Stanford Law Review

Volume 76 Symposium

ESSAY

The Surveilled Student

Danielle Keats Citron*

Abstract. We live in an age of student surveillance. Once student surveillance just involved on-campus video cameras, school resource officers, and tip lines, but now, it extends beyond school hours and premises. Corporate monitoring software, installed on school-provided laptops, does two things. First, it blocks "objectionable" material, informing administrators about content that students tried to access. Second, it scans students' searches, browsing, files, emails, chats, and geolocation to detect "problematic" material. For many students, school-provided laptops are their only computing device. They use that device to complete homework, as they must; they use it to chat with friends, explore ideas, and play. For those students, the surveillance is twenty-four hours a day, seven days a week, 365 days a year.

Totalizing surveillance makes student intimate privacy impossible and undermines the school's crucial role in educating democratic citizens. Student surveillance chills children's willingness to engage in expressive activities, including experimenting with nonmainstream ideas. Self-censorship is even more likely for disabled and LGBTQ+ students who fear judgment and reprisal. Student surveillance corrodes students' relationships with teachers. It raises the risk of suspension for Black and Hispanic students for minor infractions like profanity, a blow to equality. Companies promise that their surveillance systems can detect suicidal ideation, threats, and bullying, but little evidence shows that they work as intended. We need robust, substantive protections for student intimate privacy for the good of free expression, democracy, and equality. Schools should not use surveillance software unless companies can show

* Jefferson Scholars Foundation Schenck Distinguished Professor in Law and Caddell & Chapman Professor of Law, University of Virginia School of Law; Vice President, Cyber Civil Rights Initiative; 2019 MacArthur Fellow. Thank you to the *Stanford Law Review*, to Bella Ryb, Julia Gokhberg, Madison Marko, and to the rest of the editorial team for superb feedback. I am grateful to Caroline Corbin Mala and Alexander Tsesis for their leadership and creativity; to Mary Rose Papandrea for talking to me at length about the paper; to Eleanor Citron for her wisdom; to Jeff Stautberg and Taylor Stenberg for terrific research assistance; to Benjamin Klein, a high school senior who helped me understand his experience with student surveillance; to Kathryn Boudouris, librarian, thinker, and researcher extraordinaire; to Billi Jo Morningstar for savvy editing; to Ryan Calo, Naomi Cahn, Justin Driver, Evelyn Douek, Hany Farid, Alison Gocke, Woodrow Hartzog, Robert Post, Richard Schragger, Amelia Vance, Catharine Ward, Ari Waldman, and the participants in the 2024 Privacy Law Scholars conference for helpful suggestions; and to Dean Risa Goluboff for boundless support.

that the continuous tracking makes students safer and is designed to minimize the harm to privacy, expression, and equality.

Table of Contents

Introduction 1442

I. The United States of Student Surveillance 1448
- A. Old-School Surveillance 1449
- B. New-School Surveillance 1450
- C. Parental and Student (Non)Consent 1453

II. Undermining Schools as Citizen Incubators 1455
- A. Harm to Learning 1456
- B. Harm to Privacy, Expression, and Trust 1457
- C. Harm to Equality 1460
- D. Are Students Safer? 1463

III. A Plan for Reform 1465
- A. Law's Failure 1465
- B. First Step in Reform: Proof of Concept, Harm Minimization, and Stakeholder Involvement 1468
- C. Second Step: Duty of Nondiscrimination 1470

Conclusion 1472

Introduction

Americans want, expect, and deserve privacy in their intimate lives.[1] In June 2013, numerous elected officials cried foul upon discovering that the NSA had been amassing the telephone metadata of millions of people living in the United States.[2] Americans understood that such bulk surveillance risked self-censorship and conformity to the detriment of democratic engagement.[3] Congress appreciated this risk, and with the USA FREEDOM Act of 2015, prohibited the federal government's indiscriminate and continuous collection of call detail records.[4]

Although some government surveillance, like the bulk collection of telephone records, has been met with pushback and congressional action, *student* surveillance has been embraced by school administrators. For many years, K-12 public schools have used video cameras to record students on campus and anonymous tip lines to receive complaints.[5] Now, public schools are engaged in more comprehensive surveillance. Surveillance software is installed on school-provided laptops, enabling teachers, school resource

1. *See generally* DANIELLE KEATS CITRON, THE FIGHT FOR PRIVACY: PROTECTING DIGNITY, IDENTITY, AND LOVE IN THE DIGITAL AGE, AT xii-xiii, 4-7, 20-23, 41-47 (2022) (describing the ways in which Americans' intimate data is collected day-to-day and the impacts of this data being collected, used, shared, and sold on self-development, dignity, intimacy, and equality).

2. Dan Roberts & Spencer Ackerman, *Anger Swells After NSA Phone Records Court Order Revelations*, GUARDIAN (June 6, 2013, 9:05 PM EDT), https://perma.cc/UZ7J-6ZQ8; *see generally* ACLU v. Clapper, 785 F.3d 787, 795 (2d Cir. 2015) (describing how *The Guardian*'s publication of a leaked court order brought the telephone metadata program to the attention of the American public).

3. *See* Susan Page, *Poll: Most Americans Now Oppose the NSA Program*, USA TODAY (Jan. 20, 2014, 3:10 PM ET), https://perma.cc/MK5Y-2UH3 ("By nearly 3-1, 70-26%, Americans say they shouldn't have to give up privacy and freedom in order to be safe from terrorism."); *see also* Barry Friedman & Danielle Keats Citron, *Indiscriminate Data Surveillance*, 110 VA. L. REV. (forthcoming 2024) (manuscript at 34-37), https://perma.cc/7APS-WYBJ (describing public and official rejection, including by the Privacy and Civil Liberties Oversight Board, of the NSA's bulk indiscriminate collection of telephone data).

4. Pub. L. No. 114-23, § 501, 129 Stat. 268, 282-83 (codified in scattered sections of the U.S. Code).

5. MICHAEL PLANTY, DUREN BANKS, CHRISTINE LINDQUIST, JOEL CARTWRIGHT & AMANDA WITWER, RTI INT'L, TIP LINES FOR SCHOOL SAFETY: A NATIONAL PORTRAIT OF TIP LINE USE 3, 11 (2020), https://perma.cc/QQ9M-Z3MB (noting that 51% of public middle and high schools maintained tip lines as of 2019 and over half included local law enforcement officers in the tip-line programs); *Fast Facts: School Safety and Security Measures*, NAT'L CTR. FOR EDUC. STAT., https://perma.cc/W2BB-KGFT (archived May 1, 2024) (reporting that in 2019-2020, 91% of public schools K-12 used security cameras to monitor schools, up from 61% in 2009-10).

officers, and companies to monitor in real time students' searches, browsing sessions, emails, chats, photos, calendar invites, geolocations, and more.[6]

Monitoring software serves two central roles. The first is to block students' access to problematic content and to inform administrators about the flagged content that students tried to access. Along these lines, monitoring software can help teachers manage their classrooms, enabling teachers to see what students are viewing and, if necessary, close or switch students' tabs.[7] The second is to scan students' online activities (emails, chats, searches, browsing, files) for evidence of bullying, self-harm, and safety threats.[8] During the 2021-2022 school year, 95% of surveyed teachers reported that their schools or districts provided students with tablets and laptops; 89% reported that monitoring software was installed on school-issued and/or personal devices.[9] Separately, companies monitor students' social media activity to detect potential threats.[10] In thousands of public school districts, primary and secondary school students are being surveilled twenty-four hours a day, seven days a week, summers included. "[O]nce a school district buys [certain

6. Thousands of the 17,396 public school districts in the United States have purchased surveillance products that monitor student communications and laptop activity. CHAD MARLOW, EMILY GREYTAK, KATIE DUARTE & SUNNY SUN, ACLU, DIGITAL DYSTOPIA: THE DANGER IN BUYING WHAT THE EDTECH SURVEILLANCE INDUSTRY IS SELLING 8-10 (2023), https://perma.cc/YU5H-B9PQ. A nationally representative sample of secondary school students, who were between 14 and 18 years old, surveyed during the 2022-23 school year reported widespread use of surveillance tools in their schools. *Id.* at 10. A report issued by the Center on Democracy and Technology in 2021 found that "student activity monitoring software is used extensively in K-12 schools." HUGH GRANT-CHAPMAN, ELIZABETH LAIRD & CODY VENZKE, CTR. FOR DEMOCRACY & TECH., STUDENT ACTIVITY MONITORING SOFTWARE: RESEARCH INSIGHTS AND RECOMMENDATIONS 2 (2021), https://perma.cc/3H7R-UKG5 (noting the ability of such software to "[v]iew the contents of a student's screen in real-time").

7. *See* JAMIE GOROSH & CHRIS WOOD, LGBT TECH & FUTURE OF PRIV. F., STUDENT VOICES: LGBTQ+ EXPERIENCES IN THE CONNECTED CLASSROOM 4-5 (2023), https://perma.cc/A92Q-L3S6.

8. MARLOW ET AL., *supra* note 6, at 48-49; Peter D'Auria, *In the Wake of Texas School Shooting, a Vermont-Founded Company Draws Scrutiny*, VTDIGGER (June 7, 2022, 2:52 PM), https://perma.cc/5B7T-3TFW.

9. ELIZABETH LAIRD, HUGH GRANT-CHAPMAN, CODY VENZKE & HANNAH QUAY-DE LA VALLEE, CTR. FOR DEMOCRACY & TECH., HIDDEN HARMS: THE MISLEADING PROMISE OF MONITORING STUDENTS ONLINE 7-8 (2022), https://perma.cc/EQK2-KB37. Surveillance companies operating since the pandemic monitor nearly everything a student does online. *See* MARLOW ET AL., *supra* note 6 at 8-10. For example, companies like Gaggle scan student electronic communications, including emails, documents written on school accounts, and software applications. *Id.* at 49. Other companies like GoGuardian monitor what students search for and what websites they visit. *Id.*

10. MARLOW ET AL., *supra* note 6, at 48; D'Auria, *supra* note 8.

monitoring] services, students don't have a school-friendly alternative" for email and assignments.[11] In other words, students cannot opt out.

Everyone wants, expects, and deserves "intimate privacy"—the ability to set boundaries around our intimate lives and control the extent to which others have access to and information about our bodies, minds, health, sex, sexual orientation, gender identity, and close relationships.[12] Everyone needs intimate privacy to develop identities, freely express themselves, and forge close relationships, but this interest is especially important for children.

