children-are-in-danger-on-daily-basis/ [https://perma.cc/Z896-5YDM] (chronicling parental fears about school safety).

86. *See* Mark Keierleber, *School-Security Companies Are Thriving in the Era of Mass Shootings*, THE ATLANTIC (Aug. 9, 2018), https://www.theatlantic.com/education/archive/2018/08/school-security-mass-shootings/567080/ [https://perma.cc/DYP3-VVAZ].

disciplinary decision.[87] Accurately predicting the commission of *future* violent behavior is "almost impossible," and the FBI cautions against trying to do so.[88] Nonetheless, schools are keen to obtain any data that would help them prevent violence, especially a shooting, and so they seek any and all clues that students' words might provide.[89] Products like Gaggle make the search for clues easier.[90]

Finally, safety management platforms may reveal what administrators believe to be not only indicators of self-harm or intention to commit violence but also suggestions of verbal harassment or bullying of other students. Like other states, North Carolina requires school districts to adopt a policy prohibiting bullying or harassing behavior;[91] cyberbullying[92] is included in many such policies.[93] According to one study, seventy-two percent of internet users between the ages of twelve and seventeen reported at least one instance of cyberbullying.[94]

87. *See Threat Assessments for School Administrators & Crisis Teams*, NASP (2015), https://www.nasponline.org/resources-and-publications/resources-and-podcasts/school-climate-safety-and-crisis/systems-level-prevention/threat-assessment-at-school/threat-assessment-for-school-administrators-and-crisis-teams [https://perma.cc/T9R6-S3J6] (describing three-part process of identifying student threats to commit a violent act, determining the seriousness of the threat, and developing intervention plans that protect potential victims and address underlying problems).

88. *See* MARY ELLEN O'TOOLE, NAT'L. CTR. FOR THE ANALYSIS OF VIOLENT CRIME, FED. BUREAU OF INVESTIGATION ACAD., THE SCHOOL SHOOTER: A THREAT ASSESSMENT PERSPECTIVE 2–3 (2009).

89. *See Can Artificial Intelligence Prevent School Violence?*, INST. ELECTRICAL & ELECTRONICS ENGINEERS (2019), https://innovationatwork.ieee.org/can-artificial-intelligence-prevent-school-violence [https://perma.cc/8C6T-PSKE] (quoting Gaggle executive claiming "[s]tudies have shown that kids communicate before a violent act happens and they will communicate electronically. If you don't have the means to hear those cries out for help you're going to have children in jeopardy").

90. Gaggle is not the only such product. *See id.* for a discussion of other products that make use of artificial intelligence to enable schools to search content created by students.

91. N.C. GEN. STAT. §§ 115C-407.15 to .16 (2017).

92. David D. Luxton, Jennifer D. June & Jonathan M. Fairall, *Social Media and Suicide: A Public Health Perspective*, 102 AM. J. PUB. HEALTH (SUPP. 2), 195, 196 (2012) (defining cyberbullying as the targeting of a child or teen through threats, harassment, and humiliation, by means of technologies such as e-mail, messaging applications, texting, or social networking sites and stating this behavior as only constituting cyberbullying if it is repeated and intentional). Despite the fact that academics may define cyberbullying as requiring repetition, many states punish single instances. For example, in North Carolina, cyberbullying is a misdemeanor offense and does not require any repetition. *See* N.C. GEN. STAT. § 14-458.1(b) (2017).

93. *See, e.g.*, *Policy Code 3226/4205 Internet Safety*, WAKE CTY. PUB. SCH. SYS. (Oct. 4, 2016), https://boardpolicyonline.com/bl/?b=wake_new&s=208219#&&hs=194199 [https://perma.cc/2ANG-AYVV].

94. Suski, *supra* note 18, at 66–67. "[F]orty-six states and the District of Columbia now have laws prohibiting cyberbullying." *Id.* at 66. These states range in terms of the ways in which they define bullying—some require repeated acts, whereas many, like North Carolina, consider a single proscribed act to constitute bullying—as well as whether they require the bullying activity to have a nexus to the school environment. *Id.* at 70–72.

Three features of the internet appear to work together to explain the frequency of cyberbullying reports among young people.[95] First, the expectation of anonymity that users have when accessing the internet frees them to be bolder[96]—and sometimes crueler[97]—versions of themselves than they would be offline. The immediate social repercussions that typically attend a negative in-person interaction are absent in cyberspace.[98] Second, unlike comments and letters, internet posts are often permanent.[99] Third, networked technologies exponentially expand the audience of a hateful post. Just as the internet facilitates student collaboration on schoolwork,[100] so too might it fuel the formation of collectives of destructive behavior.[101]

### ii. Social Media Scanning Software

Another way that schools monitor student-created content is through the use of products that scan students' public social media postings, whether or not the postings are made using the devices or on-site school internet servers.

One such product is Social Sentinel.[102] Created by a former law enforcement officer, this product scans multiple social media platforms, searching students' words, images, and videos.[103] The platform is "powered by proven machine learning and artificial intelligence logic," which the company argues can allow it to sort through postings to accurately determine threats requiring immediate action as well as "insights for a broader context, leading to a greater understanding."[104] Manuel's Instagram

95. *See* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 4–5 (2014) ("The Internet extends the life of destructive posts . . . [n]etworked technologies exponentially expand the audience for cyberharassment.").

96. *Id.* at 57 ("Anonymity can bring out our worst behavior . . . [and] can nudge us to do terrible things.").

97. *See* Eric Y. Drogin et al., *Psycholegal Aspects of Cyberbullying: The Dark Side of Social Networking*, ABA SCITECH L., Spring 2012, at 5.

98. *Id.*

99. *See* CITRON, *supra* note 95, at 4 (noting that posts have no "built-in expiration dates" and "[s]earch engines produce results with links to destructive posts from years earlier").

100. *See supra* note 35 and accompanying text.

101. CITRON, *supra* note 95, at 62 ("The hoods of the Ku Klux Klan were key to the formation of mobs responsible for the death of African Americans. In our time, anonymity has encouraged the formation of destructive cyber mobs . . . ."); *see* CASS R. SUNSTEIN, REPUBLIC.COM 2.0, at 55 (2007) (explaining that when groups with similar views get together, their members hear "more and louder echoes of their own voices").

102. *Our Platform*, SOC. SENTINEL, https://www.socialsentinel.com/platform [https://perma.cc/2HUD-GSXP].

103. *Social Sentinel Adds Integration with Gmail, Image Recognition and an Anonymous Sharing Platform to its Suite of Products*, SOC. SENTINEL (Mar. 28, 2019), https://www.socialsentinel.com/post/social-sentinel-product-release-announcement [https://perma.cc/5MKD-LDDX].

104. *Our Platform*, *supra* note 102.

post presumably would fall into the category not of an emergent threat but that of "insights for a [broader] context."[105]

Because they scan all students' public posts, Social Sentinel and similar products may be less likely to generate controversy than more targeted—and duplicitous—online tactics of school administrators targeting students' private posts.[106] In the past, at least one administrator engaged in trickery—creating fake social media accounts through which she could become "friends" with students and get access to their private postings.[107]

Currently only twenty percent of North Carolina districts publicize that they are using Gaggle,[108] others note that they use social media scanning software.[109] The popularity and decreasing cost of educational technology suggest that the number of districts that use safety management platforms and social media scanning software will likely increase.[110] Indeed, school districts can apply for funding from a general safety set-aside program through the state Department of Public Instruction.[111]

105. *Id.* For a discussion of how artificial intelligence can reinforce racial and other forms of bias, see, for example, Karen Hao, *This is How AI Bias Really Happens—And Why It's So Hard to Fix*, MIT TECH. REV. (Feb. 4, 2010), https://www.technologyreview.com [https://perma.cc/D6ZM-MU5M]. For further discussion of how surveillance technologies operate inequitably, see *infra* Section II.C.

106. *See* Somini Sengupta, *Warily, Schools Watch Students on the Internet*, N.Y. TIMES (Oct. 28, 2013), https://www.nytimes.com/2013/10/29/technology/some-schools-extend-surveillance-of-students-beyond-campus.html [https://perma.cc/TG3Q-7LZX (dark archive)] (documenting case of Missouri principal who resigned amid accusations that she had spied on students using fake social media accounts).

107. *Id.*

108. *See* Resource Guide discussed *supra* note 1; *see also Bring Your Own Technology Initiative Lights Up Classroom*, CHARLOTTE-MECKLENBURG SCH. (Dec. 5, 2012), http://www.cms.k12.nc.us/News/Pages/BringYourOwnTechnologyinitiativelightsup.aspx [https://perma.cc/9X5D-V5QR]. It is possible that school districts are employing this and other technologies without notifying the public that they are doing so. For a critique of this absence of transparency, see *infra* Section III.B.

109. Derrick Lewis, *Orange County Schools Implementing Social-Media Monitoring for Students*, CBS 17 (June 28, 2018), https://www.cbs17.com/news/local-news/orange-county-news/orange-county-schools-implementing-social-media-monitoring-for-students/1269571066 [https://perma.cc/ND6K-8VSL].

110. *See supra* Section I.B.1a.

111. Current Operations Appropriations Act of 2018, ch. 5, § 7.27(a)-(b), (h), 2018-2 N.C. Adv. Legis. Serv. 1, 33 (LexisNexis) (to be codified at N.C. GEN. STAT. § 115C-105.51) (creating grant for "Safety Equipment"); *see 2018–2019 School Safety Grants School Safety Equipment Grant Application*, N.C. DEP'T PUB. INSTRUCTION (2018), http://www.dpi.state.nc.us/docs/cfss/home/equipment-application.pdf [https://perma.cc/85XM-LU95] (defining "[s]urveillance equipment and cameras" as an "[a]llowable [e]xpense[]" under the school safety equipment grant program).

*c. Video Cameras*

Nationwide, the overwhelming majority of schools use security video cameras to monitor students.[112] Cameras are increasing in sophistication. Most of the schools that use cameras also have recording systems.[113] Until recently, real-time monitoring of cameras was not feasible because it was expensive and inefficient.[114] Now, however, some surveillance cameras have cloud-based storage, which means that administrators can use a browser-based dashboard to view a video feed on their computer or phone, enabling people off campus to monitor in real time what is happening on campus.[115] In addition, school districts have, or may soon be equipped with, face recognition software.[116]

Cameras are typically stationed throughout the school—in the cafeteria, entrances, hallways, and sometimes even in classrooms.[117] The only places in schools where they consistently do not appear are bathrooms and locker rooms.[118]

112. *See Fast Facts: School Safety and Security Measures*, NAT'L CTR. FOR EDUC. STAT., https://nces.ed.gov/fastfacts/display.asp?id=334 [https://perma.cc/HRU7-UYT3] (reporting that seventy-three percent of elementary schools, eighty-nine percent of middle schools, and ninety-four percent of high schools "use security cameras to monitor the school").

113. Bryan R. Warnick, *Surveillance Cameras in Schools: An Ethical Analysis*, 77 HARV. EDUC. REV. 317, 319 (2007).

114. *See id.*

115. Dan Tynan, *Digital Surveillance Systems Help Keep K-12 Students, Staff Safe from Harm*, EDTECH MAG. (Apr. 3, 2018), https://edtechmagazine.com/k12/article/2018/04/digital-surveillance-systems-help-keep-k-12-students-staff-safe-harm [https://perma.cc/7LQQ-7HP9] (noting that an additional perceived advantage is that these cameras consume less network bandwidth than "traditional IP cameras").

116. *See* Ava Kofman, *Face Recognition is Now Being Used in Schools, but It Won't Stop Mass Shootings*, THE INTERCEPT (May 30, 2018, 12:36 PM), https://theintercept.com/2018/05/30/face-recognition-schools-school-shootings/ [https://perma.cc/EDT7-9P9D]; *see also* Tom Cheshire, *25 Big Ideas for 2012: Ubiquitous Face Recognition*, WIRED (Jan. 9, 2012, 9:22 AM), http://www.wired.com/business/2012/01/ubiquitous-face-recognition [https://perma.cc/LY56-JNEA] (noting concerns over face recognition technology "mission creep" and quoting a security technology expert as saying that "[r]ecognizing people in photographs works well, . . . [b]ut attempts to pick terrorists out of crowds have failed, resulting in systems that do a great job surveilling innocents and a terrible job identifying the guilty").

117. *See* Warnick, *supra* note 113, at 319.

