Washington Law Review

Volume 99 | Number 1

3-1-2024

The Kids Are Not Alright: Negative Consequences of Student Device and Account Surveillance

Ashley Peterson
University of Washington School of Law

THE KIDS ARE NOT ALRIGHT: NEGATIVE CONSEQUENCES OF STUDENT DEVICE AND ACCOUNT SURVEILLANCE

Ashley Peterson*

Abstract: In recent years, student surveillance has rapidly grown. As schools have experimented with new technologies, transitioned to remote and hybrid instruction, and faced pressure to protect student safety, they have increased surveillance of school accounts and school-issued devices. School surveillance extends beyond school premises to monitor student activities that occur off-campus. It reaches students' most intimate data and spaces, including things students likely believe are private: internet searches, emails, and messages. This Comment focuses on the problems associated with off-campus surveillance of school accounts and school-issued devices, including chilling effects that fundamentally alter student behavior, reinforcement of the school-to-prison pipeline, and disproportionate impacts on certain groups—including low-income students, LGBTQIA2S+ students, and students with disabilities. This Comment argues that the current legal landscape—federal and state laws, the Fourth Amendment, and the First Amendment—inadequately protects student privacy.

Drawing on aspects of existing privacy frameworks, this Comment proposes solutions that could be implemented by the Supreme Court, federal and state legislators, and school districts. All of these solutions aim to increase student privacy protections. First, the Supreme Court should clarify whether speech on school-issued devices is protected by adopting clear categories of "school speech" that are subject to discipline. Second, new federal and state protections could bolster student privacy. Such laws should limit data sharing when collected from school-issued devices used at home, mandate data minimization and further limitation of data collected, and implement mandatory tracking of the impacts of student surveillance. Third, school districts should conduct audits and increase transparency to demonstrate their commitment to protect student privacy.

INTRODUCTION

Today's students have never known a world without technology. In particular, computers and the internet permeate all aspects of students' lives.[1] The pervasiveness of this technology extends to a wide range of activities, from educational (e.g., interacting with educational technology aimed at helping students learn) to personal (e.g., using social media or

*J.D. Candidate, University of Washington School of Law, Class of 2024. Thank you to Professor Mike Hintze for his insight and guidance, my colleagues on *Washington Law Review* for their thoughtful edits, and my family and friends for their encouragement and support as I work toward achieving my goals.

1. *See Children's Internet Access at Home*, NAT'L CTR. FOR EDUC. STAT., https://nces.ed.gov/programs/coe/indicator/cch/home-internet-access [https://perma.cc/S3B7-AWQ2] (last updated Aug. 2023).

playing online games).[2] In recent years, a market has emerged for surveillance companies that monitor school-issued devices and accounts, including four main players: GoGuardian, Gaggle, Bark, and Securly.[3]

School districts have increased monitoring of students to satisfy "perceived legal requirements" and protect student safety.[4] This surveillance became even more prevalent as students moved to remote education during the coronavirus (COVID-19) pandemic, using school-issued devices and accounts for learning at home.[5] Even as most students return to in-person instruction, school districts continue to use software to monitor school-issued devices and accounts.[6]

This Comment focuses on the unique privacy implications that arise from student use of school accounts and school-issued devices off school premises. In contrast to social media monitoring and school video cameras, which surveil only public platforms and in public spaces, surveillance of school accounts and school-issued devices focuses on communication that students likely believe to be at least partially private.[7] This surveillance includes searches, emails, and messages.[8] In particular, surveillance of school accounts and school-issued devices, when conducted while students are not physically on school premises, infringes on students' most intimate data and spaces.[9]

---

2. *See* Brooke Auxier, Monica Anderson, Andrew Perrin & Erica Turner, *Parenting Children in the Age of Screens: Children's Engagement with Digital Devices, Screen Time*, PEW RSCH. CTR. (July 28, 2020), https://www.pewresearch.org/internet/2020/07/28/childrens-engagement-with-digital-devices-screen-time/ [https://perma.cc/5LH3-9WNA].

3. *See* Priya Anand & Mark Bergen, *Big Teacher Is Watching: How AI Spyware Took Over Schools*, BLOOMBERG (Oct. 28, 2021), https://www.bloomberg.com/news/features/2021-10-28/how-goguardian-ai-spyware-took-over-schools-student-devices-during-covid [https://perma.cc/FC5T-U7C9].

4. *See* 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 1, 4 (Aug. 2022), https://cdt.org/wp-content/uploads/2022/08/Hidden-Harms-The-Misleading-Promise-of-Monitoring-Students-Online-Research-Report-Final-Accessible.pdf [https://perma.cc/XSL7-E96A] [hereinafter CDT STUDENT MONITORING REPORT]; *see, e.g.*, 47 C.F.R. § 54.520 (2011) (requiring schools to adopt an internet security policy that restricts children's access to certain "obscene" content).

5. *See* Mary Louise Kelly, Enrique Rivera & Christopher Intagliata, *More Kids Are Going Back to School. So Why Is Laptop Surveillance Increasing?*, NPR (Aug. 17, 2022), https://www.npr.org/2022/08/17/1118009553/more-kids-are-going-back-to-school-so-why-is-laptop-surveillance-increasing [https://perma.cc/P2ZM-LU7C].

6. *Id.*

7. Andy Froelich, *The Increasingly Covert and Invasive Surveillance of Students and Its Visible Role in the School-to-Prison Pipeline*, 40 CHILD.'S LEGAL RTS. J. 118, 123 (2020) (contrasting the expectation of privacy on school-issued student devices with the lack of a similar expectation on public social media platforms).

8. *Id.*

9. *See id.* at 130; *infra* section I.C.

While there is a competing priority for school safety, the unrestrained nature of school-issued device surveillance negatively affects students in several ways. Surveilled groups may fall victim to a "chilling effect,"[10] eventually altering students' behavior and emotions. Increased surveillance of students can also strengthen the school-to-prison pipeline.[11] Furthermore, this type of surveillance is particularly troubling today because unrestrained surveillance could be used to further monitor students beyond the sphere of school safety, for example in states that prohibit abortion or gender-affirming care.[12] Finally, school-issued device surveillance disproportionately impacts certain student groups, including low-income students, LGBTQIA2S+ students, and students with disabilities.[13]

This Comment proceeds as follows. Part I introduces the concept of student surveillance. Within Part I, section A provides an overview of student surveillance methods. Section B outlines potential positive effects of school surveillance. Section C highlights a variety of negative effects that the use of school surveillance heightens. Part II provides an overview of the current privacy law landscape, including federal privacy statutes, a selection of state laws, the Fourth Amendment, and the First Amendment. After establishing the inadequacy of existing privacy law, Part III concludes by providing solutions, both within and outside of the legal framework. Within Part III, section A describes a proposed clarification on "school speech" by the United States Supreme Court for off-campus speech on school-issued devices. Section B outlines a recommended framework for federal and state legislatures to limit data sharing, minimize data collection, and track impacts of school surveillance. Section C highlights how school districts are positioned to conduct audits and increase transparency for students and parents. This Comment concludes by addressing the importance and urgency of contending with the privacy implications of school surveillance.

---

10. In the privacy context, a "chilling effect" refers to people who adjust their behavior, such as by limiting self-expression, because they are aware they are being monitored. *See* Hannah Quay-de la Vallee, *The Chilling Effect of Student Monitoring: Disproportionate Impacts and Mental Health Risks*, CTR. FOR DEMOCRACY & TECH. (May 5, 2022), https://cdt.org/insights/the-chilling-effect-of-student-monitoring-disproportionate-impacts-and-mental-health-risks/ [https://perma.cc/DX9F-PC9F].

11. Froelich, *supra* note 7, at 130.

12. *See infra* section I.C.2.

13. *See infra* section I.C.3.

I. UNDERSTANDING STUDENT SURVEILLANCE

This Part provides an overview of school-issued student device and account surveillance, highlighting the pros and cons. Private companies and school districts work together to monitor activity on school-issued devices and accounts, including internet activity, emails, documents, and chats.[14] Some educators argue that this monitoring promotes positive education outcomes, protects schools and individuals against bullying and violence, and ensures compliance with federal laws requiring an internet security policy.[15] Despite these asserted positives, there are also negative impacts. First, widespread surveillance can have harmful psychological effects on the surveilled, including a lack of intellectual privacy and chilling effects.[16] Second, school surveillance reinforces the school-to-prison pipeline and especially jeopardizes students living in areas where abortion or gender-affirming care are prohibited.[17] Finally, negative effects are compounded by disproportionate impacts on certain groups, particularly low-income students, LGBTQIA2S+ students, and students with disabilities.[18]

A. Overview of School-Issued Student Device and Account Surveillance

Private companies and school districts work together to monitor student accounts and activity on school-issued student devices, including flagging search terms, examining school emails and shared documents, and carrying out other aspects of student device surveillance.[19] This section explains how schools and private companies surveil student devices and accounts to show the invasive and unrestricted reach of such surveillance.

School closures due to the COVID-19 pandemic resulted in an accelerated uptake of digital learning methods as schools largely shifted to online instruction.[20] For schools that issue devices to their students,

---

14. Lois Beckett, *Under Digital Surveillance: How American Schools Spy on Millions of Kids*, GUARDIAN (Oct. 22, 2019), https://www.theguardian.com/world/2019/oct/22/school-student-surveillance-bark-gaggle [https://perma.cc/6BDK-GC7R].

15. *See infra* section I.B.

16. *See infra* section I.C.1.

17. *See infra* section I.C.2.

18. *See infra* section I.C.3.

19. Beckett, *supra* note 14.

20. Kevin Bushweller, *What the Massive Shift to 1-to-1 Computing Means for Schools, in Charts*, EDUC. WK. (May 17, 2022), https://www.edweek.org/technology/what-the-massive-shift-to-1-to-1-

one-to-one computing is the norm.[21] One-to-one computing refers to when schools provide each student with a computer, tablet, or other electronic device and is a coveted standard for schools across the country.[22] The COVID-19 pandemic rapidly increased adoption of one-to-one computing; one study showed that ninety percent of district leaders surveyed provided a device to every middle and high school student and eighty-four percent of district leaders surveyed provided a device for every elementary school student.[23] Despite a widespread return to in-person instruction,[24] students still rely, for the most part, on their school-issued devices.[25] One education reporter believes this is both because teachers find electronic tools helpful in the classroom and because schools find surveillance reassuring in the face of instances of school violence across the country.[26]

With more one-to-one computing comes increased use of surveillance software.[27] Student-monitoring software allows teachers and school officials to view and control student screens, scan text in student emails and documents, and send alerts of potential violence or mental health harms.[28] In a Center for Democracy and Technology survey, eighty-nine percent of teachers indicated that their schools use student-monitoring software.[29] Additionally, thirty-seven percent of surveyed teachers who reported use of monitoring software outside of regular school hours explained that mental health or potential violence alerts go to "a third

---

computing-means-for-schools-in-charts/2022/05 [https://perma.cc/7FWR-ZA3F]; *Map: Coronavirus and School Closures in 2019–2020*, EDUC. WK. (Oct. 13, 2021), https://www.edweek.org/leadership/map-coronavirus-and-school-closures-in-2019-2020/2020/03 [https://perma.cc/4CZC-683U].

21. *See id.* (describing how "[t]he 1-to-1 computing landscape in K-12 schools expanded at a rate few could have imagined").

22. *See* Alyson Klein, *During COVID-19, Schools Have Made a Mad Dash to 1-to-1 Computing. What Happens Next?*, EDUC. WK. (Apr. 20, 2021), https://www.edweek.org/technology/during-covid-19-schools-have-made-a-mad-dash-to-1-to-1-computing-what-happens-next/2021/04 [https://perma.cc/4HKD-6MGK].

23. Bushweller, *supra* note 20.

24. *See School Pulse Panel*, INST. OF EDUC. SCIS., https://ies.ed.gov/schoolsurvey/spp/ [https://perma.cc/84WJ-GBLP].

25. *See* CDT STUDENT MONITORING REPORT, *supra* note 4, at 7 ("[R]esearch found that schools have continued to rely heavily on technology, even with the return to in-person school that occurred in the 2021–22 school year."); Bushweller, *supra* note 20.

26. Kelly et al., *supra* note 5.

27. *See* CDT STUDENT MONITORING REPORT, *supra* note 4.

28. Pia Ceres, *Kids Are Back in Classrooms and Laptops Are Still Spying on Them*, WIRED (Aug. 3, 2022), https://www.wired.com/story/student-monitoring-software-privacy-in-schools/ [https://perma.cc/CV3D-7KB8].