Children have an interest in what we can describe as *student intimate privacy*. One's youth is a time of enormous change. Students experience profound physical and emotional growth during their school years.[13] Adolescents undergo considerable physical and emotional change; they are continuously inventing and reinventing their identities and ideas.[14] Self-development is a student's full-time job; students spend their time learning, creating, exploring, thinking, speaking, and cultivating friendships.[15] Students are meant to be developing skills of free expression and civic engagement, and schools are meant to facilitate "educating the young for citizenship."[16]

Continuous online monitoring denies young people the space that they need to learn, think, and express themselves. Totalizing student surveillance is stifling and intimidating; it chills students from seeking out certain material because they fear embarrassment, disapproval, and discipline.[17] It narrows the aperture of students' online activities and deters them from seeking advice on

11. Caroline Haskins, *Gaggle Knows Everything About Teens and Kids in School*, BUZZFEED NEWS (Nov. 1, 2019, 12:48 PM), https://perma.cc/3K3B-Z6KX.

12. CITRON, *supra* note 1, at xii-xiii (defining and making a moral case for intimate privacy).

13. For an extended discussion of childhood development as it relates to privacy and secrecy, see MAX VAN MANEN & BAS LEVERING, CHILDHOOD'S SECRETS: INTIMACY, PRIVACY, AND THE SELF RECONSIDERED 3-5, 89-101, 110-12 (1996). *See also* ERIK H. ERIKSON, INSIGHT AND RESPONSIBILITY: LECTURES ON THE ETHICAL IMPLICATIONS OF PSYCHOANALYTIC INSIGHT 45 (1964) [hereinafter ERIKSON, INSIGHT] (reflecting on Sigmund Freud's admonition to train observation back on "childhood" to detect what "spoils the genius of the child in every human being" and to preserve the "creatively good"); ERIK H. ERIKSON, IDENTITY: YOUTH AND CRISIS 122-35 (1968) [hereinafter ERIKSON, IDENTITY] (emphasizing school-age children's readiness to learn, do, and share obligations, as well as their attachment to teachers).

14. *See* ERIKSON, INSIGHT, *supra* note 13, at 90-92.

15. As John Dewey explains, the job of the pupil is "to do—and learn." JOHN DEWEY, EXPERIENCE AND EDUCATION 19-21 (Touchstone 1997) (1938) (urging schools to cultivate expression and individuality and to emphasize learning through experience).

16. W. Va. State Bd. of Educ. v. Barnette, 319 U.S. 624, 637 (1943).

17. *See* MARLOW ET AL., *supra* note 6, at 22-25.

issues central to their developing identities.[18] It makes them see themselves as problems or suspects whose online activities must be watched.[19] Without student intimate privacy, students cannot freely listen, learn, read, browse, search, speak, chat, and email.

Student surveillance is justified on the grounds that it will save student lives.[20] Companies claim that their monitoring algorithms can flag suicidal ideation, cyberbullying, and potential threats.[21] Their content moderators, they claim, can sift through thousands of alerts and notify school administrators and law enforcement about serious problems so they can intervene before the worst happens.[22]

No doubt, children's physical and emotional safety is of paramount value. Having studied the perils of online abuse for the past fifteen years, I know that the stakes for children are as high as life itself. When students face intimate privacy violations or harassment online, their mental anguish can be so severe that they take their own lives.[23] According to a 2023 study on LGBTQ+ students and school surveillance, a majority of survey participants personally experienced cyberbullying and recognized the benefits of monitoring for cyberbullying but worried about the privacy implications.[24]

If surveillance tools can help us detect destructive online abuse and minimize suffering, then we should assess how we might deploy those tools while safeguarding student intimate privacy. Student safety and intimate

18. *See id.*; *see generally* ERIKSON, INSIGHT, *supra* note 13, at 90-92 (discussing adolescence as a period of uprootedness where young people engage in identity development, defining and redefining themselves so they can "recognize [themselves] and feel recognized" by others" (emphasis omitted)).

19. *See* MARLOW ET AL., *supra* note 6, at 5, 24-25.

20. For example, the Gaggle website describes its services as providing "Online Solutions for K-12 Student Safety." GAGGLE, https://perma.cc/GWX2-DJVT (archived May 1, 2024) (claiming that "95% of district partners believe Gaggle identified students who no one knew were depressed"). From 2018-2023, Gaggle claims to have analyzed 27.7 billion student items and identified more than 43,000 imminent threats to students' well-being. *Id.*

21. *See, e.g.*, Letter from Jeff Patterson, CEO & Founder, Gaggle, to Senators Warren, Blumenthal & Markey 1 (Oct. 12, 2021), https://perma.cc/GN6H-WDN9; BARK, https://perma.cc/2PNE-WAHG (to locate, select "View the live page," and then select "Content monitoring") (noting that Bark's "powerful AI scans student . . . accounts (including emails, chats, and files) for potential issues like threats of violence, cyberbullying, and more" and is "[t]rusted by over 3,700 school districts in the U.S.").

22. *See* MARLOW ET AL., *supra* note 6, at 11-18.

23. *See* DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 11 (2014) (discussing instances of suicide among students facing cyber harassment and noting that 45% of LGBTQ+ students facing online abuse felt depressed while 25% wrestled with suicidal thoughts).

24. GOROSH, *supra* note 7, at 9.

privacy need not be a zero-sum game; both can be secured with properly calibrated safeguards. If surveillance companies have the ability to prevent tragedies, then we should focus on how to secure student safety while protecting student intimate privacy.

Before considering how safety and student intimate privacy might be balanced, we first need proof that the claimed safety benefits of student surveillance are bona fide. Right now, no impartial evidence backs self-serving corporate claims. Companies supply anecdotal stories and tout the numbers of problems averted (in the hundreds of thousands), yet they provide no independent proof in support.[25] For instance, Gaggle claims to have flagged 1.4 million student safety incidents and saved an "estimated" 5,790 lives from 2018 to 2023.[26] But these numbers have not been subject to systematic, impartial evaluation.[27]

Computer scientists have called these claims into question. Renowned computer scientist Arvind Narayanan considers the notion that algorithms can predict at-risk kids or criminal activity "[f]undamentally dubious."[28] He does not mince words: Promoting surveillance software as capable of making such predictions is tantamount to peddling "snake oil."[29]

Schools have been purchasing surveillance tools without meaningful input from the public.[30] The contracting process is secret; many parents are not notified until after new technology has been implemented in the classroom or

25. *See* MARLOW ET AL., *supra* note 6, at 14-18 (highlighting surveillance companies' reliance on unsubstantiated success metrics, general claims and insinuations of efficacy, and "one-off success stories" to make up for their lack of reliable, independent data); *id.* at 11 (explaining that the existing research literature confirms that "there is little empirical evidence to support the claim that school surveillance technologies meaningfully increase safety or reduce violence in schools"); Rebecca Heilweil, *The Problem with Schools Turning to Surveillance After Mass Shootings*, VOX (June 2, 2022, 7:30 AM EDT), https://perma.cc/3UUV-QHRT (noting the proliferation of surveillance technology following the Uvalde shooting despite the lack of evidence that such technology can prevent similar tragedies).

26. GAGGLE, *supra* note 20.

27. *See* JOHNS HOPKINS UNIV. APPLIED PHYSICS LAB'Y, A COMPREHENSIVE REPORT ON SCHOOL SAFETY TECHNOLOGY §§ 13.5, 13.6 (2016), https://perma.cc/3VTL-YDKJ (finding that few school safety technologies have undergone sustained study to determine if they are effective); *see generally* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 3-8 (2015) (exploring the opacity of automated systems used in the public and private sector).

28. Arvind Narayanan, Assoc. Professor, Princeton Univ., How to Recognize AI Snake Oil 9 (2019), https://perma.cc/PN72-WKDE.

29. *Id.* at 9-21 (questioning claims that algorithms, even with huge amounts of data about children and families, can accurately predict at-risk kids).

30. *See* LAIRD ET AL., *supra* note 9, at 17-18.

installed on students' devices.[31] Students, parents, and their elected officials must have the chance to evaluate, approve, and monitor surveillance programs. Students cannot opt out of the continuous monitoring. During school hours, they must connect their devices to the school's WiFi, which monitors the network traffic. After school hours, surveillance companies monitor everything students do with their school-issued laptops.[32] Thus, students whose families cannot afford personal devices cannot avoid the surveillance.

Student surveillance may make children less safe and less free. Studies have shown that student surveillance particularly imperils the well-being of poor students, rural students, disabled students, Black and Hispanic students, and LGBTQ+ students.[33] Rather than preventing shootings or suicides, the more common result from student surveillance is discipline for violations of school policy.[34] Black students disproportionately face suspension due to student surveillance.[35] LGBTQ+ students have been "outed" to teachers and parents, which exposes students to discriminatory treatment at school and physical and emotional abuse at home.[36] This is not protecting vulnerable students; it is endangering them.

---

31. According to one survey, 1 in 5 parents do not know if their school uses student monitoring software. *Id.* at 17. And although 92% of teachers report that a parent or student signs a form agreeing to the terms and conditions of how student's school-provided devices can be used, only 1 in 4 teachers report that the form is very effective in explaining the use of monitoring systems, and only 39% of parents and 23% of students were asked for input on the use of monitoring systems. *See id.* at 17-18'; *see also* FRIDA ALIM, NATE CARDOZO, GENNIE GEBHART, KAREN GULLO & AMUL KALIA, ELEC. FRONTIER FOUND., SPYING ON STUDENTS: SCHOOL-ISSUED DEVICES AND STUDENT PRIVACY 10-16, 19-21 (2017), https://perma.cc/H93A-G9QP (explaining that most parents and students do not understand the extent of student monitoring).

32. *See infra* notes 65-67 and accompanying text.

33. ELIZABETH LAIRD, CTR. FOR DEMOCRACY & TECH., HIDDEN HARMS: STUDENTS WITH DISABILITIES, MENTAL HEALTH, AND STUDENT ACTIVITY MONITORING 5-8 (2022), https://perma.cc/8GXX-7C75; LAIRD ET AL., *supra* note 9, at 23 (explaining that 6 in 10 Black students, 6 in 10 Hispanic students, 7 in 10 rural students, and 7 in 10 low-income students rely on school-issued laptops or tablets, and are therefore subject to the attendant harms more frequently than students from high-income families who often have personal devices).

34. In one survey, 59% of teachers reported at least one instance of student discipline resulting from activity monitoring. LAIRD ET AL., *supra* note 9, at 24 (adding that 55% of Hispanic students and 48% of Black students report getting into trouble or hearing about other students facing discipline due to student activity monitoring as opposed to 41% of White students reporting the same).

35. Odis Johnson Jr. & Jason Jabbari, *Infrastructure of Social Control: A Multi-Level Counterfactual Analysis of Surveillance and Black Education*, J. CRIM. JUST., Nov.-Dec. 2022, at 1, 5.