118. *Id.*; *see infra* notes 300–04 and accompanying text (discussing case law regarding reasonable expectations of privacy and video cameras); *see also Privacy in Education: Guide for Parents and Adult-Age Students*, PRIVACY RTS. CLEARINGHOUSE (July 1, 2015), https://www.privacyrights.org/consumer-guides/privacy-education-guide-parents-and-adult-age-students [https://perma.cc/39RY-WDLY]. When an individual "seeks to preserve [something] as private," Katz v. United States, 389 U.S. 347, 351 (1967), and his expectation of privacy is "one that society is prepared to recognize as 'reasonable,'" the Court has held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause. *Katz*, 389 U.S. at 361 (Harlan, J., concurring). Changing rooms and bathrooms, at least for now, are locations in schools in which students have expectations of privacy that courts

The justification often given for video cameras is that they deter student misbehavior—fighting, drug or alcohol use or distribution, as well as less serious infractions—through promoting student self-monitoring.[119] Under this theory, simply by knowing they are being recorded—and potentially observed—students will refrain from engaging in misbehavior. In addition, video footage can aid in after-incident investigation by administrators to determine student involvement and culpability. It can be incriminating or exculpatory, serving as evidence in school discipline proceedings and criminal prosecutions.

During the 1999–2000 school year, nineteen percent of public schools were equipped with security cameras; by the 2015–16 school year, eighty-one percent of schools had them.[120] Their popularity may derive in part from their unobtrusiveness relative to other forms of security—metal detectors, and drug-sniffing dogs, for example.[121] It is also the case that multiple funding sources for new and improved cameras are available. In North Carolina, school districts can apply for funding to install or upgrade video cameras.[122] In addition, surveillance technology companies have begun offering face-recognition software for free to school districts.[123]

### 2. Policies for Monitoring and Control

Along with using technologies that capture significant amounts of student data, scanning content created by students both in and out of

recognize as reasonable. *See, e.g.*, Brannum v. Overton Cty. Sch. Bd., 516 F.3d 489, 492, 496 (6th Cir. 2008).

119. *See, e.g.*, Lynn A. Addington, *Cops and Cameras: Public School Security as a Policy Response to Columbine*, 52 AM. BEHAV. SCIENTIST 1426, 1431 (2009) (documenting use of webcams in hallways and classrooms for, *inter alia*, deterrence of criminal activity); Mitchell L. Yell & Michael E. Rozalski, *Searching for Safe Schools: Legal Issues in the Prevention of School Violence*, 8 J. EMOTIONAL & BEHAV. DISORDERS 187. 193 (2000) (noting deterrence value of surveillance cameras); *see also Brannum*, 516 F.3d at 492, 496 (noting in a case challenging the placement of video cameras in middle school locker rooms that the school had argued that cameras were necessary to improve school security).

120. NAT'L CTR. FOR EDUC. STATISTICS, INDICATORS OF SCHOOL CRIME & SAFETY 2017, at viii (2018), https://nces.ed.gov/pubs2018/2018036.pdf [https://perma.cc/KE5Q-Z5U4].

121. *Id.* at 114, 120.

122. Current Operations Appropriations Act of 2018, ch. 5, § 7.27(a)–(b), (h), 2018-2 N.C. Adv. Legis. Serv. 1, 33 (LexisNexis) (to be codified at N.C. GEN. STAT. § 115C-105.51) (creating grant for "Safety Equipment"); *see also 2018–2019 School Safety Grants School Safety Equipment Grant Application*, *supra* note 111 (defining "[s]urveillance equipment and cameras" as an "[a]llowable [e]xpense[]" under the school safety equipment grant program).

123. Eli Zimmerman, *Company Offers Free Facial Recognition Software to Boost School Security*, EDTECH MAG. (Aug. 3, 2018), https://edtechmagazine.com/k12/article/2018/08/company-offers-free-facial-recognition-software-boost-school-security [https://perma.cc/AKS3-5DM6]. Underfunded schools are uniquely susceptible to offers of free devices and educational software from large educational technology companies. *See* BONINGER & MOLNAR, *supra* note 46, at 25.

school, and tracking students' actions while in the hallways and sometimes the classroom, schools create policies and administer programs that emphasize monitoring and control. Schools use anonymous tip lines, which enable administrators to expand their pool of knowledge about student behavior by deputizing students to report on each other.[124] In addition, codes of conduct that provide for confiscation of student cell phones can lead to investigation of a phone's contents that may disclose details about a student she may wish to keep private, such as her friends' names and contents of their correspondence.[125] What is more, SRO are provided with, or affirmatively seek, data obtained from surveillance technologies and use it to conduct investigations of children both at school and in students' homes. Information obtained through technologies and monitoring policies expands the power and capacity of SRO. Various policies for monitoring and control are discussed below.

*a. Anonymous Tip Lines*

As of the 2019–20 school year, every North Carolina local school administrative unit will be required to develop and operate a confidential, anonymous tip line.[126] These tip lines permit and encourage students to anonymously report each other for a wide range of percieved misconduct.[127]

The justification underlying the adoption of these tip lines is similar to that which motivates student monitoring software, namely, the belief that students share their plans to commit self-harm or to harm others with their peers in advance.[128] The hope is that the anonymity feature of the tip lines will encourage those peers to in turn share the information they are given with administrators.[129] The tip lines accept reports in a broad range of categories that might suggest a student constitutes a risk.[130] One district tip line's drop-down menu, for example, includes subjective categories such as

124. *See infra* Section I.B.2.a.

125. *See infra* Section I.B.2.b.

126. Current Operations Appropriations Act of 2018, ch. 5, § 7.26(a), 2018-2 N.C. Adv. Legis. Serv. 1, 33 (LexisNexis) (to be codified at N.C. GEN. STAT. § 115C-105.51).

127. *See* Press Release, Pub. Sch. of N.C., State Superintendent Mark Johnson Declares September School Safety Month in North Carolina (Sept. 4, 2018), http://www.ncpublicschools.org/newsroom/news/2018-19/20180904-01 [https://perma.cc/QL2P-XJ89].

128. Evie Blad, *More Schools Are Using Anonymous Tip Lines to Thwart Violence. Do They Work?*, EDWEEK (Aug. 10, 2018), https://www.edweek.org/ew/articles/2018/08/10/more-schools-are-using-anonymous-tip-lines.html [https://perma.cc/U5YL-QQUU].

129. *Id.*

130. *Anonymous TipLine*, CHAPEL HILL-CARRBORO CITY SCH., https://www.chccs.org/Page/9633 [https://perma.cc/43GW-9H2E].

"personal crisis" and "isolation," along with the perhaps more obvious category of "danger to others."[131]

The North Carolina General Assembly in 2018 allocated $5 million to fund these tip lines for all grades six or higher.[132] Federal funding for tip lines is also available pursuant to the 2018 STOP Violence Act.[133]

*b. Technology Confiscation Provisions*

Many North Carolina public schools have provisions in their student codes of conduct that regulate the possession and use of technology, including cell phones, that students bring to school.[134] Most schools allow students to bring devices to school—perhaps as a concession to the fact that students own cell phones at increasingly younger ages[135]—but prohibit them from turning them on unless specifically authorized by a teacher.[136] When a student violates the prohibition on activating devices, school personnel may seize them.[137] Disciplinary consequences may follow, such as when a school determines that the phone was used to cheat on a test or send an inappropriate text to another student.[138] In many cases, once confiscated, a phone or other device will be held by the school until a parent appears at the school to obtain it.[139]

131. *Id.*

132. Press Release, Pub. Sch. of N.C., *supra* note 127.

133. Andrew Ujifusa, *House Passes STOP School Violence Act One Month After Parkland Shooting*, EDWEEK (Mar. 14, 2018), https://blogs.edweek.org/edweek/campaign-k-12/2018/03/house_passes_STOP_school_violence_act_one_month_parkland_shooting.html [https://perma.cc/N4TW-VNLP].

134. *See, e.g.*, *Policy 4318: Use of Wireless Communication Devices*, BLADEN CTY. SCHS., https://boardpolicyonline.com/?b=bladen&s=141051 [https://perma.cc/4WMD-9N8W] (stating that "school employees may immediately confiscate any wireless communication devices that are on, used, displayed or visible in violation of this policy" and that "confiscated wireless communication devices will be returned only to the student's parents").

135. Monica Anderson, *Teens, Social Media & Technology 2018*, PEW RES. CTR. (May 31, 2018), http://www.pewinternet.org/2018/05/31/teens-social-media-technology-2018 [https://perma.cc/DGC3-5C2M] (noting that ninety-five percent of teens in a 2018 study stated that they have a smartphone or access to one); *see* Delaney Ruston, Andrew Orlebeke & Talia Friedman, *Survey Reveals That the Majority of U.S. Middle Schools Allow Students to Carry Cell Phones Throughout the School Day*, SCREENAGER (Dec. 13, 2017) https://static1.squarespace.com/static/5a69fe629f8dce3218418fe2/t/5a8ee7be652deaae30b8eb23/1519314881193/CPC+Survey.pdf [https://perma.cc/3DQK-W679] (noting that the average age at which youths get their first smartphone currently is 10.3 years old).

136. *See infra* note 139 and accompanying text.

137. *See, e.g.*, *Policy Code 4318: Use of Wireless Communication Devices*, ALEXANDER CTY. SCHS., https://www.boardpolicyonline.com/bl/?b=alexander#&&hs=364298 [https://perma.cc/HE6D-Z33R].

138. *Id.*

139. *Id.* (authorizing students to have phones at school as long as they are not "activated, used, displayed or visible during the instructional day or as otherwise directed by school rules or school personnel" and noting that "[t]eachers and administrators may authorize students to use the

While not explicitly articulated by school districts, the justification for these confiscation provisions is likely the evidence that students frequently use their phones in school without authorization,[140] and that this use distracts students from learning[141] and instructors from teaching.[142]

A second way in which students may lose temporary—and sometimes permanent—possession of their cell phones in schools is that phones may be seized pursuant to a search warrant[143] as evidence of a crime or in

device for instructional purposes," and establishing as consequences that phones may immediately be confiscated if "on, used, displayed, or visible" and noting further that they "will be returned only to a student's parent," and establishing that the five factors to be considered in determining appropriate consequences are whether the phone was used to: "reproduce images of tests, obtain unauthorized access to school information or assist students in any aspect of the instructional program in a manner that violates any school board policy, administrative regulation or school rule; bully or harass other students; send illicit text messages; take and/or send illicit photographs; or in any other manner that would make more severe disciplinary consequences appropriate"). For a list of all North Carolina districts' technology confiscation provisions, see Resource Guide discussed *supra* note 1.

140. *See, e.g.*, Amanda Lenhart et al., *Teens and Mobile Phones*, PEW RES. CTR. (Apr. 20, 2010), http://www.pewinternet.org/2010/04/20/teens-and-mobile-phones/ [https://perma.cc/6W87-5RD8] (noting that seventy-five percent of twelve through seventeen-year-olds own cell phones and noting further that sixty-five percent of cell-owning teens attending schools that completely ban phones nonetheless bring them to school; sixty-four percent have texted in class; and twenty-five percent have made calls in class). The popularity of cell phones makes cell phone-regulation policies difficult for schools to enforce. *See, e.g.*, Paul Barnwell, *Do SmartPhones Have a Place in the Classroom*? THE ATLANTIC (Apr. 27, 2016), https://www.theatlantic.com/education/archive/2016/04/do-smartphones-have-a-place-in-the-classroom/480231/ [https://perma.cc/27XA-HCB8] (stating that "it's a constant struggle to keep kids engaged in lessons and off their phones" and noting that in 2015, New York City rescinded its cell phone ban for its public schools).

141. *See* Barnwell, *supra* note 140 (citing evidence that "[h]igh levels of smartphone use by teens often have a detrimental effect on achievement, because teen phone use is dominated by entertainment, not learning, applications"); *see also* Louis-Philippe Beland & Richard Murphy, *Ill Communication: Technology, Distraction & Student Performance*, 41 LAB. ECON. 61, 62 (2016) (finding that "following a ban on phone use, student test scores improve by 6.41 percent of a standard deviation" and that "[t]his effect is driven by the most disadvantaged and underachieving pupils"); Alissa J. Rubin & Elian Peltier, *France Bans Smartphones in Schools Through 9th Grade. Will it Help Students?*, N.Y. TIMES (Sept. 20, 2018), https://www.nytimes.com/2018/09/20/world/europe/france-smartphones-schools.html [https://perma.cc/9REQ-Q637 (dark archive)].

142. *See, e.g.*, *Cell Phones in the Classroom: Learning Tool or Distraction*, OXFORD LEARNING (Apr. 22, 2019), https://www.oxfordlearning.com/should-cell-phones-be-allowed-classrooms/ [https://perma.cc/PV5B-JQJS] (describing how student use of cell phones can cause disruptions when teachers need to tell students to turn them off).