29. *See* CDT STUDENT MONITORING REPORT, *supra* note 4, at 8.

party focused on public safety."[30] In other words, such alerts may be going to law enforcement, especially when received outside of regular school hours.[31]

Student surveillance software monitors more than just the school-issued device itself—it monitors all of the accounts associated with an individual.[32] This monitoring involves scanning everything a student produces on their school-issued device or account, including internet activity, like search terms, as well as "student emails, documents, chats, and calendars."[33] To analyze all these interactions, the companies behind monitoring software use "a combination of in-house artificial intelligence and human content moderators paid about $10 an hour."[34] If a student uses their school email to sign up for a social media account, any email notifications from that account are scanned, even if the student used their personal device to sign up.[35] As student activity monitoring technology becomes more popular, the amount of surveillance is only increasing.[36]

Gaggle is one of the most popular surveillance companies used by school districts.[37] Gaggle's monitoring software, like those of other surveillance companies, can even reach *personal* devices plugged into a school-issued device.[38] For example, when students charged their personal phones by plugging them into school-issued laptops, they would "have what they believed to be private conversations via text [on personal phones], in some cases exchanging nude photos with significant others—which the Gaggle software running on the [school-issued] Chromebook

---

30. *Id.* at 20.

31. *Id.*; *see also, e.g.*, Jaisal Noor, *Cops in Baltimore Schools Are Monitoring Students' Laptops*, REAL NEWS NETWORK (Oct. 4, 2021), https://therealnews.com/cops-in-baltimore-schools-are-monitoring-students-laptops [https://perma.cc/X8PF-UE4Z] (describing how police "monitor GoGuardian after school hours, including on weekends and holidays").

32. Caroline Haskins, *Gaggle Knows Everything About Teens and Kids in School*, BUZZFEED NEWS (Nov. 1, 2019), https://www.buzzfeednews.com/article/carolinehaskins1/gaggle-school-surveillance-technology-education [https://perma.cc/44BQ-6RU4].

33. *Id.*

34. *Id.*

35. *Id.*; *see also, e.g.*, *Frequently Asked Questions*, GAGGLE, https://www.gaggle.net/frequently-asked-questions [https://perma.cc/999K-FKF7] (advertising on its website that the service "works at home, at school, on vacation, and on any device—as long as your children are using their school-provided . . . accounts").

36. *See* DHANARAJ THAKUR, HUGH GRANT-CHAPMAN & ELIZABETH LAIRD, CTR. FOR DEMOCRACY & TECH., BEYOND THE SCREEN: PARENTS' EXPERIENCES WITH STUDENT ACTIVITY MONITORING IN K-12 SCHOOLS 6 (July 2023), https://cdt.org/wp-content/uploads/2023/07/2023-07-28-CDT-Civic-Tech-impacts-of-student-surveillance-report-final.pdf [https://perma.cc/77C8-XKPP].

37. *See* Haskins, *supra* note 32.

38. Ceres, *supra* note 28.

could detect."[39] Depending on the personal device's settings and permissions, when a student plugs their personal device into a school-issued device, their images may be uploaded and subsequently scanned by the monitoring software.[40]

The software compares what it scans to a "blocked word list," and automatically flags any matches.[41] Although Gaggle provides options of pre-populated word lists to choose from, school districts can choose to edit what words make up their "blocked word list" or change the list entirely.[42] Anything that the artificial intelligence algorithm flags goes to a Gaggle moderator who determines whether it is a legitimate issue; if so, the flagged match becomes an "incident" that can be escalated to school administrators or even the police.[43] Common examples of legitimate incidents include "profanity" and "references to self-harm, violence, bullying, or drugs."[44] Gaggle also monitors images to ensure none resemble pornography.[45]

Gaggle classifies incidents into one of three tiers based on severity.[46] The first tier, "Violation," could include the use of any language on the blocked word list, even a false positive (e.g., a quote from a book).[47] Under its "three strike rule," Gaggle escalates minor violations to school administrators only if a student violates the rule repeatedly, like using profanity three times.[48] When this occurs, students' account privileges are limited until a school official deems otherwise.[49] The second tier, "'Questionable Content' includes material that's concerning but not an imminent threat to student safety."[50] For example, this tier could include cyberbullying, threats of violence or intentions of self-harm without evidence of an imminent threat, or viewing professional pornographic

---

39. *Id.*

40. *Id.*

41. Haskins, *supra* note 32.

42. *New and Improved Blocking Features,* GAGGLER (Gaggler.Net, Inc., Bloomington, Ill.), Oct. 2007, https://perma.cc/QM6Q-FQ2E.

43. Haskins, *supra* note 32.

44. *Id.*

45. *Gaggle's Anti Pornography Scanner (APS) Is a Hot Topic at ISTE 2012*, PR NEWSWIRE (June 22, 2012), https://www.prnewswire.com/news-releases/gaggles-anti-pornography-scanner-aps-is-a-hot-topic-at-iste-2012-160010045.html [https://perma.cc/Z289-2LEL].

46. Haskins, *supra* note 32.

47. *Id.* Gaggle's Incident Response Rubric for "Violation" includes "[c]ontent contains inappropriate use of profanity or vulgar language" and "[c]ontent is suggestive or contains a provocative image." *Id.*

48. *Id.*

49. *Id.*

50. *Id.*

images.[51] Gaggle alerts school officials via email for incidents flagged as questionable content.[52] The third tier, "Possible Student Situation," is reserved for flags that represent an "imminent threat" to the safety of students.[53] This includes "violence, suicide, pornography, or harmful family situations."[54] Flags for possible student situations result in direct contact to school officials, usually via a phone call.[55]

While non-incident data is purged after thirty days, data reflecting the above incidents is retained for longer periods.[56] This incident data is retained until one of the following criteria is met: a school district terminates their contract with Gaggle, the student graduates or leaves the district, or the school requests a full data purge.[57] If a hypothetical second-grade student was involved in a rule-breaking incident, that data could be kept for ten years.

The rapid advancement of technology in education stands in contrast with the relative leeway schools have to regulate conduct. As "schools have integrated laptops and digital technology into every part of the school day, school districts have largely defined for themselves how to responsibly monitor students on school-provided devices—and how aggressive they think that monitoring should be."[58] While services like Gaggle capture increasingly large amounts of data, school officials have failed to adequately address this growth.

---

51. *Id.* Gaggle's Incident Response Rubric for "Questionable Content" includes "[c]ontent contains professional pornography or reveals inappropriate sexual activity involving a student," "[c]ontent reveals intentions of self harm without evidence of an imminent threat," "[c]ontent reveals threats of violence without evidence of an imminent threat," "[c]ontent reveals harassment without evidence of an imminent threat," and "[c]ontent reveals use of alcohol, tobacco or drugs without evidence of imminent activity." *Id.*

52. *Id.*

53. *Id.* Gaggle's Incident Response Rubric for a "Possible Student Situation" includes "[c]ontent contains pornography that appears to include a minor or an imminent plan of inappropriate sexual activity," "[c]ontent reveals an imminent plan of suicide or self harm," "[c]ontent reveals an imminent threat of violence," "[c]ontent reveals harassment with evidence of an imminent threat," and "[c]ontent reveals possession, intent to sell or intent to procure an illegal substance." *Id.*

54. Paget Hetherington, *What Is a Gaggle Safety Audit?*, GAGGLE (Aug. 14, 2019), https://www.gaggle.net/blog/speaks/what-is-a-gaggle-safety-audit [https://perma.cc/9H5W-6ACA].

55. *Id.*

56. Letter from Jeff Patterson, CEO and Founder, Gaggle, to United States Senators Elizabeth Warren, Richard Blumenthal & Ed Markey (Oct. 12, 2021), https://www.warren.senate.gov/imo/media/doc/Gaggle_Senate_Response_Letter_10_12_21.pdf [https://perma.cc/LP8U-D7VK].

57. *Id.*

58. Beckett, *supra* note 14. For example, human analysts at Securly can "look back at the history of an individual student's internet browsing history and web searches, allowing them to connect the dots between what students are reading, writing, searching for, and, in some cases, posting on social media." *Id.*

B. Arguments for Surveillance

The line between technological advancements with educational benefits and surveillance can be blurry. In fact, schools often cite improved educational outcomes achieved *by* increased surveillance.[59] When teachers have access to improved monitoring, they may be more attuned to their students' needs and can potentially provide more individualized instruction.[60] Some supporters of school monitoring also say the use of surveillance technology is "part of educating today's students in how to be good 'digital citizens', and that monitoring in school helps train students for constant surveillance after they graduate."[61]

Artificial intelligence (AI) advancements allow teachers to easily gather and analyze more data on students and quickly assess individuals' strengths and weaknesses.[62] AI monitoring also lessens the burdens on school administrators, with one school district's technology director contrasting the ease of using Gaggle's AI with their previous process, which involved manually searching each student's school email account (looking for words like "marijuana"), reading each individual message that included that word, and following up on any concerning behavior.[63]

Following an uptick in school violence, schools face pressure to adopt additional surveillance techniques to ensure such tragic events do not occur.[64] Gun-related violence in schools has increased over the past twenty years.[65] Parents and schools also have concerns about increased

---

59. Alyson Klein, *Software that Monitors Students May Hurt Some It's Meant to Help*, EDUC. WK. (Aug. 8, 2022), https://www.edweek.org/technology/software-that-monitors-students-may-hurt-some-its-meant-to-help/2022/08 [https://perma.cc/MN22-BLSK]. *But see* Sarah D. Sparks, *'High-Surveillance' Schools Lead to More Suspensions, Lower Achievement*, EDUC. WK. (Apr. 21, 2021), https://www.edweek.org/leadership/high-surveillance-schools-lead-to-more-suspensions-lower-achievement/2021/04 [https://perma.cc/2P8G-XL52].

60. Larry Ferlazzo, *Should Teachers Be Allowed to Use Online Tools to Monitor Student Screens?*, EDUC. WK. (Mar. 21, 2023), https://www.edweek.org/technology/opinion-should-teachers-be-allowed-to-use-online-tools-to-monitor-student-screens/2023/03 [https://perma.cc/QHL7-XH5L].

61. Beckett, *supra* note 14.

62. Brian A. Jacob, *The Opportunities and Challenges of Digital Learning*, BROOKINGS (May 5, 2016), https://www.brookings.edu/research/the-opportunities-and-challenges-of-digital-learning/ [https://perma.cc/9E6P-8CLM]; *see also* Elana Zeide, *Education Technology and Student Privacy*, *in* CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 70, 70 (Evan Selinger, Jules Polonetsky & Omer Tene eds., 2018) [hereinafter Zeide, *Education Technology*] ("This information . . . [can] better inform education-related decision-making for students, educators, schools, ed tech providers, and policymakers.").

63. Beckett, *supra* note 14.

64. Ceres, *supra* note 28.

65. Donna St. George, *School Shootings Rose to Highest Number in 20 Years, Federal Data Says*, WASH. POST (June 28, 2022), https://www.washingtonpost.com/education/2022/06/28/school-shootings-crime-report/ [https://perma.cc/697H-YAVJ].

cyberbullying.[66] In addition, schools sometimes cite the data security benefits of using school devices, "highlighting potential harms to students from outside threats."[67] According to one school official, "[t]here's a lot to be said about the district-issued device, the security around that device, and the sustainability of being able to manage that device effectively."[68] Further, there are reports of "an increase in self-harm incidents and aggressive impulses" in students since the beginning of the COVID-19 lockdown.[69] Some argue that surveilling student accounts can help prevent these incidents from occurring by alerting school officials when a student's searches, texts, or emails indicate they may be considering harming themselves.[70]

The Children's Internet Protection Act (CIPA) arguably strengthens a school district's ability to surveil its students.[71] Congress passed CIPA, which is implemented by the Federal Communications Commission (FCC), in 2000.[72] Under CIPA, schools receiving federal funding must adopt an internet security policy to prevent students from accessing certain obscene or pornographic images.[73] CIPA focuses on minors accessing the internet, and particularly on information that the law deems "inappropriate."[74] Schools subject to CIPA must also adopt an internet safety policy that includes monitoring the online activity of minors and

---

66. *See id.*; Sasha Jones, *One-Fifth of Children Experience Cyberbullying, According to Their Parents*, EDUC. WK. (May 30, 2019), https://www.edweek.org/leadership/one-fifth-of-children-experience-cyberbullying-according-to-their-parents/2019/05 [https://perma.cc/SQ5V-BFVK].

67. 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 8 (Sept. 2021), https://iapp.org/media/pdf/resource_center/online_and_observed_student_privacy_implications_school_issued_devices_cdt_report.pdf [https://perma.cc/VLN8-E3BG].

68. *Id.*

69. Jessa Crispin, *US Schools Gave Kids Laptops During the Pandemic. Then They Spied on Them*, GUARDIAN (Oct. 11, 2021), https://www.theguardian.com/commentisfree/2021/oct/11/us-students-digital-surveillance-schools [https://perma.cc/UQ7Z-S4UC].

70. *See* HANKERSON ET AL., *supra* note 67, at 12 ("In discussing why they decided to seek out student activity monitoring tools, one administrator talked about interrupting students' attempts to self-harm.").