36. *See* LAIRD ET AL., *supra* note 9, at 21 (describing how nearly 1 in 3 LGBTQ+ students reported that they or someone they knew had been outed due to school surveillance software, and 31% of LGBTQ+ students reported that they or someone they knew had

footnote continued on next page

This essay introduces *student intimate privacy*[37] as a value in the student surveillance debate. Part I documents the totalizing nature of student surveillance. Part II shows how the denial of student intimate privacy wreaks havoc on students' ability to explore, learn, and speak. Students censor what they say and do online because they do not want their activities to attract suspicion or discipline.[38] Surveillance is expressive: It tells students that schools see them as potential victims or suspects rather than as future voters and citizens. Students are inhibited from using digital tools to learn and listen, to speak and share, to explore and play, and to communicate freely.

Protecting student intimate privacy may require scaling back on student surveillance and securing crucial safeguards to minimize the harm to student intimate privacy and the expression that it enables. Part III turns to legal reforms that might help us protect student intimate privacy and safety—or at least strike a far better balance than exists now. We need legal reforms that introduce transparency, accountability, and safeguards to student surveillance. Schools should not use surveillance software unless companies can show that the tracking makes students safer and minimizes the harm to privacy, expression, and equality. We need robust, substantive protections for student intimate privacy to protect free expression, democracy, and education.

I. The United States of Student Surveillance

Students are being monitored all year long, at all hours. This Part sketches the state of student surveillance in the United States. Subpart A sets the stage by describing decades-long surveillance in schools: video cameras, school resource officers, and tip lines. Subpart B turns to the more recent adoption of digital surveillance, especially since the COVID-19 pandemic, that continuously tracks students' online activities whenever and wherever they use school-issued laptops and on whatever device they post on social media. Subpart C discusses the limited role that parents, guardians, and students are allowed to play in this new world of student surveillance.

---

been contacted by police or other authorities about possibly committing a crime as opposed to 19% of non-LGBTQ+ students reporting the same).

37. *See generally* CITRON, *supra* note 1, at xii-xiii (making the moral case for intimate privacy); Danielle Keats Citron, *Intimate Privacy's Protection Enables Free Speech*, 2 J. FREE SPEECH L. 1, 1-4 (2022) (highlighting the centrality of intimate privacy to human flourishing, self-development, self-esteem and social esteem, and love).

38. GRANT-CHAPMAN ET AL., *supra* note 6, at 4.

A. Old-School Surveillance

Let us begin with what we can describe as old-school surveillance tools.[39] For decades, schools have maintained video cameras to monitor hallways, entrances, and recreation areas. The uptick in school districts' purchases of CCTV cameras began in the 1990s.[40] The trend spread as businesses sold the concept of school security.[41] As of the 2019-2020 school year, 97% of public high schools were using security cameras to monitor school activity.[42]

Surveillance cameras have grown in sophistication. For instance, CCTV cameras have "pan-tilt-zoom capabilities," which expand the areas that can be seen and recorded.[43] Some school cameras incorporate technology that allegedly can identify "anomalous" behavior and notify school officials.[44] Some CCTV sellers claim that their cameras can detect the presence of a weapon.[45] Some school surveillance cameras provide local police with real-time access to video feeds.[46]

School resource officers work for schools and districts. These officers are hybrid counselors, teachers, and police officers.[47] In the 2019-2020 school year, approximately 65% of all public schools (primary and secondary) had security staff.[48]

Another old-school tactic is the tip line. Students can report other students anonymously online. As of the 2018-2019 school year, more than 51% of public

39. Pun intended.

40. *See* RONNIE CASELLA, SELLING US THE FORTRESS: THE PROMOTION OF TECHNO-SECURITY EQUIPMENT FOR SCHOOLS 1-2, 65, 68-70 (2006).

41. *See id.* at 5-7, 68-75. This is not just a U.S. problem. We see the adoption of tech solutions for school safety around the world. *See, e.g.*, BIG BROTHER WATCH, BRIEFING ON 'BIOMETRIC DATA IN SCHOOLS' FOR THE WELSH SENEDD (2023), https://perma.cc/4DVJ-8JMM (questioning the legality, necessity, and proportionality of facial recognition software used in Welsh schools).

42. *Fast Facts*, *supra* note 5.

43. CASELLA, *supra* note 40, at 1-2.

44. MARLOW ET AL., *supra* note 6, at 48 (describing a technology sold by vendors Avigilon, Axis, BriefCam, and Verkada that "watches and analyzes video-subjects for behaviors it is either taught are problematic, or which it concludes, via self-learning, may be 'anomalous'").

45. *Id.* at 10, 50.

46. *Id.* at 46.

47. Hannah Dreier, *He Drew His School Mascot—and ICE Labeled Him a Gang Member*, PROPUBLICA (Dec. 27, 2018), https://perma.cc/T878-ZQDT; Kristin Henning, *Cops at the Schoolyard Gate*, VOX (July 28, 2021, 8:00 AM EDT), https://perma.cc/6QYT-S9MW.

48. *Digest of Education Statistics: Table 233.70. Percentage of Public Schools with Security Staff Present at Least Once a Week, and Percentage with Security Staff Routinely Carrying a Firearm, by Selected Schools Characteristics: 2005-06 Through 2019-20*, NAT'L CTR. FOR EDUC. STAT., https://perma.cc/H7FL-23G5 (archived May 1, 2024).

middle and high schools maintain tip lines via websites, phone, app, email, or text, and over half send tips to local law enforcement officers.[49]

These surveillance tactics are now paired with more invasive and far-reaching digital services provided by tech startups. The next Subpart discusses the persistent monitoring of online communications and activities.

B. New-School Surveillance

Since the COVID pandemic, primary and secondary U.S. public schools have purchased services that continuously monitor students on their school-provided computing devices. In short, wherever (home or friends' homes) and whenever (nights and weekends) students use those devices, they are being algorithmically monitored.[50] Their emails, chats, searches, browsing, documents, app activity, and more are analyzed for "problematic" behavior.[51] The monitoring is happening even if students are not working on school-related activities but instead messaging with friends or searching for health concerns.[52] If students charge their personal phones by plugging them into school-issued laptops, then their phones may be monitored as well.[53]

During remote learning amid the COVID pandemic, surveillance software gave teachers real-time access to students' online activities to make sure they stayed on task.[54] Teachers could control students' screens as they browsed.[55] But teachers, administrators, and companies got access to far more than students' in-class activities. Some surveillance software gives teachers access to any device connected to the school WiFi, including personal laptops and cellphones; other surveillance software monitors just school-provided laptops and devices.[56]

---

49. PLANTY ET AL., *supra* note 5, at 3, 8, 11.

50. *See* GRANT-CHAPMAN ET AL., *supra* note 6, at 1-2; *supra* note 21 and accompanying text.

51. *See id.*

52. *See id.*

53. Pia Ceres, *Kids Are Back in Classrooms and Laptops Are Still Spying on Them*, WIRED (Aug. 3, 2022, 12:01 AM), https://perma.cc/TM9T-6TWA.

54. *Id.*

55. *Id.*; *see also* Priya Anand & Mark Bergen, *Big Teacher Is Watching: How AI Spyware Took Over Schools*, BLOOMBERG BUSINESSWEEK (Oct. 28, 2021, 2:00 AM PDT), https://perma.cc/VT2A-ZNVP.

56. *See* Pia Ceres, *How to Protect Yourself If Your School Uses Surveillance Tech*, WIRED (Oct. 18, 2022, 7:00 AM), https://perma.cc/U67W-F2PC (advising parents and students to ask whether monitoring software "operate[s] on school devices, over the school Wi-Fi network, or both"); *see generally* Larry Ferlazzo, Opinion, *Should Teachers Be Allowed to Use Online Tools to Monitor Student Screens?*, EDUCATION WEEK (Mar. 21, 2023), https://perma.cc/3GMQ-WSVL (collecting firsthand opinions on the use of screen-monitoring tools).

Monitoring software performs two functions. First, it blocks students from accessing "objectionable" material and notifies school administrators about the material that students tried to access.[57] Second, it continuously scans students' activity for the purpose of identifying concerning activity, including potential suicidal ideation, bullying, or violent threats.[58] Companies' content moderators assess the flagged material and pass on alerts to educators and others.[59]

Consider the surveillance services of Gaggle.[60] The company's platform scans students' "school-provided email accounts, document creation, . . . calendar entries, chat, and other direct and group communication tools" and uses "keywords, algorithms, and machine learning to identify content that indicates students planning self-harm, bullying, abuse, or school violence."[61] Gaggle's software "is designed to monitor the school-provided devices and platforms 24 hours a day."[62] Gaggle's content moderators review flagged content and surrounding text to determine the urgency of the situation; if deemed serious, they alert school administrators and, if necessary, contact emergency medical services or law enforcement.[63]

The growth in student laptops with surveillance software has been astronomical. In 2014, one-third of all K-12 students in U.S. public schools used school-provided devices, generally with monitoring software installed.[64] During the 2021-2022 school year, 95% of surveyed teachers reported that their schools provided students with tablets and laptops; 89% reported that their school monitors school-issued and/or personal devices.[65]

---

57. *See* Todd Feathers, *Schools Use Software That Blocks LGBTQ+ Content, but Not White Supremacists*, VICE (Apr. 28, 2021, 6:00 AM), https://perma.cc/7CNT-EQHW.

58. *See supra* note 21 and accompanying text.

59. *See, e.g.*, MARLOW ET AL., *supra* note 6, at 48-49; GAGGLE, *supra* note 20 (noting that between July 2018 and June 2023, Gaggle software had analyzed 27.7 billion student items).

60. Mark Keierleber, *Exclusive Data: An Inside Look at the Spy Tech That Followed Kids Home for Remote Learning—and Now Won't Leave*, THE 74 (Sept. 14, 2021), https://perma.cc/5NC4-7WP8 (explaining that Gaggle monitors students' school-issued Google and Microsoft accounts).

61. Letter from Jeff Patterson, *supra* note 21, at 5-6. Gaggle says that it does not monitor students' web browsing activities or social media accounts. *Id.* at 5. Such monitoring is provided by other surveillance companies like GoGuardian, Bark, and Social Sentinel. MARLOW ET AL., *supra* note 6, at 48-49.

62. Letter from Jeff Patterson, *supra* note 21, at 11.

63. Keierleber, *supra* note 60.

64. *See* ALIM ET AL., *supra* note 31, at 5 (adding that student laptops "collect far more information on kids than is necessary," such as students' "browsing history, search terms, location data, contact lists, and behavioral information").