143. *See* Tammy Grubb, *Durham High School Students' Cell Phones Seized After Sex Acts Reported at High School*, THE HERALD-SUN (Durham May 22, 2019), https://www.heraldmailmedia.com/news/nation/durham-n-c-students-phones-seized-after-sex-acts-reported/article_6604f4f1-3641-5c2a-a4ad-b9791df75e45.html [https://perma.cc/DA8K-KNXA] (describing police warrants for student cell phones after reports of students having sex in school, videotaping it, and posting video to various social media platforms).

conjunction with an in-school arrest by a SRO.[144] For example, if Manuel had become upset and disorderly when trailed by the SRO, so much so that he had disrupted a class or perhaps become physically resistant when the SRO confronted him, he might have been arrested and charged with disorderly conduct in a school.[145] In that case, all of Manuel's belongings, including his cell phone, conceivably could have been subject to seizure pursuant to the search-incident-to-arrest doctrine.[146] Were Manuel to lack a passcode or other encryption device on his phone, any incoming texts could be visible to school police. In addition, if the officer and administration wanted to investigate their suspicion that Manuel was involved with a gang, they could apply for a search warrant to review the contents of the cell phone;[147] they might also decide on their own that no warrant is required and simply commence searching.[148]

Once school administrators obtain students' phones, they potentially have access to a wealth of personal information about these students, particularly when the phone seized is a smartphone. These devices can indicate, at a minimum, whom students know, how often they contact them, and the content of their personal communications.[149] The unique features of cell phones and smartphones—the amount of information they store, the length of time they store it for, and the amount of information that each piece of data can reveal about a smartphone owner—were noted by the Supreme Court in *Riley v. California*.[150]

144. See *infra* Section I.B.2.c. for further discussion of school policing and its role in student surveillance.

145. *See, e.g.*, N.C. GEN. STAT. § 14-288.4(A)(6) (2017).

146. Riley v. California, 134 S. Ct. 2473, 2484–85 (2014) (discussing search-incident-to-arrest doctrine as being justified by arrestee's reduced expectation of privacy, officer safety, and need to prevent destruction of evidence).

147. *Id.* at 2485–88 (holding that the rationale for the search-incident-to-arrest doctrine does not apply to cell phone contents and holding further that search warrants are therefore required to search cell phones when they are seized pursuant to an arrest).

148. For an argument that the privacy-protecting rationale for cell phones may not apply to cell phones seized in school, see Bernard James, T.L.O. *and Cell Phones: Student Privacy and Smart Devices After* Riley v. California, 101 IOWA L. REV. 343, 354 (2015); *see also infra* Section II.D.

149. In *Riley*, the Court found that "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person." *Riley*, 134 S. Ct. at 2489. One major difference is the quantity of material that a modern cell phone can store, amounting to "millions of pages of text, thousands of pictures, or hundreds of videos." *Id.* The Court then pinpointed "several interrelated privacy consequences." *Id.* Of particular note, the Court found that the collection of distinct types of information located in just one place "reveal[s] much more in combination than any isolated record." *Id.* Additionally, the storage capacity "allows even just one type of information to convey far more than previously possible." *Id.* Lastly, the Court found the length of time of recorded data allowed for far more information to be gathered at one time. *Id.* Together, "there is an element of pervasiveness that characterizes cell phones but not physical records." *Id.* at 2490.

150. *Id.*

As with digital learning devices,[151] cell phone confiscation provisions—and, indeed, any mechanism through which school officials or school resource officers obtain students' cell phones—are not necessarily implemented and relied upon for the express purpose of conducting surveillance on students. They instead reflect and express other normative values, such as the need for students to learn without electronic distraction and the imperative for evidence gathering upon certain custodial arrests. Nonetheless, particularly when considered in combination with the technologies for watching and other policies for monitoring and control, these provisions can have the effect of further diminishing students' privacy and adding to the ways in which schools increasingly resemble Bentham's Panopticon.[152]

*c. Expansion of School Policing*

According to an estimate from the 2018 North Carolina School Research Officer Survey, approximately 1200 SROs are employed in the state, up from 1000 in 2015.[153] Along with an increase in the *number* of officers, their *role* has also expanded. Many schools have written memoranda of understanding between law enforcement agencies and school districts.[154] While some memoranda demand that SROs "avoid any school disciplinary work," others do the opposite, for example empowering SROs to "enforce the school district's student disciplinary process."[155] One report described an SRO who conceded that he was "play[ing] [school discipline] by ear" and who eventually assumed a role in writing school discipline reports on issues as minor as uniform violations.[156]

One thing that appears common among SROs regardless of the role they play in school discipline is that they are privy to significant amounts of student data. Notwithstanding recent developments at the federal and state level away from the practice of treating minors like adults for all

151. *See supra* Section I.B.1.a.

152. *See* Thomas McMullan, *What Does the Panopticon Mean in the Age of Digital Surveillance?*, GUARDIAN (July 23, 2015, 03:00 EDT) https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham [https://perma.cc/G68Z-7QQA].

153. N.C. DEP'T OF PUB. INSTRUCTION, 2018 NORTH CAROLINA SCHOOL RESOURCE OFFICER SURVEY 3 (2018); N.C. DEP'T OF PUB. SAFETY, 2015 NORTH CAROLINA SCHOOL RESOURCE OFFICER CENSUS 3 (2015).

154. *See* N.C. DEP'T OF PUB. SAFETY, *supra* note 153, at 4 (describing more than three quarters of SROs who are aware of memoranda of understanding between the law enforcement department and the school).

155. Josh Gupta-Kagan, *Reevaluating School Searches Following School-to-Prison Pipeline Reforms*, 87 FORDHAM L. REV. 2013, 2040 (2019).

156. *See id.*

aspects of criminal prosecution,[157] law enforcement does not observe distinctions between adults and minors in terms of the information officers collect from individuals whom they encounter.[158]

The digital revolution has affected policing as much as it has altered education, and it has dramatically increased the ability of law enforcement to collect, store, retrieve, and share data.[159] The number of public and private entities that eventually can access law enforcement data has also expanded dramatically.[160] Recently enacted laws in other states have explicitly authorized the sharing of student data among schools, social services agencies, social media companies, and law enforcement.[161] In North Carolina, at least one school district warns students that it will share

157. *See* Miller v. Alabama, 132 S. Ct. 2455, 2460 (2012) (holding that mandatory life-without-parole sentences for juveniles violate the Eighth Amendment); J.D.B. v. North Carolina, 564 U.S. 261, 280–81 (2011) (holding that law enforcement must consider age when deciding whether an individual is in custody for purposes of providing a Miranda warning); Graham v. Florida, 560 U.S. 48, 81 (2010) (outlawing life-without-parole sentences for individuals who committed non-homicide crimes under the age of eighteen); Roper v. Simmons, 543 U.S. 551, 577 (2005) (declaring unconstitutional the imposition of capital punishment for crimes committed when the offender was under the age of eighteen); *see also* LaToya Powell, *"Raise the Age" is Now the Law in North Carolina*, N.C. CRIM. L. (Aug. 31, 2007, 7:46 AM), https://nccriminallaw.sog.unc.edu/raise-age-now-law-north-carolina/ [https://perma.cc/6R9Z-LZ9B] (describing the fact that, as of December 1, 2019, most sixteen- and seventeen-year-olds in North Carolina will now have their cases heard in delinquency rather than adult district court, in a change to historical practice that means that North Carolina is now no longer the only state to cap juvenile court jurisdiction at the age of sixteen).

158. *See* Kevin Lapp, *Databasing Delinquency*, 67 HASTINGS L. J. 195, 208 (2015).

159. *See id.* ("Computer technology has enabled networked storage, powerful search capacity, real time updating, and near instantaneous retrieval by officers in the station house and the field . . . . All told, the criminal justice system collects a remarkable amount of information about youth: contacts with police, suspicions, misbehavior, arrests, charges, convictions, and sentences. But it is not just criminal information that is being collected, stored, and shared. Law enforcement collects genetic samples from juveniles; it catalogs their friends, family, associations, and movements; and the law requires that personal information of youth convicted or adjudicated delinquent of sex offenses, such as their home address and school, be posted on the Internet."). Eisha Jain has documented how police data is often incomplete and inaccurate. Eisha Jain, *Capitalizing on Criminal Justice*, 67 DUKE L.J. 1381, 1418 (2018) ("The FBI adds between 10,000 and 12,000 new names to its criminal record database every day. There are approximately 80 million individuals in the database altogether. Despite being easy to access, these records consist of notoriously bad data. Criminal records repositories are rife with inaccuracies and mistaken identity information, as well as old, expunged, and dismissed arrest records. Nearly 50 percent of the records in the FBI database are incomplete.").

160. *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 11 (2009). Nissenbaum divides the concerns over new technologies into three categories: (1) monitoring and tracking, (2) dissemination and publication, and (3) aggregation and analysis. *Id.*

161. *See* Benjamin Herold, *To Stop School Shootings, Fla. Will Merge Government Data, Social Media Posts*, EDUC. WEEK (July 26, 2018), https://www.edweek.org/ew/articles/2018/07/26/to-stop-school-shootings-fla-will-merge.html [https://perma.cc/872A-KZDU].

student data with third-party private and public entities.[162] Privacy advocates critique the conscription of private surveillance technologies by the police, decrying what they describe as the "if you build it, they will come principle—anytime a technology company creates a system that could be used in surveillance, law enforcement inevitably comes knocking."[163] At present, SROs can likely access each of the various surveillance technologies and obtain information from the anonymous tip line as well, simply by asking for it.[164]

The 2018 North Carolina state budget allocated $5 million in additional funding for SROs in elementary and middle schools, providing for the hiring of officers to supplement the thousands already working in the state's K-12 schools.[165] Nationally, school-based policing is "the fastest growing area of law enforcement";[166] North Carolina reflects this trend.[167]

162. *See Policy Code 630: Acceptable Use for Internet and Computer Resources*, CASWELL CTY. SCHS. BOARD EDUC. POL'Y, http://images.pcmac.org/Uploads/CaswellCounty/CaswellCounty/Divisions/DocumentsCategories/Documents/ACCEPTABLE%20USE%20Revised%20June%202012.pdf [https://perma.cc/LPM5-WCUZ] (detailing the Caswell County School District's policy, which states that it "reserves the right to disclose any user's electronic communications or data to Caswell County School System or non-Caswell County School System's personnel or agencies to the extent permitted or required by law, including disclosure to public safety and social service officials or other legitimate third parties").

163. Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. TIMES (Apr. 13, 2019), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html [https://perma.cc/Q8PN-YSHV (dark archive)] (describing the "geofence" warrants law enforcement sends to Google and other tech companies that specify an area and time period and require the tech company to supply any information on all devices recorded in that area).

164. See *infra* Section II.D, for a discussion of whether and how existing judicial precedent offers any meaningful restraint on school police officers seeking to access student information.

165. Current Operations Appropriations Act of 2018, ch. 5, § 7.27(e), 2018-2 N.C. Adv. Legis. Serv. 1, 36 (LexisNexis) (allocating a total of $12 million for School Resource Officer grant program).

166. *About NASRO*, NAT'L ASS'N SCH. RES. OFFICERS, https://nasro.org/about/ [https://perma.cc/KY84-L52D]. In 1975, only one percent of school principals reported the presence of on-site police officers, but between 1999 and 2008, the U.S. Department of Justice Office of Community Oriented Policing Services ("COPS") granted over $750 million to local police departments for hiring and training more than 6500 new SROs. *See* Amanda Merkwae, *Schooling the Police: Race, Disability, and the Conduct of School Resource Officers*, 21 MICH. J. RACE & L. 147, 158–59 (2015). After the shooting at Sandy Hook Elementary School, COPS announced plans to create nearly 1000 more positions including more than 350 school resource officer positions. *See* Press Release, Eric H. Holder, Jr., Attorney Gen., Office of the Attorney General, Attorney General Eric Holder Delivers Remarks at the International Association of Chiefs of Police Annual Conference (Oct. 21, 2013), https://www.justice.gov/opa/speech/attorney-general-eric-holder-delivers-remarks-international-association-chiefs-police [https://perma.cc/9ZAJ-KZVD].

167. *See* N.C. DEP'T OF JUVENILE JUST. & DELINQUENCY PREVENTION, ANNUAL SCHOOL RESOURCE OFFICER CENSUS 2 (2008) (showing that North Carolina has followed the trend of increasing use of SROs).

## II. NOT SO FAST: IDENTIFYING COMPETING CONSIDERATIONS

Because schools are legally liable for the well-being of their students,[168] one might assume that districts have implemented surveillance[169] technologies and policies pursuant to a deliberative process in which policymakers have carefully balanced benefits against harms. Such a process ought to include the following: assessment of the efficacy of the various tools and techniques; exploration of countervailing student privacy interests; consideration of whether and how surveillance disproportionately affects marginalized students; and evaluation of whether federal or state statutes, or judicial precedent, bar or restrict the implementation of certain surveillance technologies and policies.

As the following sections will demonstrate, however, there is scant evidence that school districts have considered these issues as they have engaged in surveillance policymaking. Rather, schools have moved with undue haste to adopt ever-more sophisticated technologies and to create comprehensive monitoring policies.