71. Cody Venzke, *CDT Calls for Congress to Clarify the Privacy Impacts of CIPA*, CTR. FOR DEMOCRACY & TECH. (Sept. 27, 2021), https://cdt.org/insights/cdt-calls-for-congress-to-clarify-the-privacy-impacts-of-cipa/ [https://perma.cc/WZH7-S22L] ("[S]chool technology leaders have adopted broad, invasive monitoring software at least in part because they believe that it is required by the Children's Internet Protection Act.").

72. 47 C.F.R. § 54.520 (2011).

73. *Children's Internet Protection Act (CIPA)*, FED. COMMC'NS COMM'N, https://www.fcc.gov/consumers/guides/childrens-internet-protection-act [https://perma.cc/VE9V-DN8A] (last updated Dec. 30, 2019).

74. 47 C.F.R. § 54.520 (2011).

provides for educating minors about appropriate online behavior.[75] CIPA's provisions, while offering some protection to students from obscene images, primarily serve as a *reinforcement* for surveillance companies like Gaggle, many of whom tout their ability to "directly support[] districts' responsibility to protect students" under CIPA.[76] The federal government has subsequently passed legislation providing funds for public schools to use towards such digital surveillance.[77]

In sum, the limited benefits associated with surveillance of school-issued devices and accounts are not furthered by its vast nature. To date, no study has proven the efficacy of student surveillance as a deterrent on violent crime.[78] Although parents and students are largely comfortable with activity monitoring for *urgent* safety,[79] the current surveillance exceeds this parameter. In this case, "the solution doesn't solve the problem, and it creates new issues of its own."[80] The next section will highlight additional negative consequences of student surveillance.

C. Problems with Student Surveillance

Despite some educational benefits, the far-reaching nature of student surveillance outweighs the potential benefits. Studies show the chilling effects that constant, twenty-four-seven surveillance can have on students.[81] When students feel as though they live in a surveillance landscape, it can lead to negative psychological effects that fundamentally change student behavior.[82] Moreover, school surveillance increasingly punishes non-criminal behavior and ultimately reinforces the school-to-

---

75. *Id.*

76. Paget Hetherington, *Keeping Districts Protected as They Bridge the Digital Divide*, GAGGLE (Sept. 25, 2020), https://www.gaggle.net/blog/keeping-districts-protected-as-they-bridge-the-digital-divide [https://perma.cc/YCG9-V62M].

77. *E.g.*, S. 2938, 117th Cong. (2021).

78. Chad Marlow, *Student Surveillance Versus Gun Control: The School Safety Discussion We Aren't Having*, ACLU (Mar. 4, 2019), https://www.aclu.org/news/privacy-technology/student-surveillance-versus-gun-control-school [https://perma.cc/NR6T-7VX3].

79. CDT STUDENT MONITORING REPORT, *supra* note 4, at 9. As one parent noted: "I would be ninety percent in favor of anything that supports student privacy with minimalist exceptions that are like extreme student safety concerns. . . . I think everything else can be handled outside of monitoring and more through [sic] investigation on the school's part." THAKUR ET AL., *supra* note 36, at 16

80. Benjamin Herold, *Schools Are Deploying Massive Digital Surveillance Systems. The Results Are Alarming*, EDUC. WK. (May 30, 2019), https://www.edweek.org/technology/schools-are-deploying-massive-digital-surveillance-systems-the-results-are-alarming/2019/05 [https://perma.cc/5JRR-ESYP] (quoting Rachel Levinson-Waldman, N.Y.U. School of Law).

81. *See* HANKERSON ET AL., *supra* note 67, at 15.

82. *See* CDT STUDENT MONITORING REPORT, *supra* note 4, at 22.

prison pipeline.[83] With criminalized behavior expanding in recent years, especially as it relates to minors, the legal implications of current student surveillance practices are far-reaching. As several state laws now prohibit abortions,[84] surveillance could jeopardize students' health and safety by making them afraid to use their school-issued device or account to access critical information on medical treatments such as abortions. Additionally, some jurisdictions have recently enacted laws or policies restricting youth access to gender-affirming care, which jeopardizes students who may use their school device or account to access health information.[85] Students face an increased risk of punishment for non-criminal behavior when schools constantly surveil their laptops and potentially share the collected data with law enforcement. All these negative effects are compounded by disproportionate impacts on certain groups, particularly low-income students, LGBTQIA2S+ students, and students with disabilities.[86]

Further, concerns about surveillance are particularly prevalent in the school context, where students rarely have a choice about privacy.[87] Schools strongly encourage, and in some cases require, children and parents to engage with educational technology to participate in many school-related activities.[88] While students technically must consent before schools collect their data, they effectively have no choice due to compulsory attendance at educational institutions and the essentially mandatory nature of technology in schools.[89] Although, in theory, parents

---

83. Froelich, *supra* note 7, at 129.

84. *See After Roe Fell: Abortion Laws by State*, CTR. FOR REPROD. RTS., https://reproductiverights.org/maps/abortion-laws-by-state/ [https://perma.cc/PR8F-SMFX] [hereinafter *After Roe Fell*]; *see also, e.g.*, MO. REV. STAT. § 188.017(2) (2022) (providing an example of an abortion ban); KY. REV. STAT. § 311.772 (2019) (same); ALA. CODE § 26-23H-4 (2019) (same); MISS. CODE ANN. § 41-41-45 (2022) (same).

85. *See, e.g.*, Arkansas Save Adolescents from Experimentation (SAFE) Act, H.B. 1570, 93d Gen. Assemb. (Ark. 2021) (codified at ARK. CODE ANN. §§ 20-9-1501–1504 (LexisNexis 2021)) (banning gender-affirming medical procedures for transgender people under eighteen); Letter from Greg Abbott, Governor, State of Tex., to Jaime Masters, Comm'r, Tex. Dep't of Fam. & Protective Servs. (Feb. 22, 2022), https://gov.texas.gov/uploads/files/press/O-MastersJaime202202221358.pdf [https://perma.cc/CH43-2K4P] [hereinafter Letter from Greg Abbott, Governor] (criminalizing elective procedures for gender transitioning as child abuse, including gender-affirming surgeries and the administration of gender-affirming hormones); ARIZ. REV. STAT. § 32-3230 (2023) (prohibiting gender reassignment surgery for minors).

86. *See supra* section I.C.3.

87. Zeide, *Education Technology*, *supra* note 62, at 70 (describing how "students rarely have a choice regarding educational privacy practices").

88. *Policy Statement of the Federal Trade Commission on Education Technology and the Children's Online Privacy Protection Act*, FED. TRADE COMM'N, https://www.ftc.gov/system/files/ftc_gov/pdf/Policy%20Statement%20of%20the%20Federal%20Trade%20Commission%20on%20Education%20Technology.pdf [https://perma.cc/7JZL-KKE7].

89. Elana Zeide, *Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPs*, 8 DREXEL L. REV. 339, 383 (2016) [hereinafter Zeide, *Student Privacy Principles*].

can object to school technology or privacy practices, in reality, few parents have the means to switch schools or homeschool their children to avoid these practices.[90] Because students opting out of using educational technology "often end up at a social and academic disadvantage, . . . most parents eventually capitulate."[91]

1. Lack of Intellectual Privacy, Chilling Effects, and the Surveillance Landscape

Widespread surveillance has negative psychological implications for students. Privacy scholars believe that the concept of "intellectual privacy" spurs the creation of new ideas and the promotion of robust debate.[92] Intellectual privacy is defined as "the protection from surveillance or unwanted interference by others when [people] are engaged in the process of generating ideas and forming beliefs."[93] Creating new ideas requires access to knowledge and "places and spaces (real and virtual) in which to read, to think, [and] to explore."[94] In addition, new ideas sometimes need to develop away from intense scrutiny so that people can spend time ruminating on their ideas in private,[95] and testing those new ideas on friends and peers before sharing them publicly.[96]

Increased surveillance can restrict intellectual privacy by causing people to guard their words or thoughts.[97] As privacy scholar Neil Richards, one of the founders of the concept of intellectual privacy, stated: "If we know that someone is watching and listening, we will be careful with not just what we say but also what we read and even what we think."[98] This feeling is especially true for children in the school setting, where "fear of embarrassment, disapproval, and discipline" may restrict

---

90. Elana Zeide, *The Structural Consequences of Big Data-Driven Education*, 5 BIG DATA 164, 167 (2017) ("Even in cases wherein parents do have the choice to opt-out of specific classroom technologies, they often do not feel they can do so in practice without putting their children at a significant social and academic disadvantage.").

91. Zeide, *Education Technology*, *supra* note 62, at 78.

92. NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 95–108 (2015).

93. *Id.* at 95.

94. *Id.* at 97.

95. *Id.* at 103.

96. *Id.* at 108.

97. *Id.* at 101. For example, this may result in "a critic of government policy, if she were aware of surveillance, not only being careful of what she said privately to her confidants but also being careful in what she read and what websites she visited." *Id.* One can imagine how this example could easily extend from someone critical of government policy to a student critical of school policy.

98. *Id.*

students' true expression.[99] While schools play a central role in a child's self-development and self-expression process, this type of surveillance may endanger "the privacy that children need in their formative years to explore, learn, befriend, and communicate."[100] As students choose what they believe, research controversial ideas online, and discuss their thoughts in chats and emails with trusted friends, these behaviors create electronic records that schools actively surveil.[101] Thus, students may feel stifled and adjust their behavior if they are concerned about being punished for their choices, research, or discussions.[102] Furthermore, research itself may be limited as schools block students accessing certain websites.[103]

One of the basic tenets underlying free speech in America "is the idea that when people are subject to punishment for speaking, there is a 'chilling effect' on the exercise of their constitutional right to free expression."[104] In the privacy context, a "chilling effect" refers to people who, aware they are being monitored, alter their behavior to "curb exploration and self-expression."[105] This chilling effect may cause students to repress their own speech and conduct for fear schools will see what they do on their devices.[106] This chilling effect becomes even more troubling when it disproportionately impacts certain groups that are

---

99. Danielle Keats Citron, *The Surveilled Student*, 76 STAN. L. REV. (forthcoming) (manuscript at 6) (on file with author) ("Children experience more physical and emotional growth during their primary and secondary educations than in any other time in their lives.").

100. *Id.* at 15.

101. *Cf.* RICHARDS, *supra* note 92, at 122 ("[W]e should care about the privacy of electronic records that reveal our thoughts."). These records may include online searches, email and chat messages, and other activities associated with a school-issued device or account. *See id.*; Haskins, *supra* note 32.

102. *Cf. id.* at 104 ("[Intellectual privacy] rests on the belief that free minds are the foundation of a free society, and that surveillance of the activities of belief formation and idea generation can affect those activities profoundly and for the worse.").

103. *See* THAKUR ET AL., *supra* note 36, at 8 (describing how a tenth-grader's online research for an essay on the Defense of Marriage Act was flagged, which "seem[ed] pretty extreme" to their parent after viewing the materials).

104. RICHARDS, *supra* note 92, at 107 (arguing that "if we think that surveillance by companies or other private actors would affect our reading and thinking as well, then we should be concerned about a threat to our culture of free speech").

105. Quay-de la Vallee, *supra* note 10.

106. *See id.*; *see also* Beckett, *supra* note 14 ("A few school districts have chosen not to send students Gaggle's warnings about swear words, some because they're concerned that if students are reminded that they're being monitored, 'the children will then resort to other tools to communicate, and they'll miss the life-threatening issues they could have intervened in." (quoting Bill McCullough, a Gaggle spokesperson)); *cf.* RICHARDS, *supra* note 92, at 107 ("Keeping out those who would monitor our reading and private communications is essential if we want to generate new ideas, a fact our law has long recognized in subtle and sometimes underappreciated ways.").

already monitored more than others.[107] In addition, over time, students will likely learn which terms school districts "flag" and adjust their behavior accordingly to self-censor.[108]

A lack of intellectual privacy and the resulting chilling effects negatively impacts students, the learning environment, and society overall.[109] In fact, many parents consider continuous monitoring to be "intrusive, regardless of the possible benefits."[110] Increased surveillance could have any of the following effects: suppressed intellectual freedom (e.g., students choosing not to investigate forbidden subjects online if their online searches might be revealed); suppressed freedom of speech (e.g., students choosing not to engage in private conversations on their devices); and suppressed freedom of association (e.g., students choosing not to associate with groups they may want to keep private, such as those promoting certain political views or LGBTQIA2S+ organizations).[111] For example, as one reporter, Lois Beckett, asked: "[i]f students know their schools are monitoring their computer usage, will LGBTQ students in conservative school districts feel comfortable researching their sexuality? What about young Trump supporters in liberal school districts who want to do some political research?"[112]

Not only can increased surveillance chill students' right of expression, but it can also negatively impact students' mental health. Students report "experiencing detrimental effects" from online surveillance, including choosing not to "access[] important resources that could help them."[113] In addition, research suggests that the "sense of vulnerability" that can result from living in a surveillance landscape impedes students academically

---

107. *See supra* section I.C.3. Surveillance of school-issued student devices and accounts, by its very nature, disproportionately impacts certain groups of students, particularly low-income students, LGBTQIA2S+ students, and students with disabilities. *See supra* section I.C.3.