65. LAIRD ET AL., *supra* note 9, at 7-8. Surveillance companies operating since the pandemic monitor nearly everything a student does online. *See supra* note 9.

The monitoring of students' online activities is not limited to school hours. According to a 2021 national study, 30% of teachers surveyed reported that software monitoring is conducted "all of the time."[66] Companies' content moderators forward alerts to school administrators during the school day; they send alerts to school resource officers or law enforcement during the evenings and weekends.[67] In a study of a Minneapolis school district, 75% of incidents reported to school district officials occurred after the end of the school day, on weekends, and over the summer.[68] Because the surveillance alerts are sent when school is not in session, school resource officers or law enforcement officers may go to students' homes.[69]

Surveillance platforms also monitor students' social media activity.[70] Social Sentinel and DigitalStakeout "[s]can[] students' public social media accounts for words and phrases that are designated by the school and/or the product provider to be problematic, even when [the students] are off campus."[71] When the technology identifies a problematic post, it notifies the company's moderators, school administrators, or both.[72] One of the founders of Social Sentinel came up with the idea when, as the police chief at the University of Vermont, he investigated issues including "a planned protest at the university's executive offices."[73] True to that experience, universities including the University of North Carolina at Chapel Hill have used the technology to track student protests.[74]

66. GRANT-CHAPMAN ET AL., *supra* note 6, at 2 (adding that only 1 in 4 teachers surveyed reported that software monitoring was specifically limited to school hours).

67. LAIRD ET AL., *supra* note 9, at 14-16 (noting that 37% of teachers at schools that use surveillance software outside of school hours report that a third party, such as law enforcement, receives alerts from the monitoring system after school hours).

68. *See* Keierleber, *supra* note 60.

69. LAIRD ET AL., *supra* note 9, at 15-16; *see, e.g.*, Liz Bowie, *Baltimore School-Issued Laptops Monitored for Safety and Mental Health Reasons, Officials Say*, WASH. POST (Oct. 24, 2021, 4:40 PM EDT), https://perma.cc/5Q59-Z3JY.

70. MARLOW ET AL., *supra* note 6, at 48.

71. *Id.*

72. *Id.*

73. Gary J. Margolis, *Is Social Media Monitoring the Right Fit for Safety and Security Teams*, SOCIAL SENTINEL BLOG (Oct. 1, 2015, 2:02 PM), https://perma.cc/KC9U-HK9G; *Dr. Gary J. Margolis*, SOCIAL SENTINEL BLOG https://perma.cc/QE68-5EYA (archived May 1, 2024).

74. Ari Sen, *Texas Schools are Surveilling Students Online, Often Without Their Knowledge or Consent*, DALL. MORNING NEWS (Sept. 2, 2021, 6:00 AM CDT), https://perma.cc/Y7HS-PUCV; *see also* Arijit Douglas Sen & Derêka Bennett, *Tracked: How Colleges Use AI To Monitor Student Protests*, DALL. MORNING NEWS (Sept. 20, 2022), https://perma.cc/T44V-U63V.

Student surveillance is happening without meaningful notice or approval from parents and students, a problem to which we now turn.

C. Parental and Student (Non)Consent

Surveillance software providers usually do not notify students and parents about what is happening.[75] Instead, notice is generally provided by school districts.[76] But the notice is inadequate.[77] According to researchers, 45% of surveyed parents said that their "schools or districts did not provide parents with written disclosure" about surveillance technology.[78] As the Director of Illinois Families for Public Schools indicated, parents have difficulty sorting out which companies are tracking their children's online activities.[79] One California parent explained that the "specifics of the technology our children would use were not provided until back-to-school night, where the teacher emphasized the Chromebooks' value for individualized instruction."[80]

School districts assert that students should not expect any privacy in their online activities when using school networks and devices.[81] In a survey of thirty-six public school districts in Rhode Island, the ACLU found that twenty-three school districts claimed students should not expect any privacy

75. ELIZABETH WARREN & ED MARKEY, CONSTANT SURVEILLANCE: IMPLICATIONS OF AROUND-THE-CLOCK ONLINE STUDENT ACTIVITY MONITORING 3 (2022), https://perma.cc/5GH5-HATU.

76. *Id.*

77. *See, e.g.*, Barbara Fedders, *The Constant and Expanding Classroom: Surveillance in K-12 Public Schools,* 97 N.C. L. REV. 1673, 1723-24 (2019) (describing how a North Carolina school district provided no notice of a new tip line until after it was already operational, in a manner "typical" of student surveillance). This is par for the course: The woeful inadequacy of notice provided about corporate surveillance is well documented. *See, e.g.*, Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1463 (2019) (explaining that the notice-and-choice regime in U.S. consumer privacy law amounts to a take-it-or-leave-it model that allows companies to bury notice in dense privacy policies that hardly anyone reads or few can understand).

78. ALIM ET AL., *supra* note 31, at 10.

79. Nader Issa, *CPS Teachers Could Look Inside Students' Homes—Without Their Knowledge—Before Fix*, CHI. SUN TIMES (Oct. 5, 2020, 3:30 AM PST), https://perma.cc/2G7J-L8SB.

80. ALIM ET AL., *supra* note 31, at 11.

81. *See, e.g.*, Fedders, *supra* note 77, at 1676 n.12 (citing Durham Pub. Schs. Bd. Educ., Technology Responsible Use, https://perma.cc/X3SX-AQ5Q (archived May 10, 2024) (providing an example of a school district's technology use policy that directly states students have no expectation of privacy when using school resources). Five years have passed since Fedders published her study on the surveillance of students in North Carolina schools; software monitoring took on greater significance during the COVID pandemic and has escalated since. *Compare id.* at 1674-77, *with* Keierleber, *supra* note 60.

when using their devices.[82] Students are in no position to object during the school day because they must use computing devices when in class.[83] "Students and their families are backed into corner" because they have no "real choice to opt out of privacy-invading technology."[84]

This makes some sense when students are in class or working on their homework during the school day. This approach is in accord with the Supreme Court's position that schools stand "*in loco parentis, i.e.*, in the place of parents," when "the children's actual parents cannot protect, guide, and discipline them."[85] And yet surveillance companies' monitoring stretches this concept beyond recognition. On behalf of schools, companies are tracking children all the time, including weekends and holidays, when parents have resumed their guardianship role. The justification for school involvement is then at its lowest point.

Not every parent rejects corporate monitoring of children's online activities. It is hard to resist promises that monitoring services protect children from vicious cyberbullying or violence.[86] Parents rightly worry about the sites that students are visiting.[87] Some sites connect children with predators.[88] Others display nonconsensual intimate images.[89] Others host online abuse.[90]

82. Press Release, ACLU of R.I., ACLU of RI Report Shows Alarming Lack of Privacy Protection for Students on School-Loaned Computers (Sept. 21, 2020, 1:30 PM), https://perma.cc/8S27-A35X.

83. *See* ALIM ET AL., *supra* note 31, at 18.

84. *Id.* at 5.

85. Mahanoy Area Sch. Dist. v. B.L., 141 S. Ct. 2038, 2045-46 (2021). Catharine Ward provided invaluable feedback on these and other issues.

86. *See* LAIRD ET AL., *supra* note 9, at 11-12 (noting that "parents and students show the strongest support for student activity monitoring to keep students safe").

87. In a recent hearing, Senators demanded that tech CEOs apologize to families whose children have been harmed on their sites, with executives from Snap and X agreeing to support a federal law that would require online services to take "'reasonable measures' to prevent harm—including online bullying, harassment, sexual exploitation, anorexia, self-harm, and predatory marketing—to minors who use their platforms." Mike Isaac, *Six Takeaways from a Contentious Online Child Safety Hearing*, N.Y. TIMES (Jan. 31, 2024), https://perma.cc/3LDL-ZYZ3.

88. *See, e.g.*, Danielle Keats Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401, 401-02 (2017) (discussing the site Omegle, known to attract predators; *see generally id.* at 414-23 (proposing legal reform so that online service providers have to take "reasonable steps" to address illegality).

89. CITRON, *supra* note 1, at 71 (highlighting research finding thousands of such sites).

90. *See, e.g.*, James Dionne, *People's Dirt is Back and Running*, BLACK & WHITE (Oct. 19, 2009), https://perma.cc/2WCD-A2FS (describing how the gossip website People's Dirt had been used for cyberbullying and posting "negative and hostile" comments about students).

Parents cannot hold site operators responsible if children are harmed on their sites because the sites are shielded from liability for most user-generated content.[91] Parents want to protect their children and student surveillance, they are told, can keep their kids safe.

As Supreme Court justices have emphasized, "America's public schools are the "nurseries of democracy."[92] At school, students learn the skills of debate and values of free expression.[93] The next Part explores how indiscriminate digital surveillance has jeopardized the school's ability to cultivate habits of learning, self-expression, and cooperation, with little proven upside for safety.

II. Undermining Schools as Citizen Incubators

Schools are meant to inculcate learning and communication skills, model effective listening and speaking, and encourage personal growth.[94] As John Dewey emphasized, schools are the foundation of a healthy democratic society.[95] Through education, schools prepare students to participate in public discourse.[96] At school, students learn to express themselves, develop authentic identities, and contribute to culture.[97]

The Supreme Court has recognized the critical role of schools in students' lives. The Court has noted that schools instill "fundamental values of 'habits and manners of civility' essential to a democratic society."[98] As Justice Robert Jackson underscored in *West Virginia State Board of Education* v. *Barnette*, "[t]hat

91. Danielle Keats Citron, *How to Fix Section 230*, 103 B.U. L. REV. 713, 717, 722-24 (2023).

92. Mahanoy Area Sch. Dist. v. B.L., 141 S. Ct. 2038, 2046 (2021).

93. *See* Brown University, *Freedom of Speech in the University*, YOUTUBE, at 41:00-43:45 (Nov. 22, 2016), https://perma.cc/7DHY-JLT8; New Jersey v. T.L.O., 469 U.S. 325, 373 (1984) (Stevens, J., concurring in part and dissenting in part) (explaining that "[s]chools are places where we inculcate the values essential to the meaningful exercise of rights and responsibilities by a self-governing citizenry").

94. *See* Brown University, *supra* note 93, at 41:00-43:45.

95. *See* John Dewey, *The School as Social Center*, 3 ELEMENTARY SCH. TCHR. 73, 75-77, 86 (1902).

96. Joseph Blocher, *Institutions in the Marketplace of Ideas*, 57 DUKE L.J. 821, 870-77 (2008) (explaining that schools, particularly K-12, are viewed as "special speech institutions" because they prepare students to participate in the marketplace of ideas, even if those schools may sometimes limit student speech).

