Student Privacy's Student Neglect: Toward a Student-Centric Paradigm

*Elana Zeide**

ABSTRACT

Student privacy law does not meaningfully protect students' privacy. As federal statutes such as the Family Educational Rights and Privacy Act and the Protection of Pupil Rights Amendment mark their fiftieth anniversaries, they prove inadequate in an era of technology-mediated and data-driven education. More critically, student privacy laws are not only outdated but reflect a fundamental misalignment of priorities and lack a coherent normative foundation. So-called "student privacy" frameworks center parents and institutions rather than students themselves.

As a result, they neglect the distinct privacy needs and developmental requirements of students. This Article offers the first conceptual analysis of student privacy law, employing a novel paradigmatic analysis to identify two dominant yet problematic approaches to information governance in education: parent-centric and school-centric paradigms. These frameworks privilege parental rights and institutional priorities while often conflating students' interests with those of children and subordinating their developmental needs to adult preferences.

This Article reconceptualizes student privacy as critical infrastructure for learning and development rather than merely a protective shield against external threats. To operationalize this reconceptualization, this Article proposes six core principles for a student-centric paradigm.

Grounded in interdisciplinary privacy scholarship and educational theory, the student-centric paradigm forms a foundation for student privacy and recognizes learners as primary stakeholders with developmental needs and intellectual agency. By reconceptualizing student privacy through a student-centric lens, this Article aims to shift the focus of privacy protections to better serve students' interests, support their development, and prepare them for the privacy challenges they will face as adults in an increasingly "datafied" society. The time has come to place students at the center where they belong—to put the student back into student privacy.

* Elana Zeide, Assistant Professor, University of Nebraska College of Law; Affiliated Fellow, Information Society Project, Yale Law School, Silicon Flatirons, University of Colorado-Boulder. I'm indebted to Jack Balkin, Lyrissa Lidsky, Paul Ohm, William McGeveran, Neil Richards, Woodrow Hartzog, Harry Surden, Gus Hurwitz, Derek Bambauer, Jane Bambauer, Meg Leta Jones, Margot Kaminski, Jevan Hutson, Thomas Healy, Mailyn Fidler, Kyle Langvardt, James Tierney, Abbie Jacobs, and Catherine Smith for their insights and to the participants of the Privacy Law Scholars Conference 2023 and the Faculties at the University of Florida and Loyola Law School for their feedback.

TABLE OF CONTENTS

INTRODUCTION 537
I. THEORIZING STUDENT PRIVACY 542
A. The Digital Transformation of Education 542
B. The Student Privacy Regulatory Framework and Its Limitations 549
C. Theoretical Limitations of Current Student Privacy Paradigms 554
II. THE DOMINANT "STUDENT" PRIVACY PARADIGMS 557
A. The Parent-Centric Paradigm 558
1. FERPA's Origins: Promoting Family Privacy 559
2. The PPRA: Pushing for Parental Oversight 562
3. Parental Rights Laws: Imposing Moral Values 566
B. The School-Centric Paradigm 567
1. FERPA's Exceptions: Granting Schools Discretion 568
2. FERPA's Modern Exceptions: Promoting Technocratic Reform 571
3. Enforcement: Reinforcing the School-Centric Paradigm 574
B. Competing Adult Priorities: Tensions Between the Parent-Centric and School-Centric Approaches 577
III. DECONSTRUCTING DOMINANT PARADIGMS: CRITIQUING PARENT-CENTRIC AND SCHOOL-CENTRIC APPROACHES 582
A. Parental Control and Its Limitations 583
1. Unrealistic Burden of Privacy Management 584
2. Disregard for Students' Evolving Capabilities and Autonomy 584
3. Subordination of Students' Interests to Parental Control 586
B. Institutional Power and Its Consequences 587
1. Expansive Institutional Discretion in Data Governance 588
2. Neglect of Students' Intellectual Privacy and Autonomy 588
3. Bias Amplification and Institutional Power 589
4. Insufficient Mechanisms for Transparency and Redress 591
C. Shared Shortcomings and the Need for a Student-Centric Approach 593
1. Failure to Center Students as Primary Stakeholders and Marginalizing Students'