108. Herold, *supra* note 80.

109. *See* Quay-de la Vallee, *supra* note 10; RICHARDS, *supra* note 92, at 105–06 (describing how surveillance can simultaneously injure civil liberties, deter belief formation, and discourage intellectual experimentation).

110. Zeide, *Education Technology*, *supra* note 62, at 76. Despite an awareness of its safety benefits, the "intentional, systemic nature of the surveillance" has changed parents' perception of these companies. *Id.*

111. Marlow, *supra* note 78.

112. Beckett, *supra* note 14.

113. CDT STUDENT MONITORING REPORT, *supra* note 4, at 5; *see also* THAKUR ET AL., *supra* note 36, at 9 (describing how a student felt "humiliated, embarrassed, . . . frustrated and angry" after their online research for a school project "was incorrectly flagged as related to suicide").

and undermines the intellectual curiosity and safety typically associated with the school setting.[114]

School districts may attempt to mitigate this effect, partly because they realize its harm and partly because it will make their surveillance less effective. For example, school districts can choose whether students receive an email when they use profanity.[115] Schools may choose never to send those emails so that students are not reminded they are monitored and, thus, produce more content for schools to observe.[116] Said one school superintendent, "[o]nce the kids know they're being Gaggled, they're being watched 24-7, they tend to be more proactive in watching what they do."[117] If a student is wary of being flagged by school officials, they may limit the use of their school device and account and ultimately "shut themselves off from adults."[118]

2. School-to-Prison Pipeline

Student surveillance reinforces the school-to-prison pipeline by providing yet another link between students and law enforcement and ensuring that link is constantly open.[119] When schools punish non-criminal behavior, that discipline contributes to this pipeline.[120] With both abortion and gender-affirming care for children increasingly criminalized since 2022, privacy experts are especially concerned about the rising level of student surveillance.[121]

The "school-to-prison pipeline" describes the phenomenon where increased discipline in schools "push[es] our nation's schoolchildren, especially our most at-risk children, out of classrooms and into the

---

114. *See* Elana Zeide & Helen Nissenbaum, *Learner Privacy in MOOCs and Virtual Education*, 16 THEORY & RSCH. IN EDUC. 280, 299 (2018) (describing how "Ed tech may increase students' sense of vulnerability" and ultimately have a negative effect on individual academic performance and overall equity); *id.* at 298–300; *see also* THAKUR ET AL., *supra* note 36, at 12–13 (recounting one student's negative experience after learning the extent of monitoring, including surveillance of their personal cell phone content after it was plugged into a school-issued laptop).

115. Beckett, *supra* note 14.

116. *See id.*

117. *Id.*

118. Haskins, *supra* note 32.

119. Froelich, *supra* note 7, at 129–30 ("Increased surveillance in schools will inevitably intensify the existing disparities in school discipline.").

120. *Id.* at 128–29 (describing how "harsh, discretionary penalties for breaking school rules hold back students academically and push them into the juvenile justice system").

121. *See, e.g.*, Ceres, *supra* note 28 (describing how "the criminalization of reproductive health care" and "[p]roposals targeting LGBTQ youth, such as the Texas governor's calls to investigate the families of kids seeking gender-affirming care," make privacy concerns "more acute").

juvenile and criminal justice systems."[122] It typically begins when a student gets in trouble with their teacher, commonly for minor misbehavior.[123] The student may get in trouble again, resulting in the teacher notifying the school administration.[124] Next, the student may be suspended or expelled, followed by the possibility of juvenile detention, and from that point on, the student remains intertwined with law enforcement.[125] This interconnects the systems of school discipline and law enforcement.[126]

School-issued device surveillance reinforces the school-to-prison pipeline.[127] In 2022, seventy-eight percent of teachers reported their schools used surveillance to identify violations of disciplinary policy.[128] Forty-four percent of teachers also reported at least one instance of their school contacting law enforcement based on behaviors flagged by monitoring software.[129] Further, teacher surveys "indicate that monitoring software is more commonly used for disciplinary purposes than for identifying threats to safety or for providing mental health support."[130] A report by the Center for Democracy and Technology described the reality of these concerns: "[d]espite assurances and hopes that student activity monitoring will be used to keep students safe, . . . it is more frequently used for disciplinary purposes in spite of parent and student concerns."[131]

When setting up their chosen student device surveillance software, some districts opt into immediate contact with law enforcement rather

---

122. Amy B. Cyphert, *Addressing Racial Disparities in Preschool Suspension and Expulsion Rates*, 82 TENN. L. REV. 893, 902–03 (2015) (quoting *Locating the School-to-Prison Pipeline*, ACLU, https://www.aclu.org/sites/default/files/images/asset_upload_file966_35553.pdf [https://perma.cc/GU9W-W8AT]).

123. *School-to-Prison Pipeline*, ACLU, https://www.aclu.org/issues/juvenile-justice/juvenile-justice-school-prison-pipeline [https://perma.cc/AT3Q-868G].

124. *See id.*

125. *Id.*

126. *Id.*

127. Froelich, *supra* note 7, at 130; *see also* Clarence Okoh, *AI Is Supercharging Child Surveillance and the School-to-Prison Pipeline*, HILL (Nov. 21, 2023), https://thehill.com/opinion/technology/4319035-ai-is-supercharging-child-surveillance-and-the-school-to-prison-pipeline [https://perma.cc/F4Q5-YMUQ] ("[R]esearch demonstrat[es] that students' digital footprints are increasingly used to disproportionately discipline, expel and even arrest Black schoolchildren — effectively opening a new digital frontier in the longstanding school-to-prison pipeline.").

128. CDT STUDENT MONITORING REPORT, *supra* note 4, at 24.

129. *Id.* at 20.

130. *Id.* at 12; *see also id.* at 9 ("[S]takeholders express concerns about using student activity monitoring for disciplinary purposes: Approximately 6 in 10 parents and teachers agree that student activity monitoring could bring harm to students if it is used for discipline.").

131. *Id.* at 4.

than notifying school administrators first.[132] This decision alone can increase student contact with law enforcement, especially for surveilled activity outside of school hours or off school premises, and reinforce the school-to-prison pipeline.[133] In addition, the persistent nature of student device surveillance allows for constant monitoring.[134] Before school-issued devices, schools did not typically monitor students in the middle of the night. But now, a student's midnight Google searches could be flagged immediately, resulting in disciplinary action or contact with law enforcement.[135] Contact with law enforcement occurs even more frequently outside of regular school hours because flagged content often bypasses school administrators and goes straight to law enforcement.[136]

With both abortion and gender-affirming care for children increasingly criminalized in 2022 and 2023,[137] the rising level of student surveillance and its implications for children and parent interactions with law enforcement is concerning. The use of digital forensics to investigate people for breaking abortion rules is widespread among law enforcement.[138] For example, in Nebraska, police used a search warrant to obtain a seventeen-year-old's private Facebook messages with her mother before charging both parties "with violating the state's ban on abortions after 20 weeks of pregnancy."[139] The daughter was sentenced to ninety days in prison with two years of probation, and the mother was sentenced

132. ELIZABETH WARREN & ED MARKEY, U.S. SENATE, CONSTANT SURVEILLANCE: IMPLICATIONS OF AROUND-THE-CLOCK ONLINE STUDENT ACTIVITY MONITORING 3 (2022), https://www.warren.senate.gov/imo/media/doc/356670%20Student%20Surveillance.pdf [https://perma.cc/V785-D3LS].

133. *See* Froelich, *supra* note 7, at 130 ("[T]echnologically enhanced school surveillance and monitoring will increase the number of school discipline infractions . . . detected.").

134. Beckett, *supra* note 14 ("The new school surveillance technology doesn't turn off when the school day is over: anything students type in official school email accounts, chats or documents is monitored 24 hours a day, whether students are in their classrooms or their bedrooms.").

135. WARREN & MARKEY, *supra* note 132, at 5–6.

136. *Id.*

137. *See* Annette Choi & Will Mullery, *19 States Have Laws Restricting Gender-Affirming Care, Some with the Possibility of a Felony Charge*, CNN (June 6, 2023), https://www.cnn.com/2023/06/06/politics/states-banned-medical-transitioning-for-transgender-youth-dg/index.html [https://perma.cc/R2KL-XT5D]; *After Roe Fell*, *supra* note 84.

138. *See* Cynthia Conti-Cook & Kate Bertash, *Digital Surveillance Presents New Threats to Reproductive Freedoms*, WASH. POST (Dec. 15, 2021), https://www.washingtonpost.com/outlook/2021/12/15/digital-surveillance-reproductive-freedom/ [https://perma.cc/3M9Z-Q7PA].

139. Mark Keierleber, *With 'Don't Say Gay' Laws & Abortion Bans, Student Surveillance Raises New Risks*, THE 74 (Sept. 8, 2022), https://www.the74million.org/article/with-dont-say-gay-laws-abortion-bans-student-surveillance-raises-new-risks/ [https://perma.cc/7BK8-VCYS].

to two years in prison.[140] This has significant ramifications for students who schools surveil. The question of whether school districts can share private student information related to the enforcement of state laws, either at their own discretion or if forced to do so by law enforcement, has heightened consequences with the criminalization of abortion in several states. While a GoGuardian spokesperson has stated that its service "cannot be used by educators or schools to flag reproductive health-related search terms,"[141] that discretionary self-regulation may not be enough protection for students. There is a concern that law enforcement may compel school districts or surveillance companies to use the information they collect on students as it relates to students seeking abortions.[142] For example, in the Nebraska case, Meta (Facebook) complied with the warrant, turning over the abortion-related Facebook messages to law enforcement.[143]

In February 2022, Texas Governor Greg Abbott issued an order directing the Texas Department of Family and Protective Services (DFPS) to investigate parents who provide gender-affirming care to their children.[144] If investigated, the parents' conduct may be considered child abuse, and DFPS could remove the child from their home.[145] This order could have enormous effects for transgender children seeking to receive gender-affirming care—care that a consensus of medical experts recommends for transgender youth.[146] While a judge temporarily blocked this order, it has potentially devasting effects for transgender children and

---

140. Jesus Jiménez, *Mother Who Gave Abortion Pills to Teen Daughter Gets 2 Years in Prison*, N.Y. TIMES (Sept. 22, 2023), https://www.nytimes.com/2023/09/22/us/jessica-burgess-abortion-pill-nebraska.html (last visited Dec. 20, 2023); Michael Levenson, *Nebraska Teen Who Used Pills to End Pregnancy Gets 90 Days in Jail*, N.Y. TIMES (July 20, 2023), https://www.nytimes.com/2023/07/20/us/celeste-burgess-abortion-pill-nebraska.html (last visited Dec. 20, 2023).

141. Mark Keierleber, *The Risks of Student Surveillance amid Abortion Bans and LGBTQ Restrictions*, GUARDIAN (Sept. 8, 2022), https://www.theguardian.com/education/2022/sep/08/abortion-bans-school-surveillance-lgbtq-restrictions [https://perma.cc/YZ6H-5CXE].

142. *See* Albert Fox Cahn, *The Most Devastating Tool of Abortion Bounty Hunters in Texas Could Be the Surveillance State*, FAST CO. (Sept. 14, 2021), https://www.fastcompany.com/90675851/abortion-bounty-hunters-texas-surveillance (last visited Feb. 21, 2024) ("Texas education officials could weaponize the state's school surveillance network, identifying any public school students who search for information about abortion.").

143. Jiménez, *supra* note 140.

144. Letter from Greg Abbott, Governor, *supra* note 85.

145. *Id.*

146. *Doctors Agree: Gender-Affirming Care Is Life-Saving Care*, ACLU (Apr. 1, 2021), https://www.aclu.org/news/lgbtq-rights/doctors-agree-gender-affirming-care-is-life-saving-care [https://perma.cc/7MPW-VGXK].

their families if reinstated.[147] School surveillance could increase the number of investigations under Governor Abbott's order. If a child searches for information about gender-affirming care or being transgender online, that may be flagged based on the recommended blocked word lists used by many school districts.[148] Further, if that information is reported to school districts and possibly law enforcement, it could be used against the parents in a DFPS investigation. With more criminalized behavior, especially affecting minors, the increasing level of student surveillance and its connection to the school-to-prison pipeline raises critical concerns.

3. Disproportionate Impact on Certain Students

By its very nature, surveillance of school-issued student devices and accounts disproportionately impacts certain groups of students, particularly low-income students, LGBTQIA2S+ students, and students with disabilities. Because schools are already more likely to discipline these groups, increased monitoring of the same students has a compounding effect and further increases the frequency and number of disciplinary actions,[149] some of which may lead to further law enforcement interactions.[150] Despite the potential for disproportionate impacts, a report by Senators Warren and Markey indicates that "none of the companies have analyzed their algorithms for bias or even track whether their products over- or under-identify different groups of students."[151]

One reason increased surveillance disproportionately impacts low-income students is their heavier reliance on school-issued devices.[152] Students and parents typically must agree to a school's responsible-use

147. Eleanor Klibanoff, *Judge Temporarily Blocks Some Texas Investigations into Gender-Affirming Care for Trans Kids*, TEX. TRIB. (June 10, 2022), https://www.texastribune.org/2022/06/10/texas-gender-affirming-care-child-abuse/ [https://perma.cc/GP5N-K3FS].