97. *See supra* notes 13-16 and accompanying text; *cf.* Danielle Keats Citron & Helen Norton, *Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age*, 91 B.U. L. REV. 1435, 1443-46 (2011) (emphasizing the importance of online platforms for students to learn the value of citizenship, extending exchanges and discussions at school to online platforms where school groups meet).

98. Bethel Sch. Dist. No. 403 v. Fraser, 478 U.S. 675, 681 (1986) (quoting CHARLES A. BEARD & MARY R. BEARD, NEW BASIC HISTORY OF THE UNITED STATES 228 (William Beard ed., 1968)).

[boards of education] are educating the young for citizenship is reason for scrupulous protection of Constitutional freedoms of the individual, if we are not to strangle the free mind at its source and teach youth to discount important principles of our government as mere platitudes."[99]

Surveillance technologies undermine the project of educating the next generation of democratic citizens. This Part highlights research showing that student surveillance undermines learning, privacy, free expression, and equality. It also exposes the lack of independent evidence showing that student surveillance makes students safer.

A. Harm to Learning

Monitoring and filtering software curbs students' ability to learn from a wide array of resources. As a practical matter, it does not just filter pornography or extreme violence, as schools and companies claim. It tends to over block content, preventing students from visiting news sites, sites with resources for LGBTQ+ teens, and educational materials about sexual health.[100] In a month-long experiment, a *Vice* reporter found that the surveillance platform Bark *primarily* blocked content from news sources like the *Washington Post* and *MIT Technology Review*.[101]

Overly aggressive algorithmic filtering undermines the pursuit of truth, which requires "as few obstacles and as many open vehicles as possible. Everything that enables us to create, acquire and spread knowledge has a special claim to be protected and promoted."[102] Students cannot read what they

99. 319 U.S. 624, 637 (1943). Justin Driver offers a highly detailed conception of schools as laboratories of citizenship. His scholarship masterfully explores the role of public schools in educating young people and the Supreme Court's decisions interpreting students' constitutional rights within elementary and secondary public schools. *See* JUSTIN DRIVER, THE SCHOOLHOUSE GATE: PUBLIC EDUCATION, THE SUPREME COURT, AND THE BATTLE FOR THE AMERICAN MIND 7-23 (2018).

100. Feathers, *supra* note 57; Andrew Hope, *Unsocial Media: School Surveillance of Student Internet Use*, *in* THE PALGRAVE INTERNATIONAL HANDBOOK OF SCHOOL DISCIPLINE, SURVEILLANCE, AND SOCIAL CONTROL 425, 430-31, 437 (Jo Deakin, Emmeline Taylor & Aaron Kupchik eds., 2018). In 2011, the ACLU sued a school district in Missouri after its filtering software blocked sites supporting LGBTQ+ individuals but permitted anti-LGBTQ+ sites. After the school district refused to change the filter, the district court issued a preliminary injunction ordering the school district to discontinue using the internet filtering system as currently devised. Michael Winerip, *School District Told to Replace Web Filter Blocking Pro-Gay Sites*, N.Y. TIMES (Mar. 26, 2012), https://perma.cc/4LBC-HBBH.

101. Todd Feathers, *Schools Spy on Kids to Prevent Shootings, but There's No Evidence It Works*, VICE (Dec. 4, 2019, 6:00 AM), https://perma.cc/J4QH-5YHS.

102. TIMOTHY GARTON ASH, FREE SPEECH: TEN PRINCIPLES FOR A CONNECTED WORLD 152 (2016).

cannot read.[103] Monitoring and filtering software undermines students' ability to discover and learn from sources that would enrich their thinking and capacity for citizenship. The software also denies students' intimate privacy and chills their free expression and trust, a point to which we now turn.

B. Harm to Privacy, Expression, and Trust

Surveillance technologies endanger *student intimate privacy*—the privacy that students need to explore, learn, befriend, and communicate. Students experience enormous personal growth, especially during adolescence.[104] They are particularly vulnerable to feeling judged, misunderstood, and embarrassed.[105] Students need online spaces where they are protected from judgment, where they can try on ideas and identities, and where they can explore friendships.[106]

School surveillance makes it difficult for students to engage in self-expression. Students are less willing to engage in certain expressive activities because they know they are being monitored.[107] According to a 2022 national study, 80% of students surveyed said they are "more careful" about what they search online, and 50% of students surveyed said they do not share their "true thoughts or ideas" online because they are being monitored.[108] As Jonathon Penney has found, in the face of government online surveillance, younger internet users are more cautious in their online activities and searches.[109]

---

103. *Cf. id.* at 163 (noting that "[w]e do not see what we do not see" in relation to what data and information does and does not appear in online searches).

104. *See* VAN MANEN, *supra* note 13, at 8-9, 66, 74 (underscoring that privacy is "especially relevant for the formative growth of children and young people in school" because it enables inner growth, positive autonomy, and personal identity).

105. *See generally id.* at 142-48 (exploring feelings of shame, guilt, and embarrassment when children's private activity is exposed).

106. *See generally* CITRON, *supra* note 1, at 113 (describing judgment-free online and offline spaces as critical to self-development and individuality).

107. *Cf.* Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the "Chilling Effect,"* 58 B.U. L. REV. 685, 689-94 (1978) (defining the "chilling effect" as invidious deterrence of constitutionally protected expression).

108. LAIRD ET AL., *supra* note 9, at 22, 26; *cf.* ERIKSON, IDENTITY, *supra* note 13, at 130 (explaining that "should a young person feel that the environment tries to deprive him too radically of all the forms of expression which permit him to develop and integrate the next step, he may resist.").

109. Jonathon W. Penney, *Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study*, INTERNET POL'Y REV., May 2017, at 1, 14-19, https://perma.cc/L8G4-SL8W; Jonathon W. Penney, *Whose Speech Is Chilled by Surveillance?*, SLATE (July 7, 2017, 7:32 AM), https://perma.cc/E4WP-W6HL.

Parents have told researchers that their children fear talking or typing after administrators scolded them for trying to access certain sites.[110] Parents are concerned that their children will be deterred from engaging in activity that would help them figure out their "identity or what they believe in."[111] These findings echo scholarship foregrounding "intellectual privacy" as central to identity experimentation[112] and emphasizing the risk of compelled conformity when privacy is denied.[113]

Continuous online surveillance jeopardizes the trust that students need to forge relationships with teachers. The Court has emphasized the importance of trust and informality to the development of student-teacher relationships.[114] More than fifty years ago, Arthur Miller predicted that computerized student records would corrode "the student-teacher relationship."[115] Miller explained that students might not confide in teachers if they thought that their discussions would end up in files that might hurt them.[116]

Those insights have grown in importance. According to a 2023 study, when students are told that their activities were flagged by monitoring

110. DHANARAJ THAKUR, HUGH GRANT-CHAPMAN & ELIZABETH LAIRD, CTR. FOR DEMOCRACY & TECH., BEYOND THE SCREEN: PARENTS' EXPERIENCES WITH STUDENT ACTIVITY MONITORING IN K-12 SCHOOLS 9-11 (2023), https://perma.cc/4TW2-D4TQ.

111. *Id.* at 9-10.

112. *See, e.g.*, NEIL RICHARDS, WHY PRIVACY MATTERS 113-20 (2021) (exploring how privacy enables identity expression "on our own terms"); JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 127-52 (2012) (arguing that privacy enables the play of everyday life and identity experimentation); Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 407-26 (2008) (arguing that the protection of intellectual privacy, which encompasses our reading, browsing, sharing, communications, and other online and offline activity, enables self-expression, creativity, and identity development); Marc Jonathan Blitz, *Constitutional Safeguards for Silent Experiments in Living: Libraries, the Right to Read, and a First Amendment Theory for an Unaccompanied Right to Receive Information*, 74 UMKC L. REV. 799, 799-809 (2006); Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1374-77 (2000).

113. *See, e.g.*, Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 465-68 (2015).

114. *See* New Jersey v. T.L.O., 469 U.S. 325, 340 (1985) (recognizing the importance of flexibility in school disciplinary procedures to "preserv[e] the informality of the student-teacher relationship"); *see also id.* at 349 (Powell, J., concurring) ("The special relationship between teacher and student also distinguishes the setting within which schoolchildren operate.").

115. ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 112 (1971).

116. *See id.* Several years after Miller, Aryeh Neier raised similar concerns that when teachers included derogatory comments about students in school dossiers, it transformed teachers into "adversaries of the child." ARYEH NEIER, DOSSIER: THE SECRET FILES THEY KEEP ON YOU 27 (1974).

software, they grow distrustful of their schools and teachers.[117] Students are "cognizant of being monitored" and "alter what they say around teachers, avoiding private conversations to prevent 'getting in trouble' or having a negative outcome (e.g., telling parents)."[118] The use of monitoring software "represents a "form of control" that make students feel singled out and watched.[119] When teachers talk to students about their online activities that monitoring software has flagged as problematic, students feel like they are being accused of wrongdoing, even if that is not the case; the rapport suffers because students no longer trust their teachers to protect their interests.[120] The "interpersonal dynamics in the classroom" are also negatively impacted.[121]

Student surveillance risks teaching students that totalizing surveillance is acceptable and inevitable. In *New Jersey* v. *T.L.O.*, Justice Stevens warned that allowing a school administrator to search a high school student's purse for the minor offense of smoking taught "a curious moral for the Nation's youth"—that their privacy could be invaded for "nothing more than a minor infraction."[122] A more troubling lesson is that students must "accept constant monitoring as the normal state of affairs in everyday life."[123] In 2005, 1,500 students at a large public school in the Bronx, New York staged a walkout to protest metal detectors and security cameras in school.[124] The school's refusal to budge sent a depressing and disturbing message to students: Privacy is not yours, and no matter what you say, nothing can be done about it.[125]

---

117. THAKUR ET AL., *supra* note 110, at 11-12.

118. MARLOW ET AL., *supra* note 6, at 23.

119. THAKUR ET AL., *supra* note 110, at 11-12; *see also* EMMELINE TAYLOR, SURVEILLANCE SCHOOLS: SECURITY, DISCIPLINE AND CONTROL IN CONTEMPORARY EDUCATION 67 (2013) (noting that "a large proportion of pupils equated surveillance with mistrust" and felt the surveillance was "criminalising them").

120. THAKUR ET AL., *supra* note 110, at 11-12.

121. *Id.*

122. 469 U.S. 325, 384-86 (1985) (Stevens, J., concurring in part and dissenting in part) (noting that the school is the first place where people experience the power of government and learn "cherished ideals" of the Fourth Amendment that government may not intrude on personal privacy without a warrant or compelling circumstance). The Court in *T.L.O.* found that while the Fourth Amendment affords students some protections in schools, student searches should be governed by the less demanding standard of reasonable suspicion. *Id.* at 336-37, 341-43.