Privacy Interests 593
2. Conflating Children with Learners 595
3. Neglecting Privacy's Constitutive Role in Education 596
IV. Toward a Student-Centric Paradigm 596
A. Core Principles for Student-Centric Privacy 597
1. Recognizing Students' Evolving Autonomy 597
2. Safeguarding Intellectual Privacy. 598
3. Promoting Educational Equity. 599
4. Guaranteeing Technological Due Process. 599
5. Promoting Democratic Values 600
6. Practicing Responsible Data Stewardship. 600
B. Limitations and Challenges 602
1. Legal and Policy Challenges 602
2. Institutional Barriers and Power Dynamics 603
3. Technological and Infrastructural Constraints 604
4. Addressing Potential Objections 604
C. Implications and Future Directions. 605
1. Implications and Benefits of the Student-Centric Paradigm. 605
2. Future Directions for Research and Policy 606
Conclusion 607

Introduction

Student privacy law fails to adequately protect students' privacy interests, not merely because of outdated provisions or technological changes, but due to fundamental theoretical deficiencies in its conceptualization and application within educational contexts. This Article challenges the conventional wisdom and legal frameworks that have governed the collection, use, and dissemination of student records for over half a century under the banner of "student privacy." It reveals a critical oversight: the conspicuous absence of students' own interests from the conversation.

Consider students' realities. Every day, Zahra removes her shoes, waiting in line for uniformed police officers to scan her ID and facial features and guide her through a metal detector. This isn't airport security—it's her high school. Such intensive security is more common in schools that predominantly serve students of color, damaging their psychological well-being and academic performance.[1] Even more

[1] *See generally* Jason P. Nance, *Student Surveillance, Racial Inequalities, and Implicit Racial Bias*, 66 Emory L.J. 765 (2017) (discussing data indicative of racial inequalities presented in school surveillance systems and proposing solutions to remove implicit bias from these systems).

alarmingly, minor infractions at these schools often trigger automatic alerts to law enforcement, feeding the school-to-prison pipeline.[2]

Meanwhile, Priya's school-issued computer tracks every keystroke, online search, and communication—even after school hours. Software installed on this machine flags keywords that might indicate cyberbullying, violent thoughts, or access to inappropriate material about, for example, reproductive health.[3] School officials pass these notes on to Priya's parents.[4] Even her online learning platforms keep tabs, noting the exact times she engages with course materials or rewatches a lecture,[5] while videoconferencing software records her throughout her online classes and tracks her eye movements to assess whether she is paying attention.[6]

Jordan worries about a different type of exposure. A proposed state law would require teachers to inform parents when students question their sexual orientation or gender identity.[7] Jordan identifies as nonbinary but has kept that secret from their family. The safe space of the classroom now feels like a trap. The risks are real and severe—Jordan's parents are vocally heteronormative, and LGBTQ+ youth rejected by their families are much more likely to attempt suicide.[8]

These scenarios highlight some of the privacy intrusions that students face today. They illustrate more than isolated privacy violations—they reveal systemic failures in how current legal frameworks conceptualize and protect student privacy. In an era of rapid technological advancement and data-driven decision-making, student privacy has emerged as a critical concern in educational policy and practice.[9] The digital

---

2 *Id.* at 788–89.

3 *See generally* Pia Ceres, *Kids Are Back in Classrooms and Laptops Are Still Spying on Them*, WIRED (Aug. 3, 2022, 12:01 AM), https://www.wired.com/story/student-monitoring-software-privacy-in-schools/ [https://perma.cc/B8GZ-722E] (discussing digital surveillance in classrooms in a "post-*Roe* era").

4 *See id.*

5 *See, e.g.*, Instructure, *Instructure Launches Canvas Admin Analytics, Providing Powerful LMS Engagement Insights to Help Administrators Drive Student Success*, PR NEWSWIRE (Mar. 30, 2023, 7:20 AM), https://www.prnewswire.com/news-releases/instructure-launches-canvas-admin-analytics-providing-powerful-lms-engagement-insights-to-help-administrators-drive-student-success-301785581.html [https://perma.cc/6KLW-SNEW].