### *A. Thin Evidence Base and Unintended Harms*

The creation and implementation of technologies for watching[170] and policies for monitoring and control[171] are premised on the notion that they achieve their intended purposes: improved learning outcomes and student safety. The safety imperative seems, as evidenced by state and federal legislative priorities,[172] to be particularly pronounced.[173] However, for many

168. *See* Davis v. Monroe Cty. Bd. of Educ., 526 U.S. 629, 644 (1999).

169. *See* Richards, *supra* note 24, at 1937 (defining surveillance as involving observation and monitoring).

170. *See supra* Section I.B.1.

171. *See supra* Section I.B.2.

172. *See* Current Operations Appropriations Act of 2018, ch. 5, § 7.27(g), 2018-2 N.C. Adv. Legis. Serv. 1, 36 (LexisNexis) (allocating $3 million in school-safety training for school personnel to help students in the event of a traumatic event and establishing an anonymous tip line); *see also id.* § 7.27(f) (noting $2 million to create "Grants for Students in Crisis," including the creation of crisis respite services for parents, "training and expanded services for therapeutic foster care families and licensed child placement agencies that provide services to students who need support to manage their mental health or have cognitive or behavioral problems, developmental delays, or aggressive behavior," and "any other crisis service, including peer-to-peer mentoring, that is likely to increase school safety"). While it did not pass any legislation addressing firearm access, the North Carolina General Assembly's House Select Committee on School Safety urged the enactment of legislation requiring that students receive first-aid instruction "on the immediate response to bleeding, how to recognize life threatening bleeding, and appropriate ways to stop the bleeding." FINAL REPORT OF THE H. COMM. ON SCH. SAFETY, H. 2018 Sess., at 13 (N.C. 2018).

173. HEATHER L. SCHWARTZ ET. AL., CAN TECHNOLOGY MAKE SCHOOLS SAFER? 2 (2016) (noting that "[m]any [schools] have turned to technology . . . [as a way] to prevent, intervene in, respond to, and protect schools from . . . violent acts and risk to students' safety").

of these technologies, the evidence of efficacy is scant; others have not been tested at all.[174] What is more, the technologies and policies can lead to problematic and unintended consequences that policymakers may not have fully considered.

Consider, first, digital learning technologies generally. The embrace of big data in the classroom has occurred largely without a thorough vetting of the various products.[175] Notwithstanding enthusiasm of many educators, there is a dearth of research supporting claims that educational technology in fact improves learning outcomes for all students.[176] Particularly given countervailing privacy interests implicated by digital learning,[177] this absence of a research base is troubling as it leaves policymakers without the ability to weigh digital learning's benefits against its harms.[178]

Consider, second, safety management platforms and social media scanning. Much of what is known about their efficacy comes from the creators of the products rather than from independent research.[179] Representatives from the student monitoring software programs tout their products' effectiveness at preventing harm. Gaggle, for example, includes on its website multiple accounts of school administrators, often

174. Stefanie Dazio, *Schools Turn to Apps, Other Tech to Guard Against Shootings*, ASSOCIATED PRESS (May 16, 2019), https://www.apnews.com/867814eff37a40b8b1c4f8e67486b2d8 [https://perma.cc/L453-YQY9] (quoting Dennis Kenney, a professor at the John Jay College of Criminal Justice, saying "[w]e've kind of reached this state of frustration where we (feel like we) can't protect our students . . . . What we're trying to do is find some technological fix, and there isn't one").

175. Zeide, *Limits Of Education*, *supra* note 40, at 516 (arguing that "[t]here are few research studies showing that new technologies will provide better outcomes for students, schools, or the education system overall" and that "[m]any new data-driven education technologies have not been thoroughly vetted").

176. *See* Matt Barnum, *As Ed Reformers Urge a 'Big Bet' on Personalized Learning, Research Points to Potential Rewards—and Risks*, CHALKBEAT (May 22, 2017), https://www.chalkbeat.org/posts/us/2017/05/22/as-ed-reformers-urge-a-big-bet-on-personalized-learning-research-points-to-potential-rewards-and-risks/ [https://perma.cc/G3AJ-P73Z] (cautioning that the evidence base for personalized learning technology is in its infancy and warning against a wholehearted embrace of digital learning without fully understanding its benefits and costs).

177. *See infra* Section II.B.

178. *See infra* Part III (discussing how to engage in more appropriate, evidence-based policymaking around surveillance).

179. Heather L. Schwartz et al., *The Role of Technology in Improving K–12 School Safety*, RAND CORP. (2016), https://www.rand.org/pubs/research_reports/RR1488.html [https://perma.cc/45CT-2EKA] (noting that "rigorous research about the effectiveness of these technologies is virtually non-existent" and noting studies that state "it is important to keep in mind the limitations of the methods we employed. The most important is that we do not present causal evidence about whether specific school technologies reduce violence; this evidence is lacking from the research literature at large and an efficacy study of any one or more technologies was not within our scope" (citations omitted)).

accompanied by police, responding to students believed to be at risk.[180] The company then concludes that its intervention prevented imminent harm.

Yet these "success stories" do not consider competing accounts from other involved parties, nor do they contemplate the possibility that a Gaggle intervention led to negative long-term outcomes. For example, in one description of an incident involving interception of a student suicide plan, Gaggle asserted that "[t]he student now realizes the importance of being cautious [with] how you express yourself in an email."[181] One wonders, however, how much this student has been prevented from thoughts of self-harm as opposed to being deterred from ever again expressing her feelings about it in writing.[182] If a student has other avenues to express her pain, she may get the help she needs; if, however, this particular means of communication was her only one, she may turn her negative feelings inward, internalizing the lesson that reaching out may yield only a police visit.[183] What is more, the stigma and fear that a police visit may cause students is not discussed.[184]

180. *See, e.g.*, *Round Rock Independent School District: How Gaggle Supports David's Law and Keeps Students Safe*, GAGGLE, https://www.gaggle.net/success-stories/round-rock-independent-school-district [https://perma.cc/69AS-FAWJ] (discussing safety team that monitors student communication and recounting one incident of dispatching a team of police officers and others to the home of a student who had written about a plan to commit suicide); *Wassau School District: The Priceless Value of a Student's Life*, GAGGLE, https://www.gaggle.net/success-stories/wausau-school-district [https://perma.cc/M8BX-TWXG] (noting that "[o]n a few occasions, thanks to Gaggle notifications, the district has asked local police to do wellness checks at students' homes").

181. *Warsaw Community Schools: How Much is Student Safety Worth? Responding to Cries for Help*, GAGGLE, https://www.gaggle.net/success-stories/warsaw-community-schools [https://perma.cc/7NDB-VM6T] (discussing sending school resource officer and local police officer to home of a student who had made a self-harm threat over Gmail).

182. Stolzoff, *supra* note 75 (quoting Daphne Keller, Director of the Stanford Center for Internet and Society, critiquing these products for this reason: "Suppose you are a kid considering suicide and you want to write a diary about it or talk to your friend about the feelings that you're having, but you don't because you're afraid you'll be turned into [sic] your parent . . . I'm not sure that's a good outcome"); *see Student Safety that Saves Lives*, GAGGLE, https://www.gaggle.net/success-stories/edison-township-public-schools/ [https://perma.cc/7SLY-2U35] (describing superintendent in a district who received a late-night phone call one weekend about a student reportedly trying to hurt herself and who noted "[m]any of our students express themselves through writing"); *Wassau School District*, *supra* note 180 (describing how Gaggle's Safety Management Program allowed administrators to prevent an attempted suicide).

183. *See, e.g.*, Alice E. Marwick & danah boyd, *Networked Privacy: How Teenagers Negotiate Context in Social Media*, 16 NEW MEDIA & SOC'Y, 1051, 1061 (2014) (explaining that "teenagers create trust by revealing information" when "they are confident that it cannot hurt them").

184. *See, e.g.*, *Student Safety Doesn't Take the Summer Off*, GAGGLE, https://www.gaggle.net/success-stories/wisconsin-rapids-public-schools/ [https://perma.cc/M5GF-Q2JS] (describing team with "diverse backgrounds in education, law enforcement and other fields," that responded to a student, helped avert a crisis, but not describing any plans for subsequent investigation or assistance). *But see How Much is Student Safety Worth? Responding*

Because Gaggle does not reveal or presumably even study the long-term impacts of their interventions, it is unclear whether the potentially deterrent effect on free expression is outweighed by the platform's purported salutary features.

Other elements related to the efficacy of safety management platforms deserve, but may not receive, close investigation by education policymakers. For example, while detection and prevention of potential student self-harm are critical functions, Gaggle may not be the best way to achieve them. Much of the administration of Gaggle and similar tools is left to school Information Technology Specialists, who have neither the training nor institutional capacity to know how to evaluate and respond to students who present with mental health problems.[185] What is more, there is a troubling lack of transparency with students and families regarding what words trigger a Gaggle alert as well as how discretion is deployed regarding when to send an officer to a student's home. The design of Gaggle—and the lack of transparency regarding how it is implemented—makes the tool vulnerable to its being used for purposes other than ensuring student safety, thus potentially diminishing its efficacy overall.[186]

Third, the ubiquity of surveillance cameras might suggest that they are effective at deterring violence, crime, and lesser infractions, in addition to investigating their occurrence. One concern regarding studies that do appear to show a positive relationship between the presence of cameras and a reduction in crime, however, is that they fail to rule out the possibility of a displacement effect; that is, technology may simply move misbehavior to locations just outside the range of cameras.[187] While this concern may not seem as persuasive given, in this setting, surveillance cameras are increasingly stationed throughout most areas of a school, it is nonetheless

*to Cries for Help*, GAGGLE, https://www.gaggle.net/success-stories/warsaw-community-schools/ [https://perma.cc/LT9B-WRLY] (noting a school resource officer going to a student's home after a report of self-harm and stating that the family expressed gratitude).

185. Anya Kamenetz, *Schools Turn to Software for Suicide Prevention—But Not Everyone's On Board*, NPR (Mar. 28, 2016, 4:00 PM), https://www.npr.org/2016/03/28/472176259/schools-turn-to-software-for-suicide-prevention-but-not-everyones-on-board [https://perma.cc/TMB8-EVGX].

186. Stolzoff, *supra* note 75 (noting that one Gaggle post, since deleted, suggests that the tool could have been used to squelch teacher organizing: "'[t]hink about the recent teacher work stoppage in West Virginia,' a recent blog post reads. 'Could the story have been different if school leaders there requested search results for "health insurance" or "strike" months earlier? Occasional searches for "salary" or "layoffs" could stave off staff concerns that lead to adverse press for your school district'" (internal citation omitted)); *cf. infra* note 191 and accompanying text (explaining the diminished efficacy of tip lines due to improper use).

187. Stolzoff, *supra* note 75.

the case that other studies of the efficacy of cameras as a deterrent have yielded mixed and inconclusive results.[188]

Fourth, the evidence base for anonymous tip lines is scant at best. While the tip lines have great political appeal,[189] whether or not these tip lines will work depends on non-technological factors such as the availability of staff to both train students in how to use them and to monitor and appropriately respond to tips.[190] In the absence of such training, it will be possible that the tip lines could become repositories for student gossip or vendettas. Indeed, in Colorado, which was one of the first states to create a tip line, lawmakers documented instances of students using the tool to make false reports of suicide attempts and drug use.[191] However, other than the broad requirement that the tip line function to "receive anonymous information on internal or external risks to the school population, school buildings, and school-related activities," the enabling statutory language in North Carolina gives no guidance about the content or scope of the information that is to be collected, or whether and how students and staff will be trained in using it.[192]

Tip line efficacy ultimately depends on adults sifting through the information and responding in ways that inspire students to trust that providing this information was the right thing to do; in other words, the technology works only if a school climate of trust already exists.[193] As social scientists researching the efficacy of the tip lines explain,

188. Warnick, *supra* note 113, at 319–20.

189. *See supra* Section I.B.2.a.

190. *See infra* notes 191–94 and accompanying text.

191. Shaun Boyd, *Lawmakers Work to Keep Safe2Tell A Place To Prevent Bullying, Not Promote It*, CBS DENVER (May 3, 2018), https://denver.cbslocal.com/2018/05/03/safe-2-tell-state-capitol-school-bully/ [https://perma.cc/6ZTP-98EQ]; *see also* Blad, *supra* note 128 (noting incidents of students using the tip line to "prank" other students, including falsely reporting suicide threats).

192. N.C. GEN. STAT. § 115C-105.51 (2017). *See generally* Katherine W. Joyce, *2018 Laws Affecting School Safety in North Carolina*, N.C. ASS'N SCH. ADMINS., https://www.ncasa.net/cms/lib/NC02219226/Centricity/Domain/59/2018%20Laws%20Affecting%20School%20Safety%20in%20NC.pdf [https://perma.cc/F7LA-V8AY] (surveying laws passed to address school safety, discussing tip line, and not including any information about funding for training for staff and students about how to use the tip line).