148. Keierleber, *supra* note 141.

149. CDT STUDENT MONITORING REPORT, *supra* note 4, at 6–7, 21–24; *see also* Froelich, *supra* note 7, at 130 ("Without addressing the systemic bias in school discipline, the unfairness embedded in that system will only increase with advanced technological surveillance because school officials will be able to discover more code of conduct violations.").

150. *Id.*; *see supra* section I.C.2; *see also* Froelich, *supra* note 7, at 130 ("[T]hese enhanced surveillance methods will increase the probability that a disproportionate number of students of color and students with disabilities will be pushed into the juvenile justice system.").

151. WARREN & MARKEY, *supra* note 132, at 3.

152. *See* CDT STUDENT MONITORING REPORT, *supra* note 4, at 6 (describing how students who rely on school-issued devices are monitored more frequently).

policy to access a device.[153] While, in theory, parents could opt out of using the device, the decision to do so is not typically an easy one:[154] opting out makes educational participation very difficult and parents may feel opting out would "put[] their children at a significant social and academic disadvantage."[155] As such, opting out becomes more feasible for high-income students, who are more likely to have access to another computer besides their school-issued device.[156] In addition, evidence shows that schools monitor students using school-issued devices more than students using personal devices.[157] Thus, lower income students "bear the brunt of surveillance."[158]

Evidence also shows student surveillance disproportionately affects LGBTQIA2S+ students because many monitored terms target these students.[159] First, blocked word lists contain health terms that are specific to LGBTQIA2S+.[160] For example, GoGuardian's web-filtering tool "categorize[s] health resources for LGBTQ teens as pornography."[161] LGBTQIA2S+ students may be more likely to turn to the internet for answers about their sexual orientation, causing a compounding effect that results in disproportionately more flags of such students.[162] Second, LGBTQIA2S+ students are more likely to be contacted due to concerns about their mental health or their potential to commit a crime.[163] Finally, several school districts used monitoring software to reveal a student's sexuality and "out" them to school administrators, teachers, and even their parents.[164] One survey found that thirteen percent of students at schools using device and account surveillance reported either their own or another student's outing "because of student activity monitoring."[165] This

153. *See, e.g.*, SEATTLE PUB. SCHS., 2023–2024 STUDENT 1:1 LAPTOP DEVICE AGREEMENT, https://www.seattleschools.org/wp-content/uploads/2022/08/Fall-2022-Laptop-Packet.pdf [https://perma.cc/VFR8-TPRK] (providing an example device agreement).

154. Haskins, *supra* note 32.

155. Zeide, *Student Privacy Principles*, *supra* note 89, at 167.

156. Barbara Fedders, *The Constant and Expanding Classroom: Surveillance in K-12 Public Schools*, 97 N.C. L. REV. 1673, 1716 (2019).

157. HANKERSON ET AL., *supra* note 67, at 10–11.

158. Fedders, *supra* note 156.

159. *See* CDT STUDENT MONITORING REPORT, *supra* note 4, at 21.

160. Keierleber, *supra* note 139.

161. *Id.*

162. WARREN & MARKEY, *supra* note 132, at 3–5; Fedders, *supra* note 156, at 1717.

163. *See* CDT STUDENT MONITORING REPORT, *supra* note 4, at 21.

164. Ceres, *supra* note 28.

165. CDT STUDENT MONITORING REPORT, *supra* note 4, at 21. In addition, that percentage is more than doubled among LGBTQIA2S+ students. *Id.*

nonconsensual disclosure of sexual orientation is a prevalent problem that can impact a student's wellbeing and safety.[166]

Students with disabilities also experience increased harm from student device and account monitoring.[167] A 2022 report found that students with disabilities are less likely to express their thoughts and feelings online as a result of feeling surveilled, suggesting that "students with learning differences or physical disabilities may be especially prone to adverse negative mental health impacts from constrained free expression."[168] This likely explains why teachers report receiving more alerts regarding students with disabilities compared to the entire student population,[169] as students with disabilities are more likely to have their speech flagged and misinterpreted by surveillance software.[170]

School districts should be wary of these disproportionate impacts, as well as the others discussed above.

II. THE LEGAL LANDSCAPE OF STUDENT PRIVACY IS INADEQUATE

This Part provides an overview of the student privacy legal landscape. It first examines federal and state privacy laws associated with children and students. It then discusses how Fourth Amendment jurisprudence relates to school and devices searches. Finally, it considers First Amendment jurisprudence regarding protected school speech.

It is also important to note that student privacy protections may be even weaker than what is described below for students at private or parochial schools. For example, Family Educational and Rights and Privacy Act of

---

166. Evan Ettinghoff, *Outed at School: Student Privacy Rights and Preventing Unwanted Disclosures of Sexual Orientation*, LOY. L.A. L. REV. 579, 582 (2014) ("Forcing disclosure of sexual orientation not only interferes with an individual's privacy and autonomy but it potentially threatens that individual's well-being and safety.").

167. *See* CDT STUDENT MONITORING REPORT, *supra* note 4, at 23 ("Students with learning differences and physical disabilities report experiencing a greater chilling effect from student activity monitoring.").

168. *See Hidden Harms: Students with Disabilities, Mental Health, and Student Activity Monitoring*, CTR. FOR DEMOCRACY & TECH. 5–6, https://cdt.org/wp-content/uploads/2022/11/2022-11-01-Civic-Tech-Students-With-Disabilities-Mental-Health-Monitoring-Research-Brief.pdf [https://perma.cc/G4ER-H5J5] [hereinafter *Students with Disabilities Monitoring Report*]; *supra* section I.C.1.

169. *See Students with Disabilities Monitoring Report*, *supra* note 166, at 7; Lydia X.Z. Brown, Ridhi Shetty, Matthew U. Scherer & Andrew Crawford, *Ableism and Disability Discrimination in New Surveillance Technologies*, CTR FOR DEMOCRACY & TECH. 8 (May 2022), http://cdt.org/wp-content/uploads/2022/05/2022-05-23-CDT-Ableism-and-Disability-Discrimination-in-New-Surveillance-Technologies-report-final-redu.pdf [https://perma.cc/PZ9R-DKA5].

170. Brown et al., *supra* note 167, at 16 (describing how "a white autistic high school student in Oregon [was] profiled as a would-be school shooter in the absence of making any actual threat").

1974[171] applies only to educational institutions that receive funds from the federal government, excluding many private and parochial schools at the elementary and secondary level.[172] In addition, the Fourteenth Amendment, which prohibits states from denying federal constitutional rights, applies to state entities but not private entities.[173] As such, private school students may not be afforded the same Fourth Amendment rights as public school students, because private school officials are not considered state actors.[174] The same holds true for the First Amendment.[175] Further, even if a private or parochial school did receive government funding, that fact alone would not necessarily make it a "state actor" for purposes of the First and Fourth Amendments.[176] Therefore, all of the privacy legislation discussed in the following section, though limited, may still be more robust than what is afforded to private school students.

A. Federal & State Privacy Statutes Are Outdated

The patchwork of privacy-related statutes at the federal and state levels fails to squarely address the issues related to school device surveillance. Federal privacy statutes were written before the widespread prevalence of the internet in education and are outdated for the purpose of protecting children.[177] In addition, while a majority of states have student privacy laws, they also fall short of providing adequate protections for students.

---

171. 20 U.S.C. § 1232g.

172. *To Which Educational Agencies or Institutions Does FERPA Apply?*, U.S. DEP'T. OF EDUC., http://studentprivacy.ed.gov/faq/which-educational-agencies-or-institutions-does-ferpa-apply [https://perma.cc/EG28-UQTT].

173. U.S. CONST. amend. XIV.

174. State courts have interpreted Supreme Court precedent to suggest that the Fourth Amendment would not apply to private school employees because such employees are not government agents. *See In re* Devon T., 585 A.2d 1287, 1300 n.7 (Md. Ct. Spec. App. 1991) (interpreting *New Jersey v. T.L.O.*, 469 U.S. 325 (1985)).

175. The First Amendment only applies to government actions. *See* U.S. CONST. amend. I ("*Congress* shall make no law . . . abridging the freedom of speech." (emphasis added)). However, state law may apply to private schools. *See* CAL. EDUC. CODE § 48950 (2011) (prohibiting disciplinary action against high school students based on behavior protected by the First Amendment).

176. *See* Rendell-Baker v. Kohn, 457 U.S. 830, 832–43 (1982) (holding that there was not enough of a "symbiotic relationship" between a private school and the State to render the school a "state actor," despite the fact that ninety percent of the school's funding derived from government funding).

177. The relevant federal statutes were passed more than twenty years ago, when only twenty-one percent of children used the internet at home for school-related tasks. *See* ANNE KLEINER & ELIZABETH FARRIS, WESTAT, INTERNET ACCESS IN U.S. PUBLIC SCHOOLS AND CLASSROOMS: 1994–2001, NAT'L CTR. FOR EDUC. STATS., U.S. DEP'T OF EDUC. 1, 5 (2002), http://nces.ed.gov/pubs2002/2002018.pdf [https://perma.cc/7XV7-6FL5]; *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (July 2020), http://www.ftc.gov/business-

1. COPPA

The Children's Online Privacy Protection Act (COPPA)[178] is a federal law implemented by the Federal Trade Commission (FTC).[179] COPPA applies to operators of websites or online services that either target children or knowingly collect personal information from children under the age of thirteen.[180] Along with required consent, COPPA includes limitations on mandatory collection, use for commercial purposes (such as marketing or advertising), and retention for longer than is necessary to fulfill the purpose for which information was collected.[181]

Student device surveillance companies, like Gaggle, are considered operators under COPPA.[182] Disconcertingly, schools can act as a parent's agent and consent on their behalf to the collection of the child's information within the educational context.[183] When verifiable parental consent is required, schools can act as an intermediary to obtain this consent.[184] In such cases, "[a]s long as the operator limits use of the child's information to the educational context authorized by the school, the operator can presume that the school's authorization is based on the school having obtained the parent's consent."[185] Therefore, the operator (in this case, the student surveillance company) need not obtain consent directly from parents.[186] In addition, COPPA only applies to children under thirteen years of age.[187] Because schools both administer student accounts/devices and have the ability to consent, third party surveillance companies likely meet COPPA's parental consent obligations.[188]

---

guidance/resources/complying-coppa-frequently-asked-questions [https://perma.cc/3AH3-M22G]; *Legislative History of Major FERPA Provisions*, U.S. DEP'T OF EDUC. 1, http://studentprivacy.ed.gov/sites/default/files/resource_document/file/ferpaleghistory.pdf [https://perma.cc/U3FS-T2QJ] (last updated June 2002).

178. 15 U.S.C. §§ 6501–6506.

179. *Id.*; 16 C.F.R. § 312 (2013).

180. 15 U.S.C. § 6501(2).

181. *Id.* § 6502(b).

182. *Id.* § 6501(2); *see also COPPA*, GAGGLE.NET, http://cdn.gaggle.net/coppa.html [https://perma.cc/8DVX-G7JD] ("Use of the Free Version of Gaggle implies that your school is acting as a proxy for parental consent and agrees to the advertising, data collection, and terms of service of the Gaggle web site.").

183. *See Complying with COPPA: Frequently Asked Questions*, *supra* note 177.

184. *Id.*

185. *Id.*

186. *Id.*

187. 15 U.S.C. § 6501(1); 16 C.F.R. § 312 (2013).

188. *See, e.g.*, *Student and Staff Data Privacy Notice*, GAGGLE, http://www.gaggle.net/student-data-privacy-notice [https://perma.cc/A6TT-F6H9] (last updated July 17, 2023) (stating explicitly that Gaggle's services comply with COPPA).

However, surveillance companies must still ensure they comply with other aspects of COPPA, including providing for a parent's right to review and delete their child's personal information, posting a privacy policy online, and implementing reasonable procedures to protect kids' data.[189]

2. FERPA

The Family Educational Rights and Privacy Act[190] is a federal law administered by the U.S. Department of Education.[191] Congress enacted FERPA in 1974, almost fifty years ago, and last amended it in 2001.[192] FERPA largely contemplates paper files on each student, not the vast digital surveillance that occurs today.[193] The inherent "limited portability, permeability, and ability to repurpose paper records" meant FERPA, at the time it was enacted, implicitly prevented the disclosure and access of student information.[194] However, this context is outdated in today's digital world.