6 *See, e.g.*, Susan Fourtané, *How to Measure Student Attention During Remote Learning*, FIERCE NETWORK, (Mar. 4, 2021, 8:30 AM), https://www.fierce-network.com/distance-learning/how-to-measure-student-attention-during-remote-learning [https://perma.cc/43EG-CHFU].

7 *See, e.g.*, S.B. 272, Reg. Sess. (N.H. 2023).

8 *See* Augustus Klein & Sarit A. Golub, *Family Rejection as a Predictor of Suicide Attempts and Substance Misuse Among Transgender and Gender Nonconforming Adults*, 3 LGBT HEALTH 193, 193 (2016), https://pubmed.ncbi.nlm.nih.gov/27046450/ [https://perma.cc/K55C-245S].

9 *See, e.g.*, April Glaser, *Students Coast to Coast Write Open Letters About the Effects of Government Surveillance on Academic Life*, ELEC. FRONTIER FOUND. (May 15, 2014), https://www.eff.org/deeplinks/2014/05/students-coast-coast-write-open-letters-about-effects-government-surveillance [https://perma.cc/ED2J-GNAU].

transformation of education has created unprecedented opportunities for personalized learning and administrative efficiency, but it has also exposed students to new privacy risks that existing legal frameworks struggle to address.[10] As educational institutions increasingly rely on complex data systems and third-party technology providers,[11] the question of how to protect student privacy while fostering innovation has become more urgent and complex than ever before.

Although policymakers promise action,[12] most focus narrowly on updating half-century-old laws to address new technologies.[13] These reforms, although essential, are incomplete.[14] This Article moves beyond technical critiques to address fundamental theoretical limitations in how student privacy is conceptualized, drawing on insights from privacy theory, education law, children's rights scholarship, and surveillance studies to expose the misalignment between student privacy law's purported purpose and its actual priorities.

It argues that addressing privacy concerns in education demands more than incremental reform to existing frameworks; they require a fundamental reconceptualization of student privacy to account for students' distinctive and evolving interests. For over fifty years, policymakers and scholars have characterized the laws governing

---

10 *See* Jules Polonetsky & Joseph Jerome, *Student Data: Trust, Transparency, and the Role of Consent*, Future Priv. F. 1 (Oct. 2014), https://fpf.org/wp-content/uploads/2014/10/FPF_Education_Consent_StudentData_Oct20141.pdf [https://perma.cc/U3DX-X99W].

11 *See id.* at 1–3.

12 For example, the U.S. Department of Education has published plans to promulgate new Protection of Pupil Rights Amendment regulations. *See Protection of Pupil Rights Amendments*, U.S. Off. Info. & Regul. Affs. (2022), https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202210&RIN=1875-AA13 [https://perma.cc/5WZD-SPMD]. Lawmakers have proposed legislation to bolster existing regulations by adding additional protections. *See, e.g.*, S.B. 272, Reg. Sess. (N.H. 2023). The Biden White House also pledged to address concerns about school information practices. *FACT SHEET: Biden-Harris Administration Announces Actions to Protect Youth Mental Health, Safety & Privacy Online*, White House (May 23, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/23/fact-sheet-biden-harris-administration-announces-actions-to-protect-youth-mental-health-safety-privacy-online/ [https://perma.cc/28TY-CQ4M].