193. *See generally* Schwartz et al., *supra* note 179 (discussing successes and challenges of rolling out programs in communities across the United States). Some districts seem to recognize the need for non-technological resources to supplement tip line technology. *See* Sophie Quinton, *To Prevent Suicides and School Shootings, More States Embrace Anonymous Tip Lines*, PEW CHARITABLE TR. (Mar. 16, 2018), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2018/03/16/to-prevent-suicides-and-school-shootings-more-states-embrace-anonymous-tip-lines [https://perma.cc/U57Y-A3DM] (noting a Nevada district that hired social workers to deal with the many tips that were anticipated in the wake of the creation of the tip line).

"[t]echnology alone . . . is not the answer. School and youth engagement are critical to ensuring widespread technology adoption and use."[194]

Finally, also unanalyzed in the political and policymaking discourse around school safety is the efficacy of school resource officers. While ongoing funding seems all but assured given the spike in gun violence in 2018,[195] studies are inconclusive about whether SROs in fact make schools safer.[196] Additional research undercuts the safety claims of SRO proponents: some research indicates that a visible uniformed police presence may actually make some students—chiefly Black students and students who previously have been victimized—feel *less* safe in school.[197] And feeling safe is important to other school administration goals such as school connectedness, which is a deterrent to misconduct and violence in school[198] and is helpful in promoting positive educational outcomes.[199]

### *B. Undervaluing Student Privacy Interests*

Clearly, some question exists as to whether student surveillance technologies and policies are effective at improving safety and learning outcomes. However, the absence of a conclusive evidence base might not necessarily mean, by itself, that schools should abandon surveillance. After all, an evidence base that is thin is not the same as definitive proof of *in*effectiveness. If any of these technologies and policies, either alone or in combination, prevents even one school shooting (or minimizes its damage),

194. Hsing-Fang Hsieh et al., *Evaluating the Effectiveness of the Say Something Anonymous Reporting System to Improve School Safety*, POPULATION STUD. CTR.: INST. FOR SOC. RES., https://www.psc.isr.umich.edu/research/project-detail/37452 [https://perma.cc/J3YA-4GR6] (describing multi-year study of anonymous tip lines).

195. While 2018 was the deadliest year on record for school shootings, *see* German Lopez, *2018 Was by Far the Worst Year on Record for Gun Violence in Schools*, VOX (Dec. 10, 2018), https://www.vox.com/2018/12/10/18134232/gun-violence-schools-mass-shootings [https://perma.cc/XC6J-7A29] (surveying data from a national comprehensive database and concluding that the number of school gun violence incidents in 2018 was the highest on record), the fact remains that schools are overwhelmingly safe places for youth; school shootings are in fact rare. *See* Scott, *supra* note 84, at 541; *see also* Theriot, *supra* note 85, at 280.

196. *See* Theriot, *supra* note 85, at 280; *see also* Edward W. Hill, The Cost of Arming Schools: The Price of Stopping a Bad Guy with a Gun 3, 8 (Mar. 28, 2013) (unpublished manuscript) (on file with the North Carolina Law Review) (arguing that SROs cost more than the benefits that they provide and noting that paying for one armed SRO in each school in America would cost between $9.9 billion and $12.8 billion and questioning whether the funding spent on police security could be better spent on enhancing student academic performance).

197. Matthew T. Theriot & John G. Orme, *School Resource Officers and Students' Feelings of Safety at School*, 14 YOUTH VIOLENCE & JUV. JUST. 130, 130 (2014).

198. *Id.* at 133.

199. Robert W. Blum, *A Case for School Connectedness*, EDUC. LEADERSHIP, Apr. 2005, at 16 (surveying the research and concluding that school connectedness "increases the likelihood of academic success").

prevents student self-harm, or lessens the occurrence of other forms of violence, then doesn't the emerging surveillance regime justify itself?

This Article does not argue that surveillance is always without benefit, or that it should never be pursued.[200] It argues, instead, that education policymakers too often undervalue student privacy interests, fail to consider surveillance's often inequitable and unfair application,[201] and may be unaware of the legal constraints to surveillance.[202] This section takes up student privacy.

Julie Cohen articulates both the descriptive and normative dimensions of privacy, explaining that "[i]t is both a structural condition and a related entitlement."[203] Her assertion that "[t]o say that individuals (or communities) have—or should have—rights to privacy is to make a normative statement about the importance of preserving the breathing room necessary for self-articulation"[204] has special salience when considering the nature and importance of student privacy.

Privacy scholars identify discrete categories of privacy interests: at a minimum, "physical" privacy, which is violated when a person's legitimate efforts to conceal herself are frustrated; "informational" privacy, which is contravened when identity information a person wants to protect is nonetheless acquired; and "decisional" privacy, which is violated when an individual's ability to make choices about personal and intimate matters is abrogated.[205] Generally speaking, these rights are conceptualized as liberty rights.[206]

Courts and legislatures do not typically recognize minors as possessing liberty rights to the same degree as adults because minors lack—or are thought to lack—the cognitive and emotional capacity to engage in the necessary deliberation to make informed choices.[207] Instead,

200. *See infra* Part III (discussing principles to guide student surveillance policymaking).

201. *See infra* Section II.C.

202. *See infra* Section II.D.

203. Cohen, *Surveillance Versus Privacy*, *supra* note 6, at 458.

204. *Id.*

205. *See* ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 3 (2011); *see also* William Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960) (outlining the four key personal privacy rights: the right to seclusion, the right to control the use of one's name and likeness, the right to control publication of certain personal facts, and the right not to be depicted in false light).

206. *See, e.g.*, Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 125 (2004) ("Privacy is thus protected by reference to general, well-defined, and generally accepted political principles addressing the balance of power, which, among other things, set limits on government intrusiveness into the lives and liberty of individuals.").

207. *See, e.g.*, Roper v. Simmons, 543 U.S. 551, 569 (2005) (finding "[a] lack of maturity and an underdeveloped sense of responsibility are found in youth more often than in adults and are more understandable among the young" and that "[t]hese qualities often result in impetuous and ill-considered actions and decisions" before ruling for this reason, among others, that the juvenile

minors possess welfare[208] and dependency[209] rights—to be protected from child abuse or neglect, to be kept out of the formal labor market, and to be immunized against legal consequences that would attach if they were permitted to execute legally enforceable contracts, for example.[210] Parents and guardians of children are presumed—and given the legal authority[211]—to make decisions about their children's health and education based on a socially shared understanding that parents and guardians act in their children's best interests.[212] Schools are given the authority to act *in loco parentis* when students are in their care.[213] It seems to make little sense, then, to think of children as possessing privacy rights if those rights are understood only as liberty rights.

It *is* possible, however, to conceptualize the right to privacy as a welfare[214] or developmental[215] right and to extend it in age-appropriate ways to children. Consider the example of unwanted exposure of a child's body. As philosophy of education professor Bryan Warnick argues, such exposure "can cause serious psychological, financial, or even physical

death penalty violated the Eight Amendment's prohibition on cruel and unusual punishment because minors categorically lack the kind of criminal culpability that can justify the death penalty); Larry Cunningham, *A Question of Capacity: Towards a Comprehensive and Consistent Vision of Children and Their Status Under Law*, 10 U.C. DAVIS J. JUV. L. & POL'Y 275, 320 (2006) (noting that minors are deemed not to have the capacity to make a valid will or to otherwise make a testamentary designation).

208. Anne C. Dailey, *Children's Constitutional Rights*, 95 MINN. L. REV. 2099, 2135 n.164 (2011) (surveying field of scholarship conceptualizing children's rights as welfare rights).

209. Joel Feinberg, *The Child's Right to an Open Future*, *in* WHOSE CHILD? CHILDREN'S RIGHTS, PARENTAL AUTHORITY, AND STATE POWER 124 (William Aiken & Hugh LaFollette eds., 1980) (delineating "dependency rights" of children including right to be fed, nourished, and protected).

210. *See, e.g.*, Martha Minow, *Whatever Happened to Children's Rights*?, 80 MINN. L. REV. 267, 279–80 (1995) (describing Progressive Era initiatives to address child welfare including laws requiring school attendance and those restricting child labor).

211. *In re* Gault, 387 U.S. 1, 16 (1967) (describing that the state has power *parens patriae*, derived from chancery practice, to act *in loco parentis* to protect the property interests and person of the child).

212. *See* Parham v. J.R., 442 U.S. 584, 602 (1979) ("The law's concept of the family rests on a presumption that parents possess what a child lacks in maturity, experience, and capacity for judgment required for making life's difficult decisions."). *But see* Barbara Bennett Woodhouse, *"Who Owns the Child?":* Meyer *and* Pierce *and the Child as Property*, 33 WM. & MARY L. REV. 995, 1051–52 (1992) (describing how children's rights often conflict with parental rights).

213. *See, e.g.*, Garcia v. City of New York, 646 N.Y.S.2d 508, 510–511 (N.Y. App. Div. 1996) (providing an example of a situation where a school, acting *in loco parentis*, did not act with ordinary prudence in the supervision of a five-year-old). For a short discussion of this common-law doctrine, see *supra* note 10.

214. *See generally* Warnick, *supra* note 113, at 321–22 (describing how the right to privacy can be explained as a welfare right).

215. *See generally* Dailey, *supra* note 208, at 2103–06 (introducing the concept of developmental rights pertaining to a child's right to privacy).

harm."[216] Being able to control who sees oneself is important for a child's healthy development, and protecting children from unwanted self-exposure can help facilitate that development. Institutions can and do take steps to reinforce the notion that one can and should keep certain aspects of oneself private—stores include fitting rooms for trying on clothes, for example, reflecting and reinforcing the social norm that one should not have to sacrifice one's ability to remain clothed in public for the sake of making a purchase. In other words, privacy—even for young children—deserves and receives some social protection as a means of promoting their welfare.

The concept of developmental rights is related to the idea of children as having future rights, or "rights-in-trust."[217] Philosophers explain that rights conceptualized this way mean that children's "capacities are to be developed to their best advantage."[218] The notion of a future right is that children should be able "to have . . . future options kept open until [they are] fully formed self-determining adult[s] capable of deciding among them."[219]

When theorists speak of children as possessing future rights, they typically focus on the skills they need to develop into autonomous adults.[220] One important such skill is critical thinking.[221] Schools need to teach critical thinking, an important component of which involves the negotiation of whether and how much to argue with peers and teachers, as well as the consideration of when and how to dissent from conventional wisdom.[222] As students grow and mature, they need to engage in the processes of "boundary management" that enable and constitute self-development.[223] In other words, they need some degree of privacy, and they need to *practice privacy*—that is, to cultivate the abilities they need to one day exercise autonomy.[224] As Julie Cohen argues, "So understood, privacy is fundamentally dynamic."[225] She asserts that "[i]n a world characterized by

216. *See* Warnick, *supra* note 113, at 322.

217. *See* Dailey, *supra* note 208, at 2144 (internal quotation marks omitted) (quoting Feinberg, *supra* note 209, at 125–26).

218. *Id.* at 2144 (internal quotation marks omitted) (quoting John Eekelaar, *The Emergence of Children's Rights*, 6 OXFORD J. LEGAL STUD. 161, 170 (1986)).

219. *Id.* (internal quotation marks omitted) (quoting Feinberg, *supra* note 209, at 125–26).

220. *See id.* at 2145 ("[T]he most common meaning of autonomy in the cases and literature on children's rights is the capacity for rational choice.").

221. *Id.* ("[C]hildren's rights theorists emphasize critical thinking as the core component of the autonomy skills children must learn.").

222. *See generally id.* at 2119 ("[T]he Supreme Court has sought to balance the school's role in providing a marketplace of ideas against the school's mission to discipline students in the art of civil discourse.").

223. *See* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1906 (2013) [hereinafter Cohen, *What Privacy Is For*].

224. *See id.*; Warnick, *supra* note 113, at 323–24.