FERPA applies to all schools that receive funding from the Department of Education.[195] The law grants parents (and students age eighteen and older) access to information in the student's education record.[196] The educational records protected include "those records that are (1) [d]irectly related to a student; and (2) [m]aintained by an educational agency or institution or by a party acting for the agency or institution."[197] FERPA also protects that information by preventing disclosure to third parties without parental consent, subject to certain exceptions.[198]

One of FERPA's exceptions, the school official exception, allows a qualified "school official" to "release student records [without consent] for any educational purpose they deem legitimate."[199] The definition of "school official" includes teachers, counselors, and school administrative

189. *See Complying with COPPA: Frequently Asked Questions*, *supra* note 177.

190. 20 U.S.C. § 1232g.

191. *Id.*; 34 C.F.R. § 99.

192. *Legislative History of Major FERPA Provisions*, *supra* note 175; *see also* 121 CONG. REC. 13,990 (1975) (statement of Sen. James Buckley) (noting FERPA was originally enacted in response to "the growing evidence of the abuse of student records across the nation").

193. *See* 121 CONG. REC. 13,990 (1975) (statement of Sen. James Buckley).

194. Zeide, *Student Privacy Principles*, *supra* note 89, at 343.

195. 20 U.S.C. § 1232g; 34 C.F.R. § 99 (1988).

196. 20 U.S.C. § 1232g.

197. 34 C.F.R. § 99.3 (2011).

198. 20 U.S.C. § 1232g; 34 C.F.R. § 99 (1988).

199. 34 C.F.R. § 99.31 (2011); *FERPA: What It Means and How It Works*, STUDENT PRESS L. CTR., http://splc.org/ferpa-what-it-means-and-how-it-works/ [https://perma.cc/3ZCL-TNEY].

staff.[200] Critically, it also includes third parties who (1) perform "an institutional service or function" on behalf of the school; (2) are under direct control of the school "with respect to the use and maintenance of education records;" (3) are subject to FERPA requirements regarding disclosure; and (4) meet the definition of being a school official with "legitimate educational interests" in the education records.[201] In practice, the limits of an appropriate "school official" and "legitimate educational interest" are tenuous.[202] Because the statute delegates decision-making to schools about what qualifies as a "legitimate educational purpose," it "permit[s] schools to share student information for virtually unlimited purposes as long as they [can] provide a justification that [furthers] a legitimate educational interest."[203] This broad scope gives school districts significant discretion when sharing information externally, so long as they can provide an acceptable explanation.[204]

In 2008 and 2011, the Department of Education expanded its definition of "school officials" to include parties with whom a school contracts for institutional services.[205] Following this change, schools can release student records to companies that contract to provide surveillance software without violating FERPA, essentially delegating data-related decision-making to educators and third-party companies.[206] Further, as mentioned above, opting out is likely unrealistic in the school context.[207]

Because federal privacy legislation is outdated and does not provide robust protections for children's privacy rights, it may be necessary to turn to other enforcement mechanisms to combat the widespread discretionary use of surveillance software on school-issued devices and accounts.

3. State Laws Are a Mixed Bag

While certainly beneficial, the laws many states have in place to regulate cyberbullying also allow vast and unregulated surveillance over students.[208] Although some surveillance may be warranted, "the majority

200. 34 C.F.R. §§ 99.31(a)(1)(i)(A)–(B) (2011).

201. *Id.* § 99.31(a)(1)(i).

202. Zeide, *Student Privacy Principles*, *supra* note 89, at 365.

203. *Id.* at 367–68.

204. *Id.*

205. *Id.* at 360.

206. *Id.* at 364–65.

207. *See supra* section I.C.

208. *See Laws, Policies & Regulations*, U.S. DEP'T HEALTH & HUM. SERVS., http://www.stopbullying.gov/resources/laws [https://perma.cc/Y6RA-EGX5]; Emily F. Suski, *Beyond the Schoolhouse Gates: The Unprecedented Expansion of School Surveillance Authority Under Cyberbullying Laws*, 65 CASE W. RES. L. REV. 63, 104 (2014).

of the cyberbullying laws implicitly give schools unlimited, or nearly unlimited, and unfettered surveillance authority over students' online and electronic activity whenever, wherever, and however it occurs."[209] As such, a majority of states have at least one student privacy law on the books.[210] California is one example of this trend.[211] Florida takes an alternate approach by mandating the creation of a student database combining information across state agencies and public social media accounts.[212] Thus, California and Florida provide contrasting pictures of state laws relating to student surveillance and student privacy protections.

In California, the Student Online Personal Information Protection Act (SOPIPA)[213] regulates the industry known as "SUPER" (student user privacy in education rights).[214] SOPIPA protects students from having their data shared for noneducational purposes, for example selling their information for targeted advertising purposes.[215] This law directly affects educational technology providers by prohibiting them from "selling student data, using that information to advertise to students or their families, or 'amassing a profile' on students to be used for noneducational purposes."[216] SOPIPA is a model for protecting student data and ensuring that third parties, and not only school districts, are held liable for sharing and using student data for prohibited purposes (in contrast to federal law, like FERPA, which applies directly to schools).[217] In addition, rights under SOPIPA cannot be waived, even with consent.[218] This model strengthens privacy protections as—absent SOPIPA—schools, parents, and students may feel greater pressure to give consent.[219] However, even

209. Suski, *supra* note 208, at 63.

210. Kristie Lindell, *Student Data Privacy Regulations Across the U.S.: A Look at How Minnesota, California and Others Handle Privacy*, INSTRUCTURE (June 17, 2022), http://learnplatform.com/blog/edtech-management/student-data-privacy-regulations [https://perma.cc/2CFQ-HY2C].

211. CAL. BUS. & PROF. CODE § 22584 (2016).

212. Benjamin Herold, *To Stop School Shootings, Fla. Will Merge Government Data, Social Media Posts*, EDUC. WK. (July 26, 2018), http://www.edweek.org/technology/to-stop-school-shootings-fla-will-merge-government-data-social-media-posts/2018/07 [https://perma.cc/279A-4UD6].

213. CAL. BUS. & PROF. CODE § 22584 (2016).

214. *Id.*; FPF GUIDE TO PROTECTING STUDENT DATA UNDER SOPIPA: FOR K-12 SCHOOL ADMINISTRATORS AND ED TECH VENDORS, FUTURE OF PRIV. F. (2016), https://fpf.org/wp-content/uploads/2016/11/SOPIPA-Guide_Nov-4-2016.pdf [https://perma.cc/2K74-7383].

215. *See* Zeide, *Education Technology*, *supra* note 62, at 80.

216. CAL. BUS. & PROF. CODE § 22584 (2016); *Student Online Personal Information Protection Act (SOPIPA)*, COMMON SENSE MEDIA, http://www.commonsensemedia.org/kids-action/about-us/our-issues/digital-life/sopipa [https://perma.cc/KC2C-7YUE].

217. CAL. BUS. & PROF. CODE § 22584 (2016); COMMON SENSE MEDIA, *supra* note 216.

218. COMMON SENSE MEDIA, *supra* note 216.

219. *See id.*; *supra* section I.C.

under laws that restrict the processing of student information for noneducational purposes, "[p]rivate companies [like Gaggle] can legally use student data in ways that worry parents and advocates."[220]

In contrast, Florida recently enacted a law explicitly authorizing and *requiring* the creation of a centralized database to share students' data among a broader group of entities, including social services agencies, social media companies, and law enforcement.[221] This centralized database combines the criminal record, social service record, and social media history of each student and "provides school officials, law enforcement, and other state actors with a network of surveillance capabilities for potentially unknown purposes."[222] By improving timely access to a more complete set of information on each student, this law aims to enable "threat assessment teams" to more quickly detect and provide intervention when threats are identified.[223] Since the data is shareable among government agencies, "the idea [is] that red flags in student behavior or discipline could be detectable across bureaucratic divides."[224] However, a Florida Department of Education attorney warned that the database is unable to act as a "crystal ball" and "will not prevent school shootings or threats."[225]

This database implicates and heightens many of the concerns described in this Comment—especially how increased surveillance harms certain protected groups of students.[226] After an executive order from Florida Governor Ron DeSantis urged expediated action,[227] the State's Department of Education quietly announced that it had enacted the new

220. Zeide, *Education Technology*, *supra* note 62, at 84.

221. Benjamin Herold, *Florida Plan for a Huge Database to Stop School Shootings Hits Delays, Legal Questions*, EDUC. WK. (May 30, 2019), https://www.edweek.org/leadership/florida-plan-for-a-huge-database-to-stop-school-shootings-hits-delays-legal-questions/2019/05 [https://perma.cc/Z3XQ-9MVF].

222. Froelich, *supra* note 7, at 122.

223. Press Release, Fla. Dep't of Educ., Department of Education Announces the Florida Schools Safety Portal (Aug. 1, 2019), https://www.fldoe.org/newsroom/latest-news/department-of-education-announces-the-florida-schools-safety-portal.stml [https://perma.cc/UAJ3-BKV8] [hereinafter Fla. Dep't of Educ.].

224. Emily L. Mahoney, *Civil Rights Groups Raise Privacy Concerns over Post-Parkland School Security Database*, TAMPA BAY TIMES (July 9, 2019), https://www.tampabay.com/florida-politics/buzz/2019/07/09/civil-rights-groups-raise-privacy-concerns-over-post-parkland-school-security-database/ [https://perma.cc/E45H-G8AW].

225. *Privacy Advocates Express Concern Over Florida Schools Safety Portal for Preventing School Shootings*, CBS NEWS MIA. (Feb. 19, 2020), https://www.cbsnews.com/miami/news/privacy-florida-schools-safety-portal-preventing-school-shootings/ [https://perma.cc/F4P6-V9BT].

226. *See supra* section I.C.3.

227. *See* Fla. Exec. Order No. 19-45 (Feb. 13, 2019).

Florida Schools Safety Portal.[228] The scope of the data potentially shared could include the Florida Department of Law Enforcement's criminal intelligence information sharing platform, Florida Department of Children and Families child welfare records, Florida Department of Juvenile Justice records, and Florida Department of Education records.[229] Despite assurance that the portal "ensures compliance with all applicable state and federal privacy requirements," the fact that confidential education, health, and law enforcement data is now combined into student profiles that are available to certain school officials and law enforcement belies this assurance.[230]

B. Fourth Amendment Implications

Fourth Amendment jurisprudence related to school searches seeks to balance student privacy interests with school interests in safety and discipline. In the principal school search case, *New Jersey v. T.L.O.*,[231] the Supreme Court held that the Fourth Amendment's prohibition on unreasonable searches applies to searches by public school officials.[232] In *T.L.O.*, a school official searched a student's purse after discovering the student smoking in the bathroom.[233] The student challenged the search as "unreasonable" in violation of the Fourth Amendment.[234] While recognizing that students do not give up all of their Fourth Amendment rights when entering school grounds, the Court explained that "school officials need not obtain a warrant before searching a student" if they suspect a violation of school rules or the law.[235] Although the Court ultimately held that the search was reasonable, *T.L.O.* serves as a guiding principle when applying the Fourth Amendment to school searches.[236]

In *T.L.O.*, the Court created a standard that considers the "reasonableness, under all the circumstances, of the search."[237] Determining what is "reasonable" requires balancing "the child's interest in privacy" and "the substantial interest of teachers and administrators in

228. *See* Fla. Dep't of Educ., *supra* note 223; FLA. STAT. § 1001.212 (2023).
229. Fla. Dep't of Educ., *supra* note 223.
230. *Id.*
231. 469 U.S. 325 (1985).
232. *Id.* at 333.
233. *Id.* at 328.
234. *Id.* at 329.
235. *Id.* at 326.
236. *Id.* at 332–33.
237. *Id.* at 341.

maintaining discipline in the classroom and on school grounds."[238] The reasonableness standard has two prongs: (1) whether the "action was justified at its inception," and (2) whether the actually conducted search "was reasonably related in scope to the circumstances which justified the interference in the first place."[239] This flexible standard allows school officials ample latitude in conducting searches of students at school.[240]

The Supreme Court further expanded this doctrine in subsequent cases by routinely upholding suspicionless searches in school settings for participants in competitive extracurricular activities.[241] In both *Board of Education v. Earls*[242] and *Vernonia School District 47J v. Acton*,[243] the Court upheld drug testing requirements without suspicion of drug use. For suspicionless searches, the Court applies three factors: (1) "the nature of the privacy interest allegedly compromised," (2) "the character of the intrusion imposed," and (3) "the nature and immediacy of the government's concerns and the efficacy of the [p]olicy in meeting them."[244] As in *T.L.O.*, the Court used a balancing test, weighing student privacy interests against government (school) interests.[245] While each of these cases concerned physical searches, school districts across the United States use these cases "as guidelines when conducting searches and implementing new methods of student surveillance."[246] This is true despite the fact that these cases "were decided prior to the technologically advanced and invasive surveillance methods used by school districts today."[247]

The Supreme Court has not ruled on any case regarding searches by school officials that occur off-campus. However, student device and account surveillance in its present state may fail the *T.L.O.* reasonableness

238. *Id.* at 339.