123. Anya Kamenetz, *Software Flags 'Suicidal' Students, Presenting Privacy Dilemma*, NPR (Mar. 28, 2016, 7:00 AM ET), https://perma.cc/7SL7-9P98.

124. Jen Weiss, *Valuing Youth Resistance* Before and After *Public Protest*, 24 INT'L J. QUAL. STUD. EDUC. 595, 596-97 (2011).

125. *See id.* at 597.

Some students try to resist the surveillance by using coded messages, fake names, and other techniques to protect their privacy.[126] Students whose families can afford to buy personal devices are able to evade tracking when they are not at school.[127] This connects to another harm of student surveillance—the disproportionate impact on students from marginalized groups.

C. Harm to Equality

The most surveilled students are often the most vulnerable. Students from low-income families use school-provided devices at home and on weekends; unlike students from wealthy backgrounds, their families cannot afford to buy personal devices.[128] A national survey showed 6 in 10 Hispanic students, 6 in 10 Black students, 7 in 10 rural students, and 7 in 10 students from low-income families rely on school-issued devices.[129] Schools seemingly recognize the punitive nature of the arrangement: One school district has a "lease to own" program for school devices that gives families who purchase devices the option to *turn off monitoring software outside of school hours*.[130] Thus, families who can afford to purchase devices are able to limit student surveillance in ways that families who cannot do so.[131] This program promotes inequitable outcomes for low-income students.

Students from traditionally subordinated groups are more likely to censor themselves in the face of constant surveillance. For example, students with learning differences or physical disabilities are more likely than their peers to suppress their true thoughts online because they know they are being monitored.[132] As a result, these students are less likely to use online tools to seek help.[133] These findings are amplified by student journalists. The editorial board of a student magazine at a public high school in Austin, Texas objected to monitoring software because, "[r]ather than focusing on mental health support, in practice, Gaggle takes on more of a disciplinary nature. As opposed to getting the professional help they need, students may instead be in fear of

126. *See* Ceres, *supra* note 56 (urging students to avoid using school laptops to search for sensitive topics like health and to meet with friends in person to discuss such topics rather than communicate online); DANAH BOYD, IT'S COMPLICATED: THE SOCIAL LIVES OF NETWORKED TEENS 45-47 (2014) (discussing how teenagers use coded words and fake names on social media so friends can find them without increasing visibility to adults).

127. WARREN & MARKEY, *supra* note 75, at 6-7.

128. *Id.*

129. LAIRD ET AL., *supra* note 9, at 23.

130. *See* WARREN & MARKEY, *supra* note 75, at 7.

131. *Id.*

132. LAIRD, *supra* note 33, at 5-8.

133. *See id.*

punitive action and not reach out or get help at all."[134] Surveillance companies acknowledge this risk, perhaps unwittingly. For example, Gaggle said of a student the company identified as suicidal: "The student now realizes the importance of being cautious [with] how you express yourself in an email."[135]

Student surveillance has an adverse impact on LGBTQ+ students' expression, physical safety, and emotional well-being.[136] LGBTQ+ students, who often rely on the internet for educational and community resources, may refrain from consulting online sources related to gender and sexual orientation because they fear reprisal.[137] Their fear is warranted. Approximately 29% of LGBTQ+ students reported that they or someone they know had been involuntarily "outed" due to monitoring technology.[138] Surveillance software risks "expos[ing] the privacy of trans students who are at the greatest risk of suicide."[139]

Parents who learn about their children's sexual orientation or gender identity from schools may be precisely the people who children do not want to know.[140] Some parents reject their children's sexual orientation or gender identity; they physically and emotionally abuse their children; they kick them out of the house.[141] As a student told the privacy think tank Future of Privacy, "[I] wasn't safe at home to come out so school was really the only place I could actually do research safely."[142] We should not assume that children's interests are aligned with parents' interests.

Student surveillance increases the risk that minority students will face discipline and suspension. In a national survey, 78% of teachers say that students have been flagged by activity monitoring software for disciplinary action and 59% report that a student has actually been disciplined due to monitoring.[143] Disciplinary action fell disproportionately on non-White

134. Shield Ed. Bd., *Safety Measure Crosses Line Between Security, Privacy*, SHIELD (Dec. 10, 2021), https://perma.cc/Q5JE-TYZG.

135. Fedders, *supra* note 77, at 1703 (quoting *Warsaw Community Schools: How Much is Student Safety Worth? Responding to Cries for Help*, GAGGLE, https://perma.cc/UN8X-HWT7 (archived May 1, 2024)).

136. *See* LAIRD ET AL., *supra* note 9, at 21; GOROSH, *supra* note 7, at 6-10.

137. GOROSH, *supra* note 7, at 6-10 ("Monitoring technologies . . . ironically have a strong potential to undercut online access to care and critical resources.").

138. LAIRD ET AL., *supra* note 9, at 21.

139. Alejandra Caraballo, *Remote Learning Accidentally Introduced a New Danger for LGBTQ Students*, SLATE (Feb. 24, 2022, 9:00 AM), https://perma.cc/B7JQ-LXRC.

140. *See* Barbara Fedders, *Coming Out for Kids: Recognizing, Respecting, and Representing LGBTQ Youth*, 6 NEV. L.J. 774, 787-89 (2006).

141. *Id.* According to a 2020 survey by the Trevor Project, "29% of LGBTQ+ youth have experienced homelessness, been kicked out of their homes, or have run away." GOROSH, *supra* note 7, at 7.

142. *Id.*

143. LAIRD ET AL., *supra* note 9, at 24.

students, with 48% of Black students and 55% of Hispanic students reporting that they or someone they know got in trouble, compared to 41% of White students reporting the same.[144] According to the ACLU, "LGBTQ+ students are overrepresented in school disciplinary incidents."[145]

School surveillance sends the demeaning message that students from traditionally subordinated groups cannot be trusted. In a study of public schools in Maryland, researchers found that security cameras placed inside schools made students, especially Black students, feel as if "Big Brother is watching them."[146]

Youth criminalization is another risk of student surveillance. Black students already face a greater risk of criminalization related to school activities than White students—surveillance tools exacerbate the problem.[147] Sexual and gender minorities also are more likely to face criminal investigations; around 31% of LGBTQ+ students reported that they or someone they knew had been contacted by a police officer or other adult about possibly committing a crime, as opposed to 19% of non-LGBTQ+ students reporting the same.[148] Student surveillance tools could be used to provide evidence of abortions in states where abortion is illegal. In the wake of *Dobbs v. Jackson Women's Health Organization*,[149] female students risk discipline and criminalization if their online searches, browsing, or purchases suggest that they obtained an abortion in violation of state law.[150] Student surveillance also could be weaponized against teens seeking reproductive care.[151]

---

144. *Id.*

145. GOROSH, *supra* note 7, at 9.

146. Jane Kelly, *Do Security Cameras in Public Schools Make Students Feel Safer?*, UNIV. OF VA. SCH. OF EDUC. & HUM. DEV. (Jan. 29, 2019), https://perma.cc/C8J9-XCTZ.

147. *See* LAIRD ET AL., *supra* note 9, at 23-24; KRISTIN HENNING, THE RAGE OF INNOCENCE: HOW AMERICA CRIMINALIZES BLACK YOUTH, at xvii (2021) ("There are now generations of Black youth who have grown up under the constant surveillance and persistent threat of abuse by the police . . . . Black youth are stopped and harassed by the police for doing what teenagers do all over the world—talking on the phone, laughing with friends, shooting hoops at the local recreation center, flirting with a classmate on social media, or posting political views online.").

148. LAIRD ET AL., *supra* note 9, at 21.

149. 142 S. Ct. 2228 (2022).

150. *See* CODY VENZKE, CTR. FOR DEMOCRACY & TECH, HIDDEN HARMS: STUDENT ACTIVITY MONITORING AFTER ROE V. WADE, 1 (2022), https://perma.cc/NS9Q-9SBM; Daly Barnett, *Mandatory Student Spyware Is Creating a Perfect Storm of Human Rights Abuses*, ELEC. FRONTIER FOUND. (June 8, 2022), https://perma.cc/WM7J-JWY4 (noting that "students who use their devices to research trans healthcare or abortion related material could find those devices weaponized against them, potentially resulting in criminal charges").

151. Todd Feathers, *After Dobbs, Advocates Fear School Surveillance Tools Could Put Teens at Risk*, MARKUP (July 8, 2022, 8:00 AM ET), https://perma.cc/96UJ-7GUA.

In all of these ways, student surveillance undermines the ability of schools to provide what Robert Post calls "democratic education."[152] Constant surveillance chills students' exploration of ideas, expression, and communication with peers and teachers. To be sure, schools have a legitimate interest in ensuring students' physical safety during the school day and protecting them from online and offline bullying that can make learning impossible. The next question is whether student surveillance serves that legitimate interest.

D. Are Students Safer?

Safety is the central justification for digital surveillance, but there is little evidence that it fulfills that goal. Independent research is scant because companies are closed books.[153] The computer science literature offers some insights on the general question of whether machine learning systems can reliably predict certain kinds of harmful activities. Research has shown that algorithms cannot accurately detect self-harm because context is difficult to assess.[154] Algorithmic alerts may be over- or under-inclusive; we simply do not know for sure.[155]

Investigative journalists have provided insight into whether surveillance platforms can accurately and reliably distinguish destructive bullying from genuine joking or threats of self-harm from productive questioning. Reporters have interviewed surveillance companies' content moderators and found that they lack experience in "school safety, security, or mental health."[156] Content moderators face enormous pressure to review content quickly. Gaggle safety team members reportedly must review 300 incidents per hour, giving them seconds to look at any given alert.[157] The time pressure facing moderators and the scale of content being tagged raises serious questions as to whether surveillance systems are catching real problems like self-harm, bullying, and violent threats or instead overwhelming schools with false positives.

---

152. Robert Post, Essay, *Theorizing Student Expression: A Constitutional Account of Student Free Speech Rights*, 76 STAN. L. REV. 1643, 1655 (2024).

153. Fedders, *supra* note 77, at 1701-06.

154. SARA COLLINS, JASMINE PARK, ANISHA REDDY, YASAMIN SHARIFI & AMELIA VANCE, FUTURE OF PRIV. F., THE PRIVACY AND EQUITY IMPLICATIONS OF USING SELF-HARM MONITORING TECHNOLOGIES: RECOMMENDATIONS FOR SCHOOLS 11 (2021), https://perma.cc/LS8P-NKEE.