13 *See, e.g.*, Joel R. Reidenberg, N. Cameron Russell, Jordan Kovnot, Thomas B. Norton, Ryan Cloutier & Daniela Alvarado, Fordham L. Sch. Ctr. on L. & Info. Pol'y, Privacy and Cloud Computing in Public Schools 18–65 (2013), https://ir.lawnet.fordham.edu/clip/2/ [https://perma.cc/52DR-VTFB]; Emmeline Taylor, *Recent Developments in Surveillance: An Overview of Body-Worn Cameras in Schools*, *in* The Palgrave International Handbook Of School Discipline, Surveillance, and Social Control 371, 379 (Jo Deakin, Emmeline Taylor & Aaron Kupchik eds., 2018); April Glaser, *Students Coast to Coast Write Open Letters About the Effects of Government Surveillance on Academic Life*, Elec. Frontier Found. (May 15, 2014), https://www.eff.org/deeplinks/2014/05/students-coast-coast-write-open-letters-about-effects-government-surveillance [https://perma.cc/S9Z5-V98B].

14 *See infra* Parts I–III.

information in education as protecting student privacy without rigorously examining its theoretical underpinnings or normative foundations.[15]

Current discourse takes for granted that student privacy laws are intended to protect students' privacy.[16] This assumption obscures a critical insight: Many regulations labeled as "student privacy" laws do not adequately safeguard students' privacy because doing so is not their sole, or even primary, objective.[17] In fact, most "student privacy" statutes rarely grant rights to students[18] and provide no privacy from either parents or educators.

Crucial questions remain unexamined. What *is* student privacy? What are its aims, values, and priorities? Whose interests does it serve and values does it promote? This Article employs a paradigmatic framework to reveal three fundamental flaws in current approaches to student privacy: (1) the failure to center students as the primary beneficiaries and rights-holders, (2) the neglect of privacy's essential role in the learning process, and (3) the inability to adapt to the realities of data-driven education.

To address these theoretical gaps, this Article reconceptualizes student privacy as critical infrastructure for learning and development, forming the foundation for intellectual exploration, identity formation, and civic participation. This Article advances a straightforward yet essential argument: that student privacy law should actually protect students' privacy. Despite the apparent obviousness of this proposition, current frameworks systematically marginalize the very individuals they purport to benefit by vesting control in parents and institutions rather than recognizing learners as primary stakeholders and rights-holders who may need privacy from both parents and educational institutions. It requires understanding privacy as essential to the learning process itself, not merely as a protective shield. And it demands frameworks that acknowledge students' evolving capabilities rather than treating them as passive subjects of adult authority. To operationalize this reconceptualization, this Article puts forward six core principles for a student-centric approach to privacy governance.

In doing so, this Article makes several contributions to the discourse on student privacy law. First, it challenges prevailing assumptions within the current legislative framework regarding student privacy that do not question the purpose, goals, or interests served by student privacy law. Second, it moves beyond traditional assessments of student privacy's operational inadequacies to reveal how the Family

---

15 *See infra* Sections I.C–.D.

16 *See infra* Part I.

17 *See infra* Part II.

18 Here, as in the rest of the Article, unless otherwise specified, this Article refers to student privacy related to K-12 schoolchildren, not those in postsecondary school or beyond.

Educational Rights and Privacy Act ("FERPA")[19] and the Protection of Pupil Rights Amendment ("PPRA")[20] systematically marginalize students' interests.[21] Third, it demonstrates how current paradigms fail to recognize privacy's essential role in education.

This Article proceeds as follows. Part I introduces the problem of student privacy in the digital age, tracing the emergence of new technologies and data practices that have overwhelmed existing legal frameworks. It then diagnoses the current crisis of student privacy as stemming not just from outdated laws but from conceptual limitations in how privacy is understood and theorized in educational contexts. Part II examines the dominant paradigms of student privacy law and analyzes how they privilege the interests of parents and institutions over those of students.

Part III critiques these frameworks, exposing their conceptual flaws, the tensions between them, and their shared shortcomings in protecting student privacy. The parent-centric approach places unrealistic burdens on parental oversight, entrenches an outdated, static view of childhood, and subordinates students' privacy interests to parental prerogatives. The school-centric paradigm, meanwhile, grants institutions expansive discretion without adequate safeguards, neglects students' intellectual privacy and autonomy, amplifies biases and power asymmetries affecting marginalized students, and lacks meaningful transparency, accountability, and due process mechanisms. This Part also highlights how the tensions between these paradigms create additional challenges for policymakers, leading to legislative gridlock or inconsistent policies. Ultimately, the critique reveals not only the specific flaws of each approach but also their shared failure to recognize students as the primary stakeholders, account for privacy's essential role in learning, and adapt to the realities of data-driven education.