225. Cohen, *What Privacy Is For*, *supra* note 223, at 1906.

pervasive social shaping of subjectivity, privacy fosters (partial) self-determination."[226] Cohen's conception of privacy is that "[i]t enables individuals both to maintain relational ties and to develop critical perspectives on the world around them."[227]

Once we understand privacy as a child's welfare or developmental right, rather than only a negative right against governmental intrusion, it is easier to see how that right is worth protecting against the emerging student surveillance regime. Child development scholars argue that surveillance "does not allow students to practice acting and reasoning independently"[228] and thus keeps them from developing the skills and habits of mind they will need to one day exercise the liberty rights we afford adults. What is more, as a new generation of learners becomes acculturated to and accepting of surveillance, children may be more likely to become adults who do not value their own privacy—or that of others.[229]

Research demonstrates the damaging effect of surveillance on children's ability to develop in healthy ways.[230] Pervasive surveillance can create a climate in which adults are seen as overestimating and overreacting to risk.[231] Children, in turn, cannot develop the ability to evaluate and manage risk themselves in order to function effectively.[232]

Social science also suggests that children experience surveillance "as a form of control that limits their choices and inhibits their ability to act autonomously."[233] Surveillance shapes behavior through the threat of punishment for bad actions, which troublingly means that children may make decisions based on the potential for negative consequences instead of as an expression of their own values and beliefs.[234] This in turn can

226. *Id.*

227. *Id.*

228. Warnick, *supra* note 113, at 325.

229. *See* Josephine Wolff, Opinion, *Losing Our Fourth Amendment Data Protection*, N.Y. TIMES (Apr. 28, 2019), https://www.nytimes.com/2019/04/28/opinion/fourth-amendment-privacy.html [https://perma.cc/CB6W-FM2H (dark archive)] (warning that the "reasonable expectation of privacy" doctrine is problematic in a digital age in which people voluntarily relinquish personal information to third parties because "as soon as we begin expecting companies to collect lots of data about us, we stand to lose our Fourth Amendment protections for that data").

230. OFFICE OF THE PRIVACY COMM'R OF CAN., SURVEILLANCE TECHNOLOGIES AND CHILDREN 9 (Oct. 2012), https://www.priv.gc.ca/media/1751/opc_201210_e.pdf [https://perma.cc/C3BY-TJVX].

231. *Id.* at 6.

232. *Id.*

233. *Id.* at 7.

234. *Id.*

diminish children's ability to "self-regulate,"[235] to navigate personal boundaries, and to learn to assess risk and reward on their own.[236]

When students are aware of school surveillance, it may have the effect of inducing passivity or self-censorship.[237] When they believe that their every move is watched and every written word read, they are less likely to develop into people who believe that they can and do own and control their thoughts and actions.[238] A surveillance environment built by trusted teachers and administrators will socialize children to ignore and even accept the routine collection and retention of their personal information—to say nothing of its eventual sale to data brokers.[239] Allowing that acceptance to be normalized heightens the growing disparity in power between data users (companies) and data suppliers (students).[240]

With alarm, privacy scholars and advocates note that efforts to pass legislation and create policy to protect privacy will be futile if people continue to willingly give away the most intimate information about their lives.[241] This abdication of one's right to an intimate and private sphere is something that schools should work against. In a world in which people's privacy rights are increasingly undermined,[242] schools can either choose to follow that trend or to proactively teach students the value of privacy—that they deserve to have it, and that they must respect the privacy rights of each other.[243] Because privacy is critical to the free thought and value formation

235. *Id.*

236. Cohen, *Surveillance Versus Privacy*, *supra* note 6, at 459–60 ("Surveillance presses against the play of subjectivity and self-development in ways both metaphorical and literal.").

237. *Id.* at 460 ("The awareness of surveillance fosters a kind of passivity—a ceding of power over space."); *see also* Bruce Schneier, *Surveillance Kills Freedom by Killing Experimentation*, WIRED (Nov. 16, 2018, 9:00 AM), https://www.wired.com/story/mcsweeneys-excerpt-the-right-to-experiment/ [https://perma.cc/T2G3-VDT4].

238. *See* Warnick, *supra* note 113, at 325 ("While young people are under surveillance, they know that others are in charge and that they are not being respected as actors capable of choosing their own way.").

239. For a discussion of "omnibus information providers" that buy and sell information as their core business, see NISSENBAUM, *supra* note 160, at 45–50.

240. *See generally* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019) (raising concerns about the rise of "surveillance capitalism").

241. *See* Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 733–34 (1999); *see also* Wolff, *supra* note 229.

242. In 1999, Sun Microsystems' Chief Executive Officer, Scott McNealy, famously opined, "[y]ou have zero privacy anyway. Get over it." Polly Sprenger, *Sun on Privacy: 'Get Over It'*, WIRED (Jan. 26, 1999), https://www.wired.com/1999/01/sun-on-privacy-get-over-it/ [https://perma.cc/RB4M-GNLR].

243. *But see* Marwick & boyd, *supra* note 183, at 1052–53 (offering a sympathetic account of why teenagers both engage with technology and social media while simultaneously valuing their privacy so greatly).

that characterize participation in a liberal democracy,[244] schools have a role to play in teaching students an appreciation for it[245]—particularly since so many social forces are working toward privacy's diminution.

The filtering software required by federal statute[246] that is part of contemporary student surveillance regimes can sometimes function to keep students from obtaining important, age-appropriate reproductive health and sexual orientation/gender identity information that they need from their schools—especially if they cannot get it from their parents. Notwithstanding the legislatively and judicially presumed unity of interests between parent and child,[247] in practice, such unity does not always exist with respect to reproductive health and sexuality.[248] In these areas, courts and legislatures recognize that there may in fact be a disjunction.[249] Adolescents and teens do and should retain some degree of privacy in these areas that the law protects, even against their parents.[250] Yet student surveillance changes this equation.

In 2011, for example, the ACLU's national organization and regional chapters in several states issued letters demanding that public high schools remove web-filtering software that blocked items related to support groups for lesbian, gay, bisexual, and transgender youth.[251] The ACLU learned from students that web filters were routinely blocking access to groups such as Gay, Lesbian, and Straight Educators Network ("GLSEN")[252] and the Gay-Straight Alliance Network, along with LGBT anti-bullying and suicide prevention resources like "It Gets Better" and the "Annual Day of

244. Daniel Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 763 (2007) ("[P]rivacy has a social value.").

245. For a discussion of the relationship between public education and democracy, see, for example, Barbara Fedders, *Schooling at Risk*, 103 IOWA L. REV. 871, 879 (2018) ("The Supreme Court has recognized the centrality of education to American life, finding public schools to be, variously, 'a most vital civic institution for the preservation of a democratic system of government,' 'the most important function of state and local governments,' and to play 'a fundamental role in maintaining the fabric of our society.'" (citations omitted)).

246. *See supra* notes 66–69 and accompanying text.

247. *See supra* note 212 and accompanying text.

248. *See infra* notes 280–82 and accompanying text.

249. *See, e.g.*, *State Laws and Policies: Parental Involvement in Minors' Abortions*, GUTTMACHER INST. (Apr. 1, 2019), https://www.guttmacher.org/state-policy/explore/parental-involvement-minors-abortions [https://perma.cc/RJ6A-B9A8] (noting that certain jurisdictions allow minors to waive the parental involvement requirement for abortion procedures through a judicial bypass procedure after a showing of "clear and convincing evidence" that the minor is "sufficiently mature").

250. *See id.*

251. *See* AM. CIVIL LIBERTIES UNION, "DON'T FILTER ME:" FINAL REPORT 7–8, 16–18, https://www.aclu.org/sites/default/files/field_document/dont_filter_me-2012-1001-v04.pdf [https://perma.cc/T6N6-HURB].

252. *See Championing LGBTQ Issues in K-12 Education Since 1990*, GLSEN, https://www.glsen.org/ [https://perma.cc/98Y2-6GB2].

Silence."[253] In one Washington high school, a dean showed parents a video of their daughter kissing another girl; the parents, presumably upset by the same-sex nature of the kissing, withdrew their daughter from the school.[254] Sexuality scholars argue that the ability to control self-exposure enables the formation of queer communities and a safe form of intimacy.[255] School surveillance resulting in the private information about adolescent and teenage students being shared with a parent—in other words, "outing" a student to her parent—changes these dynamics of selective exposure, which is problematic and sometimes even dangerous when, for example, a parent is homophobic and such information could lead to verbal or physical abuse.[256]

A third and final way that student surveillance negatively affects students' privacy interests is that digital learning technologies capture—but may not protect—significant amounts of student data. Schools have always gathered, created, and maintained student data—health information, standardized test scores, grades, and behavioral records, just to name a few.[257] But today's digital learning devices have expanded the scope of the available data schools can gather and have made its collection infinitely easier.[258] Indeed, nationwide, "the volume of collected data is growing exponentially."[259]

When students use digital learning devices and technologies, it is not only their teachers who gain information about them. Multiple public and private entities can access student data, just as they can access other sorts of data.[260] Apart from the educational metadata and paradata available

253. *See* AM. CIVIL LIBERTIES UNION, *supra* note 251, at 7–8.

254. Neal Conan, *Security Cameras in School: Protective or Invasive?*, NPR (Sept. 4, 2012), https://www.npr.org/2012/09/04/160551340/security-cameras-in-school-protective-or-invasive [https://perma.cc/22J6-P7ER].

255. Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181, 197–98 (2008) [hereinafter Cohen, *Privacy, Visibility, Transparency*] (surveying literature).

256. *See generally* Barbara Fedders, *Coming Out for Kids: Recognizing, Respecting, and Representing LGBTQ Youth*, 6 NEV. L. J. 774, 788–89 (2006) (discussing how conflicts at home over sexual orientation can lead to negative outcomes for LGBTQ youth).

257. CTR. FOR DEMOCRACY & TECH., STATE STUDENT PRIVACY LAW COMPENDIUM 3 (2016), https://cdt.org/files/2016/10/CDT-Stu-Priv-Compendium-FNL.pdf [https://perma.cc/Q4ND-DGJ8].

258. *Student Privacy*, CTR. FOR DEMOCRACY & TECH., https://cdt.org/issue/privacy-data/student-privacy/ [https://perma.cc/WM66-792Q]; *see* Andrew D. Selbst, *Disparate Impact in Big Data Policing*, 52 GA. L. REV. 109, 109 (2018) ("No institution in society seems immune from the enthusiasm that automated decision-making generates.").

259. Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 354 (2015).

260. CTR. FOR DEMOCRACY & TECH., *supra* note 257, at 3; *see also* Jain, *supra* note 159, at 1427–28 (noting number of private entities that make use of arrest and criminal records for their own purposes unrelated to traditional goals of criminal justice); Daniel J. Solove, *Digital Dossiers*

about individuals and entire classes—suggesting which students are struggling, what they are struggling with, and whether and how they can improve—digital devices can also provide a composite picture so that educational researchers can study and improve pedagogy and curriculum on a widespread basis.[261] Perhaps for this reason, the Department of Education has encouraged schools to use "big data"[262] analysis to improve assessment and educational innovation.[263]

The goal of using data to improve pedagogy and curriculum may be normatively unobjectionable; however, even as schools use these technologies to further their educational mission, they may also be making students vulnerable to data capture for non-educational uses by the companies that provide the products. These companies engage, for example, in myriad if subtle forms of marketing to students, either in the present or by obtaining data for future marketing; as the 2016 report *Learning to be Watched: Surveillance Culture at School* notes, "[w]hile such massive amounts of specific and personal data are being collected about children at school, there is little understanding of how that information may be used in the future, or how it may be used to manipulate children and cultivate them as current and future consumers."[264] In 2017, the Electronic Frontier Foundation ("EFF") reported that the providers of educational technology "are spying on students—and school districts are . . . unwittingly helping them do it."[265] This report focuses on the collection of student informational data by digital learning devices as well as the weak privacy policies of educational technology companies, which typically lack encryption, data retention guidelines, and protection against nonconsensual data sharing.[266]

*and the Dissipation of Fourth Amendment Privacy*, S. CAL. L. REV. 1083, 1089–95 (2002) (discussing law enforcement's ability to obtain sensitive data from third parties).

261. Alim et al., *supra* note 54, at 33–34.

262. This Article adopts Julie Cohen's definition of "big data." *See* Cohen, *What Privacy Is For*, *supra* note 223, at 1920–21 ("'Big Data' is shorthand for the combination of a technology and a process. The technology is a configuration of information-processing hardware capable of sifting, sorting, and interrogating vast quantities of data in very short times. The process involves mining the data for patterns, distilling the patterns into predictive analytics, and applying the analytics to new data. Together, the technology and the process comprise a technique for converting data flows into a particular, highly data-intensive type of knowledge.").

263. Alim et al., *supra* note 54, at 7 (describing "technology in schools [as] giv[ing] states opportunities to understand student performance over time and be accountable for the effects of educational initiatives").