239. *Id.* at 341 (quoting Terry v. Ohio, 392 U.S. 1, 20 (1968)).

240. *Id.* at 341–43.

241. *See, e.g.*, Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 664–65 (1995) (holding that any student athlete could be tested without reasonable suspicion); Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls, 536 U.S. 822, 838 (2002) (applying the same standard to students participating in a competitive extracurricular); *cf.* Safford Unified Sch. Dist. #1 v. Redding, 557 U.S. 364, 368 (2009) (finding that a strip search of a thirteen-year-old female student was unreasonable despite school's reasonable suspicion that she possessed prescription ibuprofen).

242. 536 U.S. 822 (2002).

243. 515 U.S. 646 (1995).

244. *Earls*, 536 U.S. at 830–38.

245. *Id.* at 828 n.3.

246. Froelich, *supra* note 7, at 131–32.

247. *Id.* at 132.

test.[248] First, it likely fails the "justified at its inception" prong because such broad surveillance is likely too far-reaching to be considered necessary. Schools may argue that an increase in school violence, bullying, and other similar problems justify the "search." However, one can rebut that the extremely broad nature of the search (a scope which includes everything on a student's school-issued device, at all hours of the day) is not justified.

Second, constant student device and account monitoring is not reasonable in relation to the circumstances that originally justified the search. Although threats of school violence and bullying are real dangers, that likely does not warrant the constant monitoring associated with student device surveillance. Unlike in *Earls* and *Vernonia*, the students being monitored are not a specific subset of students opting in to certain extracurriculars or activities; it is the entire student body. Comparing the student privacy interests at risk with the schools' interest, the clunky nature of this suspicionless surveillance should weigh in favor of students.

While the Fourth Amendment could provide additional protections to students under these standards, the Supreme Court has not yet interpreted it to. Consequently, there is a strong need for additional regulations.

C. First Amendment Implications

In 1969, the Supreme Court recognized that the First Amendment's freedom of speech protection extends to students, although it is limited in light of the "special characteristics of the school environment."[249] Indeed, the Court has stated that the government does not have "a free-floating power to restrict the ideas to which children may be exposed."[250] Supreme Court rulings related to students in the school setting attempt to balance the important privacy rights of students with essential school interests,[251] and the Court has stated that students do not "shed their constitutional rights . . . at the schoolhouse gate."[252] In *Tinker v. Des Moines Independent School District*[253] and *Mahanoy Area School District v.*

248. Suski, *supra* note 208, at 96–97 (arguing that school surveillance "allows for the unjustified collection of potentially vast amounts of information communicated by students electronically at any time, thus demonstrating the expansion of school authority under cyberbullying laws far beyond the boundaries of school and the school day").

249. Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 506 (1969).

250. Brown v. Ent. Merchs. Ass'n, 564 U.S. 786, 794–95 (2011).

251. *See, e.g.*, *Tinker*, 393 U.S. at 506–07 (establishing a student right to free speech); New Jersey v. T.L.O., 469 U.S. 325, 326 (1985) (establishing a student right against unreasonable search and seizure).

252. *Tinker*, 393 U.S. at 506.

253. 393 U.S. 503 (1969).

B.L.,[254] the Court decided how the First Amendment applies to on- and off-campus speech, respectively. However, several of the cases discussed below were decided in an era before widespread use of the internet in schools. Further, these cases do not address off-campus speech on school devices. As such, there is significant space ahead for further student privacy protections.

1. On-Campus Speech

In *Tinker*, the seminal school free speech case, the Supreme Court clarified freedom of speech protections in the school setting after students were suspended for wearing black armbands to their high school to protest the Vietnam War.[255] When the school hastily passed a policy stating that students who refused to remove armbands would be suspended, multiple students wore their armbands to school and were sent home.[256] The students sued the district for violating their First Amendment right of expression and sought to enjoin the district from disciplining them.[257] The Supreme Court agreed, holding that the students' rights to free speech were violated.[258]

The *Tinker* Court created the "substantial interference" test to decide when school officials' suppression of student speech would not violate the First Amendment.[259] The Court held that school officials can regulate student speech *only* when it "materially and substantially interfere[s]" with the learning environment.[260] Although this test limits the constitutional rights of students, the Court outlined that for "school officials to justify prohibition of a particular expression of opinion, [they] must be able to show that [their] action was caused by something more than a mere desire to avoid the discomfort and unpleasantness that always accompany an unpopular viewpoint."[261] In addition, the Court highlighted that a school regulation either forbidding discussion of or opposition to the Vietnam conflict altogether would "obvious[ly] . . . violate the constitutional rights of students."[262]

254. 594 U.S. ____, 141 S. Ct. 2038 (2021).

255. *Tinker*, 393 U.S. at 504.

256. *Id.*

257. *Id.*

258. *Id.* at 510 ("In the absence of a specific showing of constitutionally valid reasons to regulate their speech, students are entitled to freedom of expression of their views.").

259. *Id.* at 512–13.

260. *Id.*

261. *Id.* at 509.

262. *Id.* at 513.

2. Off-Campus Speech

Although the conduct in *Tinker* occurred on school premises, the Supreme Court emphasized that "conduct by the student, in class *or out of it*, which for any reason . . . materially disrupts classwork or involves substantial disorder or invasion of the rights of others, is . . . not immunized by the constitutional guarantee of freedom of speech."[263] This decision set the stage for further regulations of student conduct outside the school setting. In *Mahanoy*, the Supreme Court reinforced students' First Amendment rights, this time involving the use of technology off school premises. In *Mahanoy*, a student posted a picture of herself to the social media app Snapchat with the caption "[f]uck school fuck softball fuck cheer fuck everything."[264] After the picture was shared with several followers, it eventually made its way to the student's coaches, who suspended the student from junior varsity cheerleading for the upcoming year.[265]

In holding that student speech was protected, the Court affirmed *Tinker*'s substantial interference test applied to off-campus speech.[266] The Court failed to set an all-encompassing rule regarding off-campus speech, writing: "[p]articularly given the advent of computer-based learning, we hesitate to determine precisely which of many school-related off-campus activities" would be considered school speech.[267] However, despite failing to set a broad rule, the Court outlined three features of off-campus speech that "diminish the strength of the unique educational characteristics that might call for special First Amendment leeway" and may afford students stronger constitutional protections.[268] First, off-campus speech typically falls "within the zone of parental, rather than school-related, responsibility."[269] Second, the combination of on- and off-campus speech regulations may necessarily "include all the speech a student utters during the full 24-hour day."[270] With the realistic assumption of on-campus speech regulation, the addition of off-campus speech regulation becomes more burdensome on a student. As such, courts should be skeptical of a school's attempts to regulate off-campus speech, because it is important

263. *Id.* at 504, 513 (emphasis added).

264. Mahanoy Area Sch. Dist. v. B.L., 594 U.S. __, 141 S. Ct. 2038, 2043 (2021).

265. *Id.*

266. *Id.* at 2045.

267. *Id.*

268. *Id.* at 2046.

269. *Id.* (noting that schools "will rarely stand *in loco parentis*" when regulating off-campus speech (emphasis added)).

270. *Id.*

for students to have some outlet to speak freely.[271] Third, schools themselves have an interest in protecting a student's off-campus speech.[272] The Court emphasized that the free marketplace of ideas, even unpopular ideas, is an important cornerstone of democracy, and it is critical that students' education puts this into practice.[273]

Although the Court recognized compelling school interests, it found that the privacy interests of the student held greater weight.[274] First, although the school had an interest in punishing the use of vulgar language, this interest was "weakened considerably" by the fact that the speech occurred outside the school.[275] In addition, the school presented no evidence of any other efforts "to prevent students from using vulgarity outside the classroom."[276] On balance, the interest in punishing vulgar language did not outweigh the student's interest in free expression.[277] Second, the school presented no evidence that the cheerleader's conduct was a "'substantial disruption' of a school activity or a threatened harm to the rights of others."[278] Thus, under the *Tinker* test, the school's actions were not justified.[279] Recharacterizing the *Tinker* standard as "demanding," the Court found that the social media post did not rise to the level of conduct that would substantially disrupt school activities.[280] Finally, in response to the school's argument that the student's comments would negatively impact team morale, the Court expressed skepticism that a concern for "morale" would ever justify a "substantial disruption" of school activities.[281] In concluding the majority opinion, Justice Breyer emphasized that even "superfluous" speech should be protected.[282] In a concurring opinion, Justice Alito emphasized that "school officials should proceed cautiously before" regulating the "many types of off-premises

271. *Id.*

272. *Id.*

273. *Id.*; *see also supra* section I.C.1 (describing how increased surveillance can restrict students' intellectual privacy, which is especially important in a school setting).

274. *Mahanoy*, 141 S. Ct. at 2047.

275. *Id.* (highlighting examples where, if the student delivered the same speech outside the school context, it would have been protected).

276. *Id.*

277. *Id.*

278. *Id.* (citing Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 514 (1969)).

279. *Id.* at 2048.

280. *Id.*

281. *Id.*

282. *Id.*

student speech."[283] A recurring concern for stifling off-campus student speech ran throughout both opinions.[284]

In sum, the current legal landscape includes federal and state laws, the Fourth Amendment, and the First Amendment. First, privacy-related statutes were largely written before the prevalence of the internet in education and fall short of adequately protecting students. Next, Fourth Amendment jurisprudence fails to specifically address off-campus searches and may not meet the *T.L.O.* reasonableness test. Finally, First Amendment jurisprudence leaves unclear the question of off-campus speech on school devices. As it currently stands, this legal landscape inadequately protects student privacy.

III. SOLUTIONS

As student surveillance on school-issued devices may run afoul of the Fourth and First Amendments, the current Supreme Court should act to strengthen student privacy protections. Even if the Supreme Court did increase student privacy protections,[285] action should be taken at the federal, state, and school district levels to protect student privacy.

A. The Supreme Court Should Clarify Speech on School-Issued Devices

While the Supreme Court has attempted to balance students' privacy rights with important school interests,[286] most cases on this topic were decided before the widespread use of school-issued devices at home. Student speech on school-issued devices and accounts, when conducted off school premises, appears to fall somewhere in between on-campus and off-campus speech. One can argue that this type of speech leans more towards on-campus speech, given that it occurs on a school-issued device

283. *Id.* at 2059 (Alito, J., concurring).

284. *Id.* at 2044 (majority opinion) ("[M]inors are entitled to a significant measure of First Amendment protection." (alteration in original) (quotation marks omitted) (quoting Brown v. Ent. Merchs. Ass'n., 564 U.S. 786, 794 (2011)); *see also id.* at 2054 (Alito, J., concurring) ("While the in-school restrictions discussed above are essential to the operation of a public school system, any argument in favor of expansive regulation of off-premises speech must contend with this fundamental free-speech principle.").

285. In addition, the Supreme Court may be hesitant to act to strengthen students' rights, such as free speech. *Id.* at 2059 (Thomas, J., dissenting) (arguing against increased student protections because "schools historically could discipline students in circumstances like those presented here," including "for off-campus speech or conduct that had a proximate tendency to harm the school environment").

286. *See, e.g.*, Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503 (1969) (student right to free speech); New Jersey v. T.L.O., 469 U.S. 325 (1985) (student right against unreasonable search and seizure).

or account. Some of the speech may be directly school-related, for example in Word documents for school assignments. However, if a student searches on YouTube at 2:00 a.m., when they are at home, is that still on-campus speech? The constant monitoring leads to questions of whether this might necessarily include *all* online speech of students, especially if students have limited access to the internet outside of that particular school-issued device.[287] As stated in *Mahanoy*, the courts should be skeptical of additional regulation of speech because it is important that students have outlets to freely express themselves.[288]

While a student's First Amendment rights are not absolute, there must be some guidelines in place for when a student uses their school device and account off-campus. Perhaps the question should not be whether the speech occurred on-campus or off-campus, but instead whether the speech can be disciplined by a school. The substantial disruption test in *Tinker* does not provide enough guidance for the current use of surveillance software on school-issued devices or accounts and the resulting disciplinary actions that occur.[289]

As such, the Supreme Court should adopt discrete categories of "school speech" that are subject to discipline. First, speech that threatens the school community should be classified as "school speech" and removed from First Amendment protections. This would include speech that implicates safety concerns, such as threats of violence, as well as mental health issues that may indicate self-harm. Speech that breaches school security, such as instructions for hacking into the school's computer system, would also qualify here.[290] Second, speech that intentionally targets certain individuals or groups may qualify as "school speech" subject to discipline or regulation. This captures bullying and harassment that may not reach the level of a threat but nevertheless detracts from the school environment, even when occurring off campus. Importantly, off-campus speech that does not fall under the "school speech" category will *not* subject students to discipline. This will diminish the school-to-prison pipeline by reducing the amount of disciplinary interactions a student may have, thus lessening or even removing them from that cycle.[291]

In sum, it is important to balance constitutional student speech interests with school interests in educating and protecting students. Schools that

---

287. *See Mahanoy*, 141 S. Ct. at 2045–46.