---

19 Family Educational Rights and Privacy Act (FERPA) of 1974, 20 U.S.C. § 1232g (2018).

20 Protection of Pupil Rights Amendment (PPRA) of 1978, 20 U.S.C. § 1232h (2018).

21 Schools must also block obscene or pornographic content to qualify for federal discounts on internet services. 47 C.F.R. § 54.520 (2022). This implicates many of the same issues identified in the discussion of the PPRA below regarding constraint of students' intellectual exploration. *See infra*, note 373 and accompanying text. The Children's Online Privacy Protection Act ("COPPA") indirectly influences educational information practices. Children's Online Privacy Protection Act (COPPA) of 1998, 15 U.S.C. §§ 6501–6506; 16 C.F.R. pt. 312 (2022). COPPA is a consumer protection law enforced by the Federal Trade Commission ("FTC") that requires education technology vendors to obtain consent before collecting personal information from children under thirteen. 15 U.S.C. § 6502. Although schools are not subject to COPPA, the FTC permits schools to consent on parents' behalf as long as vendors only use the information for educational purposes. *See* Lisa Weintraub Schifferle, *COPPA Guidance for Ed Tech Companies and Schools During the Coronavirus*, Fed. Trade. Comm'n (Apr. 9, 2020) https://www.ftc.gov/business-guidance/blog/2020/04/coppa-guidance-ed-tech-companies-and-schools-during-coronavirus [https://perma.cc/XP36-HBL6]. A detailed examination of COPPA and other children's privacy laws is beyond the scope of this Article; however, it is something the Author will address in future articles.

Part IV proposes a student-centric approach to privacy in education settings, offering six core principles: (1) recognizing the evolving autonomy of students, (2) safeguarding their intellectual privacy and safety, (3) ensuring educational equity, (4) guaranteeing technological due process, (5) promoting democratic values, and (6) practicing responsible data stewardship. Finally, this Article concludes by considering the implications of this new paradigm for policymaking, educational practice, and future research.

I. Theorizing Student Privacy

Student information has never been more plentiful—or vulnerable. The digital transformation of education has exposed significant vulnerabilities in student information practices, creating new ways for schools and technology providers to collect, use, and share student information that the primary federal student privacy statutes did not contemplate and that newer laws fail to adequately address.

The transition from analog to digital and data-driven education has dramatically expanded the scope and nature of data collected about students, raising profound questions about privacy, autonomy, and the future of education.[22] This Part examines the proliferation of educational technology, the current legal frameworks governing student privacy, and the theoretical limitations of these frameworks in addressing modern challenges.

The digital transformation of education constitutes more than technological modernization—it represents a fundamental reconstitution of educational spaces as complex sociotechnical systems that mediate learning, development, and institutional power. This Part examines how the proliferation of educational technologies has exposed critical gaps in current approaches to student privacy.[23]

A. The Digital Transformation of Education

The pervasive integration of technology into education touches every aspect of the student experience.[24] From the moment students

---

22 *See generally* Elana Zeide, *The Structural Consequences of Big Data-Driven Education*, 5 Big Data 164 (2017) (discussing the effect "big data-driven learning environments" have on classrooms and student privacy).

23 *See infra* Part III.

24 *See* Elana Zeide, *19 Times Data Analysis Empowered Students and Schools: Which Students Succeed and Why?*, Future Priv F., Mar. 22, 2016, at 1, 7, 13–14, https://fpf.org/wp-content/uploads/2016/03/Final_19TimesData_Mar2016-1.pdf [https://perma.cc/Z6HX-CXD9]; Amy VanScoy, Kyle M.L. Jones & Alison Harding, *Student Privacy in the Datafied Classroom: Facilitating Conversations with Campus Stakeholders*, 85 Coll. & Rsch. Libs. News 296 (2024); Ben Williamson, *Psychological Surveillance and Psycho-Informatics in the Classroom*, Code Acts

step onto campus or enter virtual classrooms, a vast array of digital tools track, analyze, and influence their educational journey. Contemporary educational environments employ surveillance and monitoring tools including geolocation trackers that read license plates, recognize faces, and track class attendance.[25]