264. BONINGER & MOLNAR, *supra* note 46, at 14.

265. Alim et al., *supra* note 54, at 5.

266. BONINGER & MOLNAR, *supra* note 46, at 16; *see infra* Section II.D.

Surveillance can produce reality rather than simply reflecting it.[267] Instead of just neutrally monitoring and recording students' words and actions, surveillance can convey certain problematic values to students in ways that are not contested or even interrogated by most public-school stakeholders. For example, surveillance normalizes the notion that corporate interests have a legitimate role in education.[268] In addition, through its ubiquity across time and space, surveillance may encourage students to avoid experimentation that might draw unwanted attention, even though such experimentation is developmentally appropriate for young people whose identities are in flux. Surveillance scholars

> argue that "identity" is neither fixed nor unitary, but rather is constituted by performances that are directed at different audiences. From this perspective, the problem with surveillance is that it seeks to constitute individuals as fixed texts upon which invariant meanings can be imposed. The struggle for privacy is recast as the individual's effort to assert multiplicity and resist "norming."[269]

All told, in their embrace of digital technology, educators may unwittingly be creating a new generation of users accustomed to surveillance and relinquishing of their data in return for putative benefits.[270] And if any students reject the data sharing as a diminution of their privacy, those students may find themselves at odds with the institutions they need to prepare them for healthy development.

### *C. Equity*

While student surveillance is by now nearly universal in public schools, its application is uneven and inequitable. Surveillance is, in many cases, reflective of the biases of the people who create and administer its technologies and create policies. Already vulnerable populations are those most likely to experience negative repercussions from being surveilled.[271]

267. Warnick, *supra* note 113, at 324–25 (explaining that surveillance changes behaviors and the meanings that attach to them, arguing that "[a]ctions have different meanings when they are done alone versus when they are performed in front of an audience. Think of the difference between criticizing someone in public versus doing the same thing in private—these are two distinct activities").

268. BONINGER & MOLNAR, *supra* note 46, at 3 (writing that the study was "conducted with the implicit blessing of administrators, teachers, and parents," and the digital technology regime "combine[s] to normalize for children the notion that corporations have a legitimate role in their education and in their lives more generally").

269. Cohen, *Privacy, Visibility, Transparency*, *supra* note 255, at 187.

270. BONINGER & MOLNAR, *supra* note 46, at 20–23.

271. BRIDGES, *supra* note 27, at 32; *see* Kimberly D. Bailey, *Watching Me: The War on Crime, Privacy, and the State*, 47 U.C. DAVIS L. REV. 1539, 1557 (2014); Hao, *supra* note 105.

Low-income students are likely to need school-issued computers for homework more than higher-income students;[272] they are thus more likely to bear the brunt of surveillance policies that facilitate a school's ability to reach into a student's home.[273] While one might suggest that a possible remedy is for the student to use her own device rather than the device issued by the school, such a response ignores the reality that many low-income students cannot afford the technology on which schools increasingly rely.[274]

In addition, studies document the ways in which SROs disproportionately investigate and arrest students of color, particularly Black students.[275] Perhaps counterintuitively, as SROs incorporate information from surveillance technologies into their work, the racial disparities may well continue or even intensify. The reasons for this are twofold and related. Surveillance technologies are imbued with a sense of subjectivity by their makers, users, and proponents.[276] Officers may believe that using data from technology, rather than relying on non-digital means

272. LINDA DARLING-HAMMOND ET AL., USING TECHNOLOGY TO SUPPORT AT-RISK STUDENTS' LEARNING 11 (2014), https://edpolicy.stanford.edu/sites/default/files/scope-pub-using-technology-report.pdf [https://perma.cc/YJ8J-DQ6N] (describing a study examining the "implementation of a one-to-one laptop program in three economically different schools in California" and finding that "lower-income youth demonstrated significantly higher gains in mathematics relative to the higher-income students, and [that] teachers were most likely to say they found the laptops to be useful for learning by 'at-risk' youth"). When schools increasingly rely on digital learning materials to deliver material, the need for students to access the internet increases as well; when low-income students do not have regular and reliable access to the Internet, the use of digital learning technologies can exacerbate rather than ameliorate wealth-based learning gaps. Monahan, *supra* note 37 (quoting a Washington public school assistant superintendent as saying "[o]nce you've converted the curriculum, the material, it's more project-based learning. You kind of need the Internet for all those pieces to work well. If you're not able to provide that last level of connectivity, you've now widened the gap in terms of what kids can do, not to mention the expectation around that").

273. Suski, *supra* note 18, at 69; *see* T.V. v. Smith-Green Cmty. Sch. Corp., 807 F. Supp. 2d 767, 771 (N.D. Ind. 2011) (documenting that a school disciplined students for posting developmentally normative, if "raunchy," pictures of themselves taken during a slumber party that occurred in the summer).

274. Alim et al., *supra* note 54, at 6; *see* DARLING-HAMMOND et al., *supra* note 272, at 2–4 (noting wealth-based gaps in technology ownership).

275. *See, e.g.*, Kenneth Alonzo Anderson, *Does More Policing Make Middle Schools Safer?*, BROOKINGS BROWN CTR. CHALKBOARD (Nov. 8, 2019), https://www.brookings.edu/blog/brown-center-chalkboard/2018/11/08/does-more-policing-make-middle-schools-safer/ [https://perma.cc/EHW8-68T9] (noting and describing in detail "evidence of racial disparities in arrests by SROs"); Nance, *Students, Security, and Race*, *supra* note 17, at 41 ("[A]s [a] school's percentage of minority students increases, the odds of using combinations of security measures also increases.").

276. *See, e.g.*, Nelli Piattoeva, *The Imperative to Protect Data and the Rise of Surveillance Cameras in Administering National Testing in Russia*, 15 EUR. EDUC. RES. J. 82, 86 (2015) (noting that "'[o]bjectivity' is a term that figures prominently as an argument to justify the introduction of . . . digital technologies" into educational policymaking).

of investigation, may make their work less, rather than more, biased. Manuel's experience—drawing attention as a Latino young man with a group of friends he refers to as his "crew"—is instructive in this regard. The gestures he and his friends are making are ambiguous, but surveillance technologies deem them suspicious.[277] Indeed, a significant body of emerging research has documented that the algorithms on which much digital technology is based are themselves reflective of the biases of their creators.[278] Thus, communities traditionally disproportionately negatively affected by policing will draw little if any comfort from the fact that officers now use supposedly objective surveillance technologies.[279]

Finally, LGBTQ students disproportionately rely on the internet to find each other and find information about sexuality otherwise unavailable to them.[280] When they are not open about their sexual orientation and gender identity to peers or parents and fear that they will be bullied, abused, or worse, they must be able to keep their internet activity private.[281] Yet such privacy is all but absent in contemporary school surveillance regimes, which may result in "outing" students to their parents or peers in ways that can be harmful.[282]

### *D. Legal Constraints*

The law has not kept up with technological innovation.[283] As Omar Tene and Jules Polonetsky argue:

277. *See supra* Section I.B (discussing Manuel hypothetical).

278. *See, e.g.*, Hao, *supra* note 105 (noting and giving examples of bias in artificial intelligence before concluding that "[w]e often shorthand our explanation of AI bias by blaming it on biased training data. The reality is more nuanced: bias can creep in long before the data is collected as well as at many other stages of the deep-learning process").

279. *See* BRIDGES, *supra* note 27, at 32–34 (discussing the history of the diminution of privacy rights of poor people—especially poor women of color).

280. *See, e.g.*, GLSEN, CIPHR & CCRC, OUT ONLINE: THE EXPERIENCES OF LESBIAN, GAY, BISEXUAL, AND TRANSGENDER YOUTH ON THE INTERNET, at ix–x (2013), https://www.glsen.org/sites/default/files/Out%20Online%20FINAL.pdf [https://perma.cc/6J46-KQNQ] (finding that "LGBT youth were five times as likely to have searched for information online on sexuality or sexual attraction as non-LGBT youth (62 percent vs. 12 percent) . . . more likely to have searched for health and medical information compared to non-LGBT youth (81 percent vs. 46 percent) . . . [and] four times as likely to have searched for information on HIV/AIDS and other STIs (sexually transmitted infections) compared to non-LGBT youth (19 percent vs. 5 percent)").

281. *See* Allison S. Bohm et al., *Challenges Facing LGBT Youth*, 17 GEO. J. GENDER & L. 125, 151–55 (2016) (discussing the "bullying, harassment, and violence" experienced by LGBT youth).

282. *See id.* at 156 (discussing LGBT students' potential legal recourse when outed by school officials).

283. *See* Omar Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy, and Shifting Social Norms*, 16 YALE J. L. & TECH. 59, 73 (2013).

> In an environment of rapidly shifting social norms and expectations, the law can be a crude and belated tool. By the time the Supreme Court decided that tracking a suspect with a GPS device required a warrant, law enforcement authorities were already using drones. As multiple circuits continue to debate the minutiae of law enforcement's access to email, users have migrated en masse to new communication technologies such as instant messaging and VoIP. The surge in innovation and socio-technological progress has left entire industries drifting without clear ethical guidelines, as the law fails to catch up with rampant technologies.[284]

Likely, the rapid development of student surveillance can be attributed to this dearth of judicial precedent and statutes that specifically regulate the ever-evolving set of surveillance technologies. School districts, eager to do—or appear to be doing—everything they can to promote academic success and student safety, seem to view the absence of laws clearly proscribing or limiting use of a particular technology as permission to proceed with its implementation.

Proceeding quickly, however, does have its costs. These may include adverse legal rulings, when students and their families have the resources and inclination to enforce the meager set of rights they do have. They also may include negative publicity when surveillance violates privacy expectations and social norms—even if not the law—and thus seems "creepy."[285] Consider the following three examples.

First, when a school district's zeal to investigate a student's cell phone outweighs careful consideration of countervailing constitutional principles, the school may lose in court. In *New Jersey v. T.L.O.*,[286] the touchstone case for student searches, the Supreme Court endorsed a delinquency adjudication of a student who was charged with drug offenses based on items she had in her purse.[287] In ruling that the search and seizure of the purse—conducted with neither a warrant nor probable cause—did not offend the Fourth Amendment, the Court referenced the perceived link between a school's ability to have flexibility in administering discipline and the maintenance of order and security.[288] The Court announced that "reasonableness" would govern school searches, which is measured by assessing, first, whether a search is justified at its inception, and second, whether the search is reasonably related in scope to the circumstances

284. *Id.* (citations omitted).
285. *See id.*
286. 469 U.S. 335 (1985).
287. *See id.* at 347–48.
288. *See id.* at 341.

justifying the initial intrusion.[289] In its ruling, the Court specified that a search could be countenanced by both suspected violations of the criminal law and suspected infractions of school rules.[290]

The breadth of the category that can justify the initial search, combined with the low legal threshold of "reasonableness," means that few searches of a student's personal possessions are found unconstitutional.[291] Courts have upheld searches of students when they were sullen or boisterous; unusually quiet or loud; fatigued or overactive; withdrawn or excessively engaged with peers; disheveled or too neat.[292] In sum, behavior that is seemingly innocuous can justify the suspicion of a teacher or administrator who can claim familiarity with a child. And a search undertaken based on what in fact is nothing more than a lucky guess can be found reasonable by reviewing courts given the fact that the mere suspicion of a school-rule infraction can trigger the search in the first instance.[293] Warrants are required only when searches are conducted by outside law enforcement.[294]

*T.L.O.* and its progeny might seem also to countenance warrantless searches of student cell phones—notwithstanding the comparatively robust Fourth Amendment protections that attach to cell phones and smartphones—given the low "reasonableness" standard.[295] However, one school district, even before the decision in *Riley*, was found to have violated a student's Fourth Amendment rights in the wake of a warrantless cell phone search.[296] The student had a history of depression and marijuana usage.[297] He violated school policy regarding cell phone usage in the classroom.[298] Even taken together, however, the reviewing court deemed

289. *Id.* at 341–42 (following the twofold inquiry announced in *Terry v. Ohio*, 392 U.S. 1, 20–21 (1967)).

290. *Id.* at 342.

291. *See, e.g.*, *Developments in the Law—Policing Students*, 128 HARV. L. REV. 1747, 1761–62 (2015) ("Even if there is a distinct special need to maintain school safety and order justifying use of the balancing test, courts generally fail to accord proper weight to students' privacy interests and generally overvalue the government's interests. The weight courts give to students' privacy interests does not rely on or even consider the likely consequences of the search—school discipline or criminal prosecution.").

292. Martin H. Belsky, *Random Versus Suspicion-Based Drug Testing in the Public Schools: A Surprising Civil Liberties Dilemma*, 27 OKLA. CITY U. L. REV. 1, 19–21 (2002).

293. *See* Sarah Jane Forman, *Countering Criminalization: Toward a Youth Development Approach to School Searches*, 14 SCHOLAR 301, 319–20 (2011) ("The problem is that reasonable suspicion provides so much latitude for searching that school officials can construe almost anything as reasonable.").

294. *See id.* at 310–12.

295. *See id.* at 317.

296. G.C. v. Owensboro Pub. Sch., 711 F.3d 623, 634 (6th Cir. 2013).

297. *Id.* at 627.