155. *See* Mark Keierleber, *Gaggle Surveils Millions of Kids in the Name of Safety. Targeted Families Argue It's 'Not That Smart,'* THE 74 (Oct. 12, 2021), https://perma.cc/A5AW-3JXE.

156. Mark Keierleber, *Meet the Gatekeepers of Students' Private Lives*, THE 74 (May 2, 2022), https://perma.cc/R5HZ-U4LR.

157. *Id.*

Companies offer their own accounts of the efficacy of their surveillance tools. When asked by Senators Elizabeth Warren, Ed Markey, and Richard Blumenthal to substantiate their claims of efficacy, surveillance companies pointed to large numbers of alerts and anecdotal success stories.[158] Gaggle claimed that it had alerted over 1,500 school district partners of more than 235,000 occasions where student communications suggested self-harm or harm to peers or teachers.[159] The company provided several examples of alerts that led to schools assisting students as well as laudatory quotes from school officials.[160]

Alert numbers and anecdotes, without more, reveal little about the reliability and accuracy of these surveillance systems. Surveillance companies have not addressed if any of the thousands of alerts involved false positives or false negatives. Nor have they suggested that they checked with schools to see if prior alerts were accurate and helped students. Companies could coordinate with schools to see what happened with a sample size of reports to check for accuracy or disparate impact on marginalized communities, but from what we can tell, there has been no auditing.[161]

Investigative reporting casts doubt on some corporate claims. In 2021, *Vice* asked Bark to support its claim that it had prevented sixteen school shootings.[162] After refusing to provide evidence, the company removed the statistic from the top of its homepage.[163]

Consider Social Sentinel, which promotes its service as having the ability to identify social media threats and thus help prevent tragedies from occurring. The Uvalde, Texas school district was using Social Sentinel when a former student shot and murdered nineteen children and two teachers and injured seventeen others at Robb Elementary School.[164] JP Guilbault, CEO of

158. Letter from Jeff Patterson, *supra* note 21, at 1-3.

159. *Id.* at 1.

160. *Id.* at 1-3.

161. Senators Warren and Markey have pointed out that companies are not monitoring the disparate impact of their technologies on marginalized groups. WARREN & MARKEY, *supra* note 75, at 3.

162. Feathers, *supra* note 57.

163. The company tried to explain away the demotion of that statistic by saying that it rotated statistics on the homepage, but the homepage was saved thirty-nine times by the Internet Archive and the school-shooting statistic appeared prominently each time until *Vice* asked for proof. *Id.*

164. Emily Baucum, *The High-Tech Software 1 in 4 Schools—Including Uvalde—Uses to Scan for Threats*, FOX SAN ANTONIO (June 8, 2022, 10:11 PM), https://perma.cc/ZY7C-E8H9; Bernard Condon, *Uvalde School Shooter Left Trail of Warning Signs Ahead of Attack*, PBS NEWS HOUR (July 19, 2022, 11:16 AM EDT), https://perma.cc/HF65-GHJV; Stephen Groves & Adriana Gomez Licon, *'Day by Day:' Uvalde Survivors Recover from Wounds, Trauma*, ASSOCIATED PRESS (June 2, 2022, 9:50 AM PDT), https://perma.cc/Y3CW-RTU5.

Navigate360—which owns Social Sentinel—suggested that it was no fault of the software because it only scans students' public social media posts and could not detect the shooter's rage-filled private chats.[165] That explanation was less an absolution than an admission that Social Sentinel's surveillance business is more "security theater" than actual help. Persistently tracking students' public social media activity undermines free speech values and, as the Uvalde tragedy shows, may be an ineffective tool with little safety upside.

The next Part explains why current law does not protect student intimate privacy and offers suggestions for reform.

III. A Plan for Reform

Rather than incentivizing schools to engage in activities that cultivate an engaged and informed citizenry, the law, or at least its interpretation, is being used to undermine that possibility. This Part begins by describing the law's failure to protect student intimate privacy and free expression. Then, I consider potential reforms that would help ensure that surveillance technologies make students safer, are designed to minimize harms to students, and allow parents, students, and other community stakeholders to have a say. The final suggestion involves imposing a duty of nondiscrimination on surveillance companies.

A. Law's Failure

Local education agencies insist that surveillance tools are required by the federal Children's Internet Protection Act of 2000 (CIPA),[166] given its mandate to filter obscene content.[167] Under CIPA, schools receiving internet access at a federally discounted rate must have a "policy of Internet safety" that protects students from accessing material with obscene visuals, child exploitation, or images harmful to minors.[168] CIPA says that such a policy should include "monitoring the online activities of minors."[169]

165. Baucum, *supra* note 165; *JP Guilbault: Chief Executive Officer*, NAVIGATE360, https://perma.cc/J4JG-49Z3 (archived May 10, 2024).

166. Pub. L. No. 106-554, 114 Stat. 2763 (codified as amended at 20 U.S.C. § 9134 and 47 U.S.C. § 254).

167. DEVAN L. HANKERSON, CODY VENZKE, ELIZABETH LAIRD, HUGH GRANT-CHAPMAN & DHANARAJ THAKUR, CTR. FOR DEMOCRACY & TECH., ONLINE AND OBSERVED: STUDENT PRIVACY IMPLICATIONS OF SCHOOL-ISSUED DEVICES AND STUDENT ACTIVITY MONITORING SOFTWARE 11 (2021), https://perma.cc/NBN2-LMND; WARREN & MARKEY, *supra* note 75, at 9.

168. 47 U.S.C. § 254(h)(5)(B)(i).

169. *Id.*

Schools misconstrue this statute, using it to justify student surveillance. The history, purpose, and text of CIPA do not support indiscriminate and continuous tracking of children's online activities.

When CIPA was passed in 2000, teachers were best situated to prevent students from accessing harmful material during the school day. At that time, computers in schools were kept in special rooms like computer labs or learning resource centers.[170] Computers were bulky, heavy, and expensive—nothing like today's portable laptops, tablets, and smart phones. Public schools had a limited number of computers; teachers oversaw the use of those computers. Senator Leahy expressed skepticism about the need for the bill because, as he noted, "not too many kids are going to go pulling up inappropriate things on the web sites when their teachers, their parents, and everybody else are walking back and forth and looking over their shoulder."[171]

CIPA was designed to address children's online safety while students were physically in school. Lawmakers never contemplated that students would be given individual computing devices that they could take home and use on weekends and holidays. Members of Congress did not imagine or license the large-scale, continuous, and indiscriminate surveillance of students' online activities.

Schools that point to CIPA's internet safety policy and monitoring provision to justify utilizing private surveillance services ignore a clear provision in CIPA: This "Disclaimer Regarding Privacy" provides: "*Nothing in this title or the amendments made by this title shall be construed to require the tracking of Internet use by any identifiable minor or adult user.*"[172] Advocacy groups have highlighted this statutory language in urging Congress to clarify that CIPA's monitoring requirement does *not* mandate "broad, invasive, and constant surveillance of students' lives online."[173] Although the Federal Communications Commission (FCC) is charged with interpreting and enforcing CIPA, it has not addressed concerns raised by advocates.[174]

Students' educational records enjoy some privacy protections under federal law, but that law does little to constrain student digital surveillance. The Family Educational Rights and Privacy Act of 1974 (FERPA)[175] limits

170. *See* Hope, *supra* note 100, at 429.

171. 146 CONG. REC. S5844 (daily ed. June 27, 2000) (statement of Sen. Leahy).

172. 47 U.S.C. § 254 note (emphasis added).

173. Letter from Ctr. for Democracy & Tech., et al. to Members of House & Senate Com. Comms. (Sept. 21, 2021), https://perma.cc/AHA2-HQ6V.

174. *See generally id.* (describing concerns).

175. Pub. L. No. 93-380, tit. 5, § 513(a), 88 Stat. 571 (codified as amended at 20 U.S.C. § 1232g).

access to student education records by third parties, including employers.[176] Under FERPA, however, schools may disclose students' personally identifiable information, including digital activity and data, to third parties designated as "school officials" if they assist schools in providing institutional services and have "legitimate educational interests" in the records.[177] Schools can categorize private surveillance companies as "school officials" to enable surveillance companies to access students' intimate lives.[178]

Much like federal law, state law provides little protection against third-party surveillance of students' online activities. Most state student privacy laws do not apply to corporate access to and monitoring of school-provided laptops. The Minnesota Student Data Privacy Act (MSDPA)[179] is the only state law that explicitly addresses the monitoring of students on school-issued devices, and even that law offers little help. MSDPA prohibits government entities or technology providers from monitoring student interactions with school-issued devices, including web-browsing activity.[180] But the law guarantees its own irrelevance by exempting "activity . . . necessary to comply with federal . . . law," and "activity . . . necessary to participate in federal funding programs."[181] Those exemptions make it easy for Minnesota schools to say that their surveillance programs are required under CIPA.[182]

176. Elana Zeide, *Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPs*, 8 DREXEL L. REV. 339, 354-58 (2016) (online corrected) (describing FERPA's history and procedural commitments).

177. *See id.* at 359 (quoting 34 C.F.R. § 99.31(a)(B)(1)). As Elana Zeide explains, FERPA allows schools to share student data with third parties deemed "school officials"—defined as parties that perform "an institutional service or function" for which employees otherwise would be used—that have "'legitimate educational interests' in the education records, as defined by the school or district in its annual notification of FERPA rights." *Id.* (quoting 34 C.F.R. § 99.31(a)(B)(1)). "School officials" may not further disclose covered information unless there is an understanding that they may do so on the school's behalf. *Id.* However, aside from these guardrails, schools have "broad discretion and minimal transparency obligations" under the "school official" exception. *Id.* They have wide latitude to decide which outside parties count as "school officials" and do not have to document disclosure to those third parties. *Id.* at 360-61. To illustrate the point, Professor Zeide notes that teachers may share student educational records with "free apps without any documentation or institutional oversight." *Id.* at 361.

178. *See* Fedders, *supra* note 77, at 1683-84.

179. 2022 Minn. Laws ch. 69.

180. S. 2307, 92d Leg., Reg. Sess. 8056 (Minn. 2022).

181. *Id.*

182. *See, e.g.*, *524 Policy: Student Technology and Internet Access and Acceptable Use*, STILLWATER AREA PUB. SCHS., https://perma.cc/A8K4-5KLF (last updated Dec. 20, 2022) (noting that the district is subject to CIPA, and therefore, "required to comply with additional standards in restricting possible access to inappropriate materials," which means that it will "monitor online activities . . . by all users on the network.").

In the face of this regulatory vacuum, lawmakers must consider reforms that protect student intimate privacy, free expression, and equality, if schools and districts continue to contract with private surveillance companies to monitor student online activity.