Examples abound. Student IDs embedded with radio-frequency identification chips can capture movements, recording every book borrowed, meal purchased, and facility entered.[26] Learning management systems like Canvas meticulously log student activities, tracking page visits and video interactions.[27] Adaptive learning platforms like Dreambox customize exercises based on individual performance,[28] while videoconferencing tools not only capture class discussions but are capable of analyzing students' eye movements and facial expressions to gauge attention.[29] Digital dashboards revolutionize how teachers evaluate student progression, performance, and engagement, allowing for real-time monitoring and sending automated warnings to parents or students.[30]

IN EDUC. (Jan. 17, 2017), https://codeactsineducation.wordpress.com/2017/01/17/psycho-surveillance-classroom/ [https://perma.cc/TCB2-LXBF].

25 *See, e.g.*, Drew Harwell, *Colleges Are Turning Students' Phones into Surveillance Machines, Tracking the Locations of Hundreds of Thousands*, WASH. POST (Dec. 24, 2019, 8:00 AM), https://www.washingtonpost.com/technology/2019/12/24/colleges-are-turning-students-phones-into-surveillance-machines-tracking-locations-hundreds-thousands/ [https://perma.cc/C494-H34G].

26 *See, e.g.*, *Children and RFID Systems*, ELEC. PRIV. INFO. CTR., https://epic.org/privacy/rfid/children.html [https://perma.cc/P6TG-JQMF]; David Kravets, *Tracking School Children with RFID Tags? It's All About the Benjamins*, WIRED (Sept. 7, 2012), http://www.wired.com/2012/09/rfid-chip-student-monitoring/ [https://perma.cc/XB5F-SM3Y].

27 *See, e.g.*, Instructure, *supra* note 5.

28 DREAMBOX LEARNING, https://www.dreambox.com/ [https://perma.cc/B4PB-SVRJ].

29 *See, e.g.*, Fourtané, *supra* note 6; *see also* Steve Komorek, *Children's Privacy in the Zoom Classroom*, J. TECH. & INTELL. PROP. BLOG (Jan. 22, 2021), https://jtip.law.northwestern.edu/2021/01/22/childrens-privacy-in-the-zoom-classroom/ [https://perma.cc/K2C7-M7DP]. Zoom discontinued its attention tracking feature in 2020 after the public outcry. *See Attendee Attention Tracking*, ZOOM SUPPORT, https://support.zoom.com/hc/en/article?id=zm_kb&sysparm_article=KB0069153 [https://perma.cc/AG63-EXG2].

30 *See* INSTRUCTURE, EDTECH TOP 40: A LOOK AT K-12 EDTECH ENGAGEMENT DURING THE 2022–23 SCHOOL YEAR 4–5 (2023), https://www.instructure.com/resources/research-reports/edtech-top-40-look-k-12-edtech-engagement-during-2022-23-school-year [https://perma.cc/4C6V-ZJTG]; Ben Williamson, *Big EdTech*, 47 LEARNING, MEDIA & TECH. 157, 160–61 (2022); Natasha Singer, *How Google Took over the Classroom*, N.Y. TIMES (May 13, 2017), https://www.nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html [https://perma.cc/MN66-B4LE]; GALLUP, EDUCATION TECHNOLOGY USE IN SCHOOLS: STUDENT AND EDUCATOR PERSPECTIVES (2019), http://www.newschools.org/wp-content/uploads/2019/09/Gallup-Ed-Tech-Use-in-Schools-2.pdf [https://perma.cc/R6JJ-2WQP]; *How to Keep Parents Engaged in School Activities Using an LMS*, CYPHER LEARNING, https://www.cypherlearning.com/resources/infographics/academia/how-to-keep-parents-engaged-in-school-activities-using-an-lms [https://perma.cc/VMY7-T36V]; *Using LMS Data to Inform Course Design*, UDL ON CAMPUS, https://udloncampus.cast.org/page/assessment_data [https://perma.cc/Q9QS-FEW2].