298. *Id.* at 628.

these factors insufficient to justify a search of the student's phone; the court ruled that the search exceeded the scope of the reason for the phone seizure.[299]

Second, in a different district, school administrators installed video cameras in a student locker room.[300] Upon an argument by a group of parent plaintiffs that this installation violated the students' Fourth Amendment rights, the Sixth Circuit Court of Appeals held that this specific kind of video surveillance was unconstitutional.[301] The court found that while the safety rationale articulated by the school supported video surveillance generally, it was insufficient to justify the specific and particular intrusion into a locker room.[302] As in the pre-*Riley* student cell phone case, the issue for the Sixth Circuit was one of scope:

> A search—and there can be no dispute that videotaping students in a school locker room is a search under the Fourth Amendment—is 'permissible in its *scope* when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the age and sex of the student and the nature of the *infraction* as the commonly understood expectation for privacy increases, the range and nature of permissible government intrusion decreases. Given the universal understanding among middle school age children in this country that a school locker room is a place of heightened privacy, we believe placing cameras in such a way so as to view the children dressing and undressing in a locker room is incongruent to any demonstrated necessity, and wholly disproportionate to the claimed policy goal of assuring increased school security, especially when there is no history of any threat to security in the locker rooms.[303]

In other words, while safety concerns may generally countenance surveillance, there are in fact legal constraints on indiscriminate placement of surveillance devices, and in some cases the school will be held accountable when it cannot actually demonstrate that safety concerns justify a particular intrusion on a student's privacy interests.[304]

Third, schools that adopt sophisticated technologies without full awareness—or in disregard—of the technologies' potential may incur political blowback when the technologies cross a "creepy" line.[305] The

299. *Id.* at 634.
300. Brannum v. Overton Cty. Sch. Bd., 516 F.3d 489, 492 (6th Cir. 2008).
301. *Id.* at 498.
302. *Id.*
303. *Id.* at 496, 498 (citation omitted).
304. *Id.* at 498.
305. *See supra* note 283 and accompanying text.

following example from a Pennsylvania high school is illustrative. In the early part of the last decade, the school installed webcams in school-issued computers. Apparently unbeknownst to the school, the webcams could be activated without the students' knowledge, and they captured photographs and screenshots of students at their homes, often in their bedrooms, sometimes sleeping and frequently in states of undress.[306] The school claimed that it was using the technology only to track the computers in the event that they were lost or stolen, yet it did not weigh these apparent benefits against the serious privacy violations.[307] In a torrent of litigation and bad publicity—a successful lawsuit by the families of several students claiming tortious invasion of privacy and Fourth Amendment violations, a federal criminal investigation, and Senator Arlen Spector calling the program "surreptitious eavesdropping" during a Senate Judiciary Subcommittee meeting[308]—the school discontinued the program.

## III. TOWARD BETTER SURVEILLANCE POLICYMAKING

Teaching, by its nature, requires watching: ensuring that first graders stay in their seats, that middle schoolers do not copy each other's tests, and that high schoolers do not leave school grounds without permission.[309] As Bryan Warnick argues, to the extent that they merely enhance schools' ability to be watchful,[310] many surveillance technologies may be normatively unobjectionable.

The previous part identified ways, however, in which student surveillance technologies and policies do something fundamentally different in kind and degree from pre-digital age watchfulness. Namely, these technologies infringe on important privacy interests of students in

306. *See* Complaint at 7, 14, Robbins v. Lower Merion Sch. Dist., No. 10-665, 2010 WL 1957103 (E.D. Pa. May 14, 2010) (noting that "the webcam will capture anything happening in the room in which the laptop computer is located, regardless of whether the student is sitting at the computer and using it" and that the webcams captured students in various stages of undress).

307. Robert X. Cringley, *When Schools Spy on Their Students, Bad Things Happen*, PCWORLD (Feb. 23, 2010), https://www.pcworld.com/article/190019/school_spying_webcams.html [https://perma.cc/F5KX-VASJ]; Vince Lattanzio, *WebcamGate Teen: "I Hope They're Not Watching Me*, NBC (Feb. 2, 2010), https://www.nbcphiladelphia.com/news/tech/WebcamGate-Teen-I-Hope-Theyre-Not-Watching-Me-84826357.html [https://perma.cc/3BBS-MYDY] (discussing case).

308. Gregg Keizer, *Pa. School Spy Case Sparks Fight Over Money*, NETWORK WORLD (Mar. 19, 2010, 1:00 AM), https://www.networkworld.com/article/2204922/pa--school-spy-case-sparks-fight-over-money.html [https://perma.cc/PS7G-PWQQ].

309. TUCKER & VANCE, *supra* note 44, at 3.

310. Warnick, *supra* note 113, at 329 (arguing that "it seems to make little ethical difference if the watchfulness is aided by electronic tools").

ways that threaten to harm them in the short- and long-term. In addition, the contemporary surveillance regime does not affect students equitably.[311]

Notwithstanding the above-cited examples of courts stepping in to moderate the harm of surveillance technologies, it is nonetheless the case that students, families, and public-school stakeholders must depend for the most part on school districts to police themselves when it comes to developing ethical, age-appropriate surveillance strategies.[312] The following, non-exhaustive list is aimed at beginning a normative conversation about the values that should inform student surveillance policymaking.[313]

### *A. Minimization*

Among other features, the vast storage capacity of surveillance technology renders it qualitatively different from in-person watching during the pre-digital age. Digital educational technologies can maintain student information for a long period of time.[314] As such, they threaten to preserve in perpetuity students' often developmentally normative misbehavior,[315] which presumably may be reviewed far in the future by a potential employer, college, or graduate school.[316] This result severely undermines some of the traditional aims of school, which include the encouragement of intellectual risk-taking and forgiveness of misbehavior that arises from immaturity and developmentally normative poor judgment.[317] For these reasons, school administrators should seek to minimize their use of all surveillance technologies.

Minimization of surveillance technology has three additional benefits. First, to the extent that pervasive surveillance conveys messages of mistrust, those messages will be weakened. Second, surveillance minimization helps students value their privacy; it sets a precedent for students that surveillance is for particularized occasions and must be used

311. *See supra* Section II.C.

312. *See* Allen, *supra* note 241, at 733 (noting that surveillance "technology marches on" with few constraints).

313. *See* Adam M. Samaha, *What Good is the Social Model of Disability?*, 74 U. CHI. L. REV. 1251, 1253 (2007) (discussing the fact that a normative orientation should guide policymakers as they consider competing interests and confront questions of cost).

314. Elana Zeide, *Education Technology and Student Privacy*, *in* THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 71, 77 (2018) (discussing storage capacity of educational technology).

315. *See supra* note 207 and accompanying text (discussing the recognition, in the Supreme Court case of *Roper v. Simmons*, that young people are categorically less culpable than adults because they are impulsive, susceptible to peer pressure, and less able to weigh risk than adults).

316. *See* Zeide, *Limits on Education*, *supra* note 40, at 505–06.

317. Warnick, *supra* note 113, at 339.

with care.[318] Third, and finally, surveillance minimization empowers students to practice autonomy—to use their educational experience to try on new behaviors and identities toward an end of actualizing their right to an open future.[319]

### *B. Notice and Transparency*

When the Chapel Hill-Carrboro City Schools district in North Carolina rolled out its anonymous tip line, it did so in a way that seems typical of most student surveillance—namely, with no meaningful notice. In fact, the Director of School Safety informed students, staff, and families of the implementation of the tip line in a short email—and only *after* the tip line was already operational.[320] In response to a query about why parents were not told—either in writing or at a school board meeting with opportunity for discussion—about the tip line *prior* to its implementation, the Chapel Hill-Carrboro City Schools Board Chair responded: "Thank you for the message. This is an effort to increase safety at our schools and so not necessarily part of a public process for feedback. The board and administration has [*sic*] discussed questions of potential abuse and will continue to monitor the process to minimize unintended consequences."[321]

This disregard for the value of notice seems to demonstrate a belief either that students and parents do not care about surveillance or that they do not deserve to be informed about it in advance. However, such a belief runs counter to the Fair Information Practice principles, a set of aspirational principles developed over the past fifty years used to model rules for

318. *See supra* Section II.B. (discussing pedagogical work of surveillance).

319. John Eekelaar, *The Importance of Thinking that Children Have Rights*, 6 INT'L J.L. & FAM. 221, 229 (1992); Joseph Millum, *The Foundation of the Child's Right to an Open Future*, 45 J. SOC. PHIL. 522, 522 (2014).

320. The email said:

> Greetings CHCCS students, staff and families. As a school district and as a community, we depend on students to "say something" if they notice anything in or around school that looks like bullying, threats, drugs/alcohol or violence of any kind. To that end, earlier today Chapel Hill-Carrboro City Schools rolled out a new anonymous reporting option. This new Tipline allows students, parents or staff to anonymously submit any sensitive or urgent student issue quickly to school officials at the touch of a button. The Tipline link can be found on the front page of the new district website in the "Quick Links" section (www.chccs.org) and on the front page of each individual school website. It also can be accessed on the district app (search CHCCS in the App Store or Google Play). Once a tip is submitted, administration will take appropriate action. All messages submitted will remain completely anonymous.

Email from Chapel Hill-Carrboro City Schools to author (Sept. 26, 2018, 5:26 PM) (on file with the North Carolina Law Review).

321. E-mail from Rani Dasi, Chair of the Chapel Hill-Carrboro City Schools School Board, to author (Oct. 2, 2018, 6:56 PM) (on file with the North Carolina Law Review).

responsible data practices. These principles enshrine the values of notice and transparency.[322] Indeed, informing a public-school community about surveillance serves several important goals. First, a policy of transparency about surveillance permits students and families to protect their privacy interests as much as possible, if doing so is important to them. Second, a policy of transparency is critical to permit stakeholders to weigh in on whether and how much schools should deploy tools of surveillance. Given the costs and harms surveillance may produce, such a debate is critical. Indeed, schools are public institutions and must be operated with some degree of democratic accountability in the structuring of surveillance—notice and transparency should be required.[323]

### *C. Deletion*

Information obtained through surveillance should not be maintained indefinitely. The "transcendence of time"[324] through storage increases the likelihood that information gleaned about a particular student can be obtained by non-educational entities and later used for non-educational ends.[325] A policy of regular and routine deletion of student information both protects against the possibility of misuse and has an important signaling function that student misbehavior is something from which one can learn and out of which one can grow.[326]

### *D. Ongoing Recalibration of Benefits Versus Harms*

Omar Tene and Jules Polonetsky propose that, given the pace of technological innovation, individuals and institutions should engage in an ongoing recalibration of privacy expectations and norms to make determinations about whether and how much technology to use.[327] Such recalibration is critical for educational surveillance policymaking.

For one, the nature and extent of threats to students changes over time. The tools of surveillance should be proportional to the threats they are designed to address, and they should be discontinued if they do not in fact address those threats in some way.[328] Second, technologies may have unanticipated harms, as in the case of the webcam in the school-issued

322. *See* Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 952–53 (2017).
323. Warnick, *supra* note 113, at 339.
324. *Id.* at 333.
325. *See supra* notes 60–63, 264–66 and accompanying text.
326. Warnick, *supra* note 113, at 340.
327. Tene & Polonetsky, *supra* note 283, at 73.
328. Warnick, *supra* note 113, at 339.

laptops in the Pennsylvania high school.[329] Thus, even when a technology seems commensurate to a particular threat, its use may be so harmful that a particular school district must find a different way to address it.

School districts demonstrate an understanding of the value to students of being able to remove harmful data from their records. One North Carolina school district, for example, permits expungement of certain disciplinary data from student records.[330] Just as school districts are willing in some cases to jettison data that, on balance, they believe do more harm than good, so too must districts be willing to abandon technologies when the costs outweigh the benefits.[331]

## CONCLUSION

Scholars have established that the surveillance state has arrived, and that the most interesting and important issues to be considered are its normative content and scope. I have aimed to contribute to the discussion of surveillance with three principal contributions: by providing a typology of student surveillance technologies and policies; by analyzing the competing considerations relevant surveillance that typically are not—but should be—considered; and by offering preliminary thoughts on better student surveillance policymaking.

329. *See supra* notes 305–08 and accompanying text.

330. *Policy Code: 4345: Student Discipline Records*, ASHEVILLE CITY SCHS. (Oct. 3, 2011), https://www.ashevillecityschools.net/site/handlers/filedownload.ashx?moduleinstanceid=216&dataid=1241&FileName=4345-Student-Discipline-Records.pdf. [https://perma.cc/4NHP-43MC].

331. For a thoughtful and related examination of how to weigh competing values surrounding the use of police-generated digital video, see generally Richard E. Myers II, *Police-Generated Digital Video: Five Key Questions, Multiple Audiences, and a Range of Answers*, 96 N.C. L. REV. 1237 (2018) ("Any well-crafted policy regarding digital video must have calibrated answers to five key questions that arise as we consider the life cycle of the video: How will we handle (1) creation, (2) storage, (3) access, (4) redaction, and (5) use of the digital video created by these camera systems?").