288. *See supra* section I.C.1.

289. *Tinker*, 393 U.S. at 512–13.

290. *See* Brief for the United States as Amicus Curiae Supporting Petitioner at 20, Mahanoy Area Sch. Dist. v. B.L., 594 U.S. __, 141 S. Ct. 2038 (2021) (No. 20-255), 2021 WL 859695, at *20.

291. *See supra* section I.C.2. If a student is not disciplined in the first place, they will not be in a cycle of getting in trouble that may eventually escalate and lead to interactions with law enforcement.

wish to regulate additional content can always add internet filters on their devices to ensure students act as the school deems appropriate. The Supreme Court should enumerate a few distinct categories of "school speech" subject to school discipline to ensure that student speech is not constantly restrained.

B. New Federal and State Laws Can Protect Student Privacy

Congress will ideally act to remedy this issue so that federal law will mandate student privacy protections nationwide.[292] Individual states can also strengthen existing laws or pass new laws to bolster privacy protections. Such legislation should limit the sharing of student data, minimize the data that is collected, and address the potential harms of surveillance.

First, data collected from software on school-issued devices at home should not be extensively shared. Although FERPA's school official exception exists to limit sharing, in practice it allows anyone performing a school function to receive data from schools.[293] This provides wide discretion to school officials in deciding with whom they contract and share data.[294] Schools should be *required* to regularly evaluate with whom they share data and include robust limitations in contracts with third parties.[295] For example, data that is not directly related to student safety should not be shared with law enforcement. A more robust sharing limitation would essentially be a subset of a use limitation, which is a common principle in modern privacy frameworks.[296] If legislators

---

292. A report by Senators Elizabeth Warren and Ed Markey called for "federal action to protect students' civil rights, safety, and privacy." Press Release, Elizabeth Warren, United States Senator, Warren, Markey Investigation Finds that EdTech Student Surveillance Platforms Need Urgent Federal Action to Protect Students (Mar. 30, 2022), https://www.warren.senate.gov/oversight/reports/warren-markey-investigation-finds-that-edtech-student-surveillance-platforms-need-urgent-federal-action-to-protect-students [https://perma.cc/DR6S-BSWG].

293. *Who Is a "School Official" Under FERPA?*, U.S. DEP'T OF EDUC., https://studentprivacy.ed.gov/faq/who-school-official-under-ferpa [https://perma.cc/U83C-TZ2N].

294. *See supra* section II.A.2.

295. *See, e.g.*, *supra* section III.C (proposing audits); *FTC Proposes Strengthening Children's Privacy Rule to Further Limit Companies' Ability to Monetize Children's Data*, FED. TRADE COMM'N (Dec. 20, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/ftc-proposes-strengthening-childrens-privacy-rule-further-limit-companies-ability-monetize-childrens [https://perma.cc/9YPC-XJJG] (describing possible limits).

296. *See, e.g.*, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, OECD 15 (2002), https://doi.org/10.1787/9789264196391-en [https://perma.cc/ZTX5-LZJZ] (describing how the use limitation principle requires that "[p]ersonal data should not be disclosed, made available or otherwise used for purposes other than those specified . . . except with . . . consent of the data subject or . . . by the authority of law").

codified such a sharing limitation, schools would be prohibited from disclosing data, making data available to third parties, or otherwise using data for different purposes. Further, this recognizes that the use of surveillance does not always align with performing a school function. This would mitigate the school-to-prison pipeline by reducing law enforcement's ability to monitor students in non-critical situations. Thus, students would likely have less contact with law enforcement. For example, considering the rise in states criminalizing both abortion and gender-affirming care, this could serve to protect students' data related to abortion and gender-affirming care from being used against them by law enforcement. Federal or state legislation should create a stricter sharing limitation to ensure that data is only used for school functions.

Second, data minimization is key. Digital surveillance companies can maintain student data for long periods of time. This leads to fears of students having "a proverbial permanent record," that may be used against them in the future.[297] Such a record could limit students' academic prospects (being denied admission to college) or professional opportunities (being passed over for a job).[298] Federal or state legislation should *require* schools to minimize their use of surveillance technology and, more specifically, the actual data collected. In addition, schools should limit data they filter and collect—for example, removing certain terms from the flagged words list that triggers school official notification. This can better protect LGBTQIA2S+ students, to whom some monitored terms apply disproportionately, if health terms specific to LGBTQIA2S+ are no longer included on flagged word lists. This can also serve to strengthen students' access to intellectual privacy, which is especially important to cultivate while at school.[299] Limiting data collected will also lead to positive impacts on low-income students who are especially reliant on school-issued devices.

As with use limitations, data minimization is also a commonly included principle in modern privacy frameworks.[300] The General Data Protection Regulation (GDPR), an important cornerstone of privacy law in the European Union (EU), serves as a guideline.[301] Under the GDPR, for

297. ELANA ZEIDE, THE PROVERBIAL "PERMANENT RECORD," N.Y.U. SCH. OF L. INFO. L. INST. (2014).

298. Zeide, *Education Technology*, *supra* note 62, at 77.

299. *See* RICHARDS, *supra* note 92, at 95–108.

300. *See, e.g.*, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, On the Protection of Natural Persons with Regard to the Processing of Personal Data and On the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 35–36 (providing an example of a "data minimization" principle in the EU).

301. *Id.*

example, "[p]rocessing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed."[302] Data minimization would reduce the school-to-prison pipeline by limiting the search terms accessible by law enforcement to those directly related to safety. In addition, data limitation promotes intellectual privacy by reducing the number of terms that will trigger school notification, thus allowing students freer rein to use and search a broader set of information on their devices without fear of being punished. Including a data minimization requirement in federal legislation "would ensure baseline student privacy protection, without relying on ineffectual notice and consent mechanisms or institutional discretion."[303]

Finally, federal legislation should *require* school districts and surveillance companies to track the impact of student surveillance. Given the potential for disproportionate impact on certain student groups,[304] it is important to hold both the schools and surveillance companies accountable. The Department of Education already uses surveys to identify disproportionate rates of discipline for certain protected groups;[305] it could similarly collect data from schools on disproportionate impacts related to the use of student surveillance tools. In addition, companies that provide student account and device monitoring should be required to transparently examine the impact of their software on student groups. This would allow schools, parents, and even students themselves to be better informed, and would provide the companies with valuable information "to continually refine their products."[306]

Either federal or state governments could enact each of these solutions. To date, the majority of privacy legislation in the United States has been enacted by states.[307] Successfully passing legislation at the state level may be more realistic given the relative difficulty in passing federal

302. *Id.*; *see also Principles of Data Protection*, DATA PROT. COMM'N, https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection# [https://perma.cc/2H2H-9FMU] (describing what is required to comply with data minimization).

303. Zeide, *Student Privacy Principles*, *supra* note 89, at 389.

304. *See supra* section I.C.3.

305. WARREN & MARKEY, *supra* note 132, at 9.

306. *Id.*

307. *U.S. State Privacy Laws*, ELEC. PRIV. INFO. CTR., https://epic.org/issues/privacy-laws/state-laws/ [https://perma.cc/5TX4-P6UJ].

legislation.[308] And, in general, federal privacy laws have not historically preempted stronger state protections or enforcement.[309]

However, there are also reasons why federal legislation may be more compelling. Although there has historically not been federal preemption in the privacy sphere, the most recently proposed federal comprehensive data privacy bill faltered in part due to the California delegation's concerns over preemption of state privacy laws.[310] In addition, federal legislation would reach the entire country rather than create a patchwork of different laws with different protections in each state. In sum, there are pros and cons of each approach: while federal laws may take more time to enact, there is a risk of state privacy laws being preempted if later federal action does occur.

C. School Districts Should Act to Self-Regulate

In the absence of new federal or state laws protecting student privacy, school districts should act to protect their students. Along with implementing any of the solutions described above, school districts are particularly well positioned to conduct audits and increase transparency.

To begin, school districts should conduct audits when processing sensitive personal information. Under the GDPR, a Data Protection Impact Assessment (DPIA) is required any time a covered entity "begin[s] a new project . . . likely to involve a 'high risk' to other people's personal information."[311] Under EU laws, the current surveillance on students in the United States would likely already trigger a DPIA because it involves processing children's data.[312] However, even when a DPIA is not mandatory (as it will likely not be for U.S. schools processing information from U.S. data subjects only), schools should consider conducting a similar assessment to study the privacy impacts of this type of data processing. Not only can the practice of auditing highlight privacy risks at an early stage, but it can also show that the school is committed to

---

308. Roslyn Layton, *Washington Gridlock Will Put States at the Forefront of Tech Policy in 2023*, FORBES (Dec. 20, 2022), https://www.forbes.com/sites/roslynlayton/2022/12/20/washington-gridlock-will-put-states-at-the-forefront-of-tech-policy-in-2023/?sh=74f304001587 [https://perma.cc/EXN4-9S9M] (describing how "states will take the lead in technology policy as gridlock dominates Congress").

309. *U.S. State Privacy Laws*, *supra* note 307.

310. Joseph Duball, *State Views on Proposed ADPPA Preemption Come into Focus*, IAPP (Sept. 27, 2022), https://iapp.org/news/a/state-level-views-on-proposed-adppa-preemption-come-into-focus/ [https://perma.cc/S7K5-5LL6].

311. Ben Wolford, *Data Protection Impact Assessment (DPIA)*, GDPR, https://gdpr.eu/data-protection-impact-assessment-template/ [https://perma.cc/7Q7U-GP7H].

312. *Id.*

protecting its students' privacy.[313] In addition, schools can plan ahead and use DPIA findings to implement safeguards designed to mitigate risks such as those identified in this Comment.

Second, school districts should actively seek to increase transparency for both students and parents. Rather than merely signing a permission form, parents should have the opportunity to learn about the privacy and data collection practices of both the school and the surveillance company. In addition, school districts can take this opportunity to educate students about their privacy rights, both inside and outside of the school context.[314]

This proactive approach will lead to "greater understanding of the schools' and districts' data privacy policies and practices [and] will help alleviate confusion and misunderstandings about students' data use."[315] In fact, the Department of Education specifically recommends school districts going beyond the legal minimum requirements and providing parents with, for example, the following information: a data inventory of data elements collected, why each particular data element is collected, how the school's or district's policies protect personal information, and whether student information is shared with any third parties.[316] With increased transparency, parents will be better informed when deciding whether they feel comfortable with how the school processes their children's digital information. Additionally, students will learn the importance of managing their own privacy settings in today's digital age.

CONCLUSION

This issue is urgent. Every day, children and adolescents are in the process of actively developing their identities while under constant threat of privacy violations. If unaddressed, the costs of student surveillance may permanently affect students and, in turn, their—and our—future.

Schools may view student surveillance as "necessary," whether to manage learning, promote safety, or comply with perceived requirements

313. *See, e.g.*, Richard Morley, *Data Protection Impact Assessments – What Are They and Why Are They Important?*, SCHOOLPRO TLC (May 29, 2020), https://schoolpro.uk/2020/05/data-protection-impact-assessments-what-are-they-and-why-are-they-important/ [https://perma.cc/R93Q-VDP9] (highlighting that a DPIA can "demonstrat[e] that privacy is being taken seriously" and provide "evidence of an organisation's commitment to accountability").

314. The U.S. Department of Education advocates for openness when schools communicate about the student information they collect. *See* TRANSPARENCY BEST PRACTICES FOR SCHOOLS AND DISTRICTS, PRIV. TECH. ASSISTANCE CTR. (2014), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/LEA%20Transparency%20Best%20Practices%20final.pdf [https://perma.cc/7STJ-Q44B].

315. *Id.*

316. *Id.*

of federal laws.[317] However, as student surveillance has increased in recent years, the potential harms have also increased. These harms far outweigh any limited benefits. Surveillance of school accounts and school-issued devices, when conducted while students are not physically on school premises, infringes on students' most intimate data and spaces. Although this type of surveillance has important consequences, current federal, state, and constitutional privacy protections for students are inadequate.

Schools are intended to be a place where children and adolescents learn, not only how to read and write, but also about who they are as individuals. However, the surveillance landscape fundamentally changes student behavior, leading to negative psychological and chilling effects. This can jeopardize students' health and safety if they fear using their school-issued device to access critical information on abortions or gender-affirming care in jurisdictions where obtaining such medical care is illegal. These negative consequences are particularly heightened for low-income students, LGBTQIA2S+ students, and students with disabilities.

Students should be free to develop and explore new ideas without feeling the need to guard their thoughts. Absent widespread surveillance of students' entire online presence, they will feel empowered to read, write, research, discuss, and create without fearing punishment. With increased privacy protections, students will again have intellectual privacy.

Students do not "shed their constitutional rights . . . at the schoolhouse gate."[318] Judicial, federal, state, and school district decisionmakers should act to ensure student privacy is adequately protected.

317. *See* HANKERSON ET AL., *supra* note 67, at 11, 15.

318. Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 506 (1969).