The COVID-19 pandemic served as a catalyst, dramatically accelerating the adoption of educational technology.[31] During the height of the pandemic more than ninety percent of households with school-aged children participated in some form of distance learning.[32] This rapid digital transformation fundamentally altered the educational landscape, with approximately two-thirds of teachers now incorporating digital learning tools into their daily instruction.[33] School districts nationwide now employ 2,600 distinct educational technologies on average—three times as many as they did just five years ago.[34]

Beyond basic instructional tools, education technology includes behavioral monitoring and safety systems.[35] Platforms like ClassDojo monitor students' classroom behavior and progress toward socioemotional goals.[36] Although these systems aim to provide valuable feedback and

---

31 *See, e.g.*, *Use of Digital Classroom Tools Holds Steady Post-Pandemic*, GovTech (Apr. 19, 2022), https://www.govtech.com/education/k-12/report-use-of-digital-classroom-tools-post-pandemic [https://perma.cc/G8BN-LSMT]; Ceres, *supra* note 3; Neil Selwyn, Thomas Hillman, Annika Bergviken Rensfeldt & Carlo Perrotta, *Digital Technologies and the Automation of Education—Key Questions and Concerns*, 5 Postdigital Sci. & Educ. 15 (2023); Neil Selwyn, Thomas Hillman, Annika Bergviken-Rensfeldt & Carlo Perrotta, *Making Sense of the Digital Automation of Education*, 5 Postdigital Sci. & Educ. 1 (2023); Natalia Kucirkova, *The Promise and Pitfalls of Personalised Learning with New EdTech*, *in* Education Data Futures: Critical, Regulatory and Practical Reflections 220 (Sonia Livingstone & Krukae Pothong eds., 2022); Neil Selwyn & Dragan Gašević, *The Datafication of Higher Education: Discussing the Promises and Problems*, 25 Teaching Higher Educ. 527 (2020).

32 Kevin McElrath, *Nearly 93% of Households with School-Age Children Report Some Form of Distance Learning During COVID-19*, U.S. Census Bureau (Aug. 26, 2020), https://www.census.gov/library/stories/2020/08/schooling-during-the-covid-19-pandemic.html [https://perma.cc/D3KR-S5EU].

33 Gallup, *supra* note 30, at 6.

34 *Id.* at 5.

35 *See, e.g.*, Elizabeth Warren & Ed Markey, U.S. Senate, Constant Surveillance: Implications of Around-the-Clock Online Student Activity Monitoring 5–6, 9 (2022), https://www.warren.senate.gov/download/356670-student-surveillance [https://perma.cc/V4AY-53KX]; 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 14–15, 20–21 (2022); Stephen J.J. McGuire, Yang Zhang, Cathy Jin, Manika Tiwari, Niyati Gosalia, Sofyan Dowiri & Venkata Bhamidipati, *Geo Listening at the Glendale Unified School District*, 3 J. Rsch. & Inquiry 188, 196–97, 201–03 (2017); Isabelle Fleury & Erin Dowdy, *Social Media Monitoring of Students for Harm and Threat Prevention: Ethical Considerations for School Psychologists*, 26 Contemp. Sch. Psych. 299, 299–300 (2022); Khayaal Desai-Hunt, *Gaggle: MPS's New Student Surveillance Software Brings Possible Protection and Danger*, Southerner (Mar. 14, 2021), https://www.shsoutherner.net/features/2021/03/14/gaggle-mpss-new-student-surveillance-software-brings-possible-protection-and-danger/ [https://perma.cc/AKL5-XCM2]; Lucy Dockter, *Gaggle Monitors Student Online Behavior, Threatens Student Privacy*, Inklings News (Mar. 10, 2021), https://www.inklingsnews.com/opinions/2021/03/10/gaggle-monitors-student-online-behavior-threatens-student privacy/ [https://perma.cc/QYY3-EDPC].