B. First Step in Reform: Proof of Concept, Harm Minimization, and Stakeholder Involvement

Lawmakers could ban public schools from using digital surveillance technologies given the harms and unproven benefits. The Biden Administration's proposal for an AI Bill of Rights takes the position that "[c]ontinuous surveillance and monitoring should not be used in education."[183]

We need regulatory reform in the strong likelihood that lawmakers do not ban schools from using digital surveillance technologies. I remain open to the possibility that student surveillance *could* be conducted in a manner that minimizes harms to students and maximizes their safety. Federal and state lawmakers must adopt reforms designed to ensure that surveillance products actually make students safer and that they minimize the harm to student intimate privacy, expression, and equal opportunity.

Let's first consider federal reform. First, Congress should revise CIPA to make clear that the "monitoring" provision does not require tracking students' online activity to obtain federal funding for internet access.[184] Alternatively, the FCC has rulemaking authority over CIPA and could make clear that CIPA does not mandate continuous, indiscriminate surveillance of students' online activities.[185] But far more must be done. Not only should Congress be clear that indiscriminate and continuous digital monitoring is not required; Congress should *regulate* such monitoring.

The precautionary principle should animate the federal approach. The precautionary principle is as follows: "When an activity raises threats of harm to human health or the environment, precautionary measures should be taken even if some cause and effect relationships are not fully established scientifically. In this context the proponent of an activity, rather than the public, should bear the burden of proof."[186] CIPA should be amended to make clear that schools using federal discounts for internet service can adopt surveillance technologies *only if* those technologies are independently shown

183. OFF. SCI. & TECH. POL'Y, WHITE HOUSE, BLUEPRINT FOR AN AI BILL OF RIGHTS: MAKING AUTOMATED SYSTEMS WORK FOR THE AMERICAN PEOPLE 6 (2022), https://perma.cc/5Z77-WNYE.

184. *See* Letter from Ctr. for Democracy & Tech., *supra* note 173.

185. *See supra* notes 172-74 and accompanying text.

186. *Wingspread Conference on the Precautionary Principle*, SCI. & ENV'T HEALTH NETWORK (Aug. 5, 2013), https://perma.cc/RJ39-PD8D.

(1) to be effective, and (2) to minimize harms to student intimate privacy, expression, and equality. Knowing that federal discounts are on the line, schools will have strong reason to demand proof that corporate surveillance technologies solve the problems that schools want solved (like detecting self-harm, bullying, and threats), and that they are designed to minimize harms to student intimate privacy, free expression, and equality.

This approach would effectively shift the burden to companies to show their proof of concept. Schools considering surveillance products would ask for evidence that a company's surveillance programs are effective in addressing the school's specific goals and are designed to minimize harm to privacy, expression, and equality. Companies would not be able to rely on anecdotes and laudatory quotes from friendly school superintendents. They would have to test their products for efficacy and accuracy before obtaining school contracts. They would have to assess the risks to privacy, expression, and equality and to minimize those risks to the greatest extent possible. Companies would have to monitor their products to ensure that their part of the deal is kept.

Reform also should come from state or local lawmakers. State or local lawmakers should require transparency and oversight over the processes that result in student surveillance. Schools should be required to make public the purpose of student surveillance services, the extent to which students' lives would be monitored, and the steps being taken to protect privacy, free expression, and equality. The details of the contracting process and the terms of contracts should be out in the open. Companies should be required to provide schools with independent evaluations about the efficacy of their products and their harm reduction efforts; schools should be required to release the results of those independent assessments.[187] School districts should be required to give stakeholders—especially students—an opportunity to provide input before surveillance products are adopted and contracts are signed.

Why not trust school districts to take care of this themselves? I am not convinced that they will change their ways unless lawmakers intervene. Perhaps cities and counties might adopt rules to rein in these practices and ensure transparency and oversight. As my colleague Richard Schragger has astutely explored, city government has enormous potential and promise to experiment with policymaking.[188] Indeed, some city governments are experimenting with innovative policies to improve their citizens' lives and to

187. *See generally* Andrew D. Selbst, *An Institutional View of Algorithmic Impact Assessments*, 35 HARV. J. L. & TECH. 117, 122-135 (2021) (explaining that algorithmic impact assessment requirements require firms to consider social impacts of systems and work to mitigate them before development and to document decisions and testing).

188. *See* RICHARD SCHRAGGER, CITY POWER: URBAN GOVERNANCE IN A GLOBAL AGE 2-4 (2016).

reduce inequality.[189] City officials might step in where state lawmakers do not. I encourage them to do so.

C. Second Step: Duty of Nondiscrimination

My second proposal draws on my work calling for a comprehensive federal privacy law that treats intimate privacy as a civil right. In *The Fight for Privacy*, I argue that "Congress should adopt privacy legislation that obligates entities to act as data guardians."[190] One aspect of that proposal is essential here: a duty of nondiscrimination.[191]

Consider surveillance companies' responses to congressional inquiries into whether they have addressed potential bias in their training data and algorithmic models. Gaggle explained that its "algorithm reviews anonymous content, so we have no context or background on students when we first identify potential issues," and that its "algorithms are created and trained from de-identified student communication."[192] The company seemed to be saying that it was technically impossible to test its training data and algorithms for bias. In the company's view, "[r]eviewers trained for unintended bias is [sic] the most effective way to mitigate for bias."[193] GoGuardian similarly replied that it "cannot currently perform rigorous and precise analyses of algorithmic biases related to student-level demographic or socio-economic data."[194] Senators Warren and Markey did not accept these evasive answers; they demanded that companies analyze their algorithms and training data for bias and to track whether their products under- or over-identify certain groups of students, including LGBTQ+ students.[195]

If federal privacy law imposed a duty of nondiscrimination backed by clear regulation from agencies like the Department of Education, then those responses would not be sufficient. To ensure that they could satisfy a duty of nondiscrimination if challenged by state and federal regulators, companies would surely test their products to ensure that they do not disproportionately

189. *See id.* at 16-17 (explaining that cities have creatively responded to challenges facing residents including poverty, sustainability, and more).

190. CITRON, *supra* note 1, at 156.

191. *See id.*

192. Letter from Jeff Patterson, *supra* note 21, at 7. Gaggle says that its safety team supervisors "regularly review alerts to ensure that the Gaggle Safety Team produces accurate and unbiased decisions." *Id.*

193. *Id.* at 8.

194. Letter from Advait Shinde, CEO & Co-Founder, GoGuardian, to Senators Warren, Markey & Blumenthal 7 (Oct. 26, 2021), https://perma.cc/T4ZS-YNCQ.

195. *See* WARREN & MARKEY, *supra* note 75, at 3, 10. Ironically, the companies claimed that privacy concerns prevented them from assessing the impact of their services. *Id.* at 7.

harm protected communities. Companies could not wave away concerns by saying they do not analyze the impact of their surveillance services on protected classes. The notion that privacy concerns make it impossible for surveillance companies to assess risk and mitigate harm[196] is absurd; they are monitoring—in bulk, indiscriminately and continuously—all of students' online activities.

That duty should be paired with agency rulemaking power and remedies. Surveillance companies should be required to defend their practices to federal agencies like the Department of Education and the FCC as well as state attorneys general.[197] Federal and state law enforcers should be given power to bring actions and seek civil penalties.[198] In addition, students and their families "should be able to bring lawsuits against companies that fail to adhere to those rules via 'private rights of action.'"[199] Companies would have to design their surveillance tools with that duty in mind and be prepared to provide proof of compliance to private litigants, state attorneys general, and federal law enforcers. This duty would be a part of a more comprehensive federal privacy law that would protect intimate privacy as a civil right.[200]

Existing civil rights law might provide some support for a duty of non-discrimination. The Center on Democracy and Technology, along with other advocacy groups, has urged the Office of Civil Rights of the U.S. Department of Education to investigate the discriminatory impact of schools' online monitoring of students of color, LGBTQI+ students, and students with disabilities.[201] The groups argued that "[s]tudent activity monitoring is subjecting protected classes of students to increased discipline and interactions with law enforcement, invading their privacy, and creating hostile environments for students to express their true thoughts and authentic identities."[202] They also urged the Office of Civil Rights to issue a policy statement condemning the use of student monitoring software and to state its intent to take enforcement actions against violations that result in discrimination.[203] And yet here we are with no movement. My reform

196. *See supra* note 195.

197. *See generally* WARREN & MARKEY, *supra* note 75, at 10 (proposing roles for the Department of Education and FCC in overseeing monitoring tools).

198. CITRON, *supra* note 1, at 163.

199. *Id.*

200. CITRON, *supra* note 1, at 119-25.

201. Letter from Ctr. for Democracy & Tech., et al. to Catherine E. Lhamon, Assistant Sec'y for C.R., U.S. Dept. of Educ. (Aug. 2, 2022), https://perma.cc/L36P-EJZ5.

202. *Id.* at 3.

203. *Id.*

proposal would expand the number of enforcers on the beat, which in turn could lead to progress.

Conclusion

Student mental health, bullying, and violence prevention are hard problems. Name any thorny issue, and digital tools are posited as *the* solution.[204] School districts with limited budgets are seduced by promises of easy fixes. Surveillance software companies obtain funding and fees, no matter the results.[205]

Schools are meant to be centers of learning, discourse, and community. They are where adolescents learn to listen and speak—where students learn how to be citizens. But schools cannot encourage student expression by indiscriminately and continuously surveilling it. The damage to students' intimate privacy, free expression, and equality is profound while the benefits to student safety are unproven. We need to ensure that schools only use surveillance tools that have been independently shown to make students safer and that those tools are designed to minimize the harm to privacy, free expression, and equality.

We need to act now so students hear that their intimate privacy and free expression matter, that their schools and teachers are on their side, that they are going to be protected rather than suspected. Students need to develop the skills of citizenship—skills that are crucial at a time of distrust about what our eyes and ears are telling us.[206] Students are our future. We need to protect their intimate privacy to enable them to develop ideas, acquire knowledge, and freely express themselves.

204. On tech "solutionism," see Evan Selinger, *The Delusion at the Center of the A.I. Boom*, SLATE (Mar. 29, 2023, 10:00 AM), https://perma.cc/YLD9-Y23E.

205. For example, in August 2021, private equity firm Tiger Global Management invested $200 million in GoGuardian, which was valued at over $1 billion. Mark Bergen, *Tiger Global Plows $200 Million into EdTech Firm GoGuardian*, BLOOMBERG (Aug. 5, 2021, 5:00 AM PDT), https://perma.cc/FKR4-X52U.

206. *See generally* Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753 (2019) (warning of the harms associated with deep fakes).