36 ClassDojo, Presentation on Behavior Management with ClassDojo 4, 7–13, https://static.classdojo.com/img/2022/ClassDojoSchool/Behavior+Management+with+ClassDojo_+Slides.pdf [https://perma.cc/GUP5-TNH6].

encourage positive behavior, they also raise concerns about the long-term implications of digitally tracking and quantifying students' social and emotional development.[37] The data collected by these platforms could potentially follow students throughout their academic careers, creating digital behavioral profiles that may influence future educational or even employment opportunities.

Other services like Gaggle, Bark, and Securely monitor students' browsing habits, social media activity, and communications to alert educators, and sometimes parents, to signs of distress and danger.[38] Although the intent behind these monitoring systems is often to protect student safety, they represent a form of surveillance that extends far beyond the traditional boundaries of school oversight. The use of such technologies blurs the line between school and personal life, potentially chilling students' free expression and hindering their ability to explore ideas and identities in digital spaces.[39] Furthermore, the involvement of parents in this monitoring raises complex questions about student autonomy and the right to privacy from family members, particularly for older students.

The widespread adoption of online proctoring systems represents another significant technological intrusion into student privacy. These platforms record students in their private spaces during exams,[40] often employing facial recognition and eye-tracking technologies. These systems serve the crucial goal of preserving academic integrity but also involve significant intrusion into students' personal spaces.[41] Moreover, online proctoring systems have been criticized for potential bias,

---

37 *See* Zeide, *supra* note 22, at 169 (warning that overreliance on quantifying students' behaviors may inhibit soft skill development).

38 *See, e.g.*, Warren & Markey, *supra* note 35, at 3–4; Laird et al., *supra* note 35, at 4–6, 9; McGuire et al., *supra* note 35, at 188, 196; Fleury & Dowdy, *supra* note 35, at 299–300 (2020); Desai-Hunt, *supra* note 35; Dockter, *supra* note 35.

39 *See* Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. Rich. L. Rev. 465, 490–92, 501–06 (2015) (discussing studies that examined the impact of surveillance on university students' behavior); *see* Neil Richards, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age 95–122 (2015) (employing "intellectual privacy" to describe the relationship between free speech and privacy that is necessary to cultivate an environment for freedom of expression); Jonathon W. Penney, *Understanding Chilling Effects*, 106 Minn. L. Rev. 1452, 1458 (2022) (advancing the author's "social conformity theory of chilling effects" through a discussion of what chilling effects are and what makes them manifest).

40 *See* Elana Zeide, *Big Proctor: Online Proctoring Problems and How FERPA Can Promote Student Data Due Process*, 3 Notre Dame J. on Emerging Techs. 74, 77 (2022); Albert Fox Cahn & Grace Deng, *Remote Test-Taking Software is an Inaccurate, Privacy-Invading Mess*, Fast Co. (Dec. 16, 2020), https://www.fastcompany.com/90586386/remote-test-taking-software-is-an-inaccurate-privacy-invading-mess [https://perma.cc/TH7B-FBE4].

41 *See generally* Zeide, *supra* note 40 (critiquing the implementation of online proctoring software in schools).

particularly against students of color or those with disabilities, highlighting the intersection of privacy concerns with issues of equity and inclusion.[42]

Biometric technologies, including facial recognition and fingerprint scanners, serve to authenticate students' identities upon entry into their school and prevent unauthorized access to school grounds.[43] Yet these systems do more than secure facilities—they normalize intensive surveillance from an early age, potentially reshaping students' expectations of privacy in society.[44] Moreover, collecting and storing biometric data present unique privacy risks, as this highly personal information, if breached, cannot be changed like a password.[45]

The algorithmic transformation of education extends beyond immediate classroom applications to shape students' academic pathways and institutional decisions.[46] Artificial intelligence now plays a significant role in determining students' educational trajectories, influencing curricula, assessment methods, disciplinary actions, academic placements, and even scholarship eligibility.[47] But these presumably

---

42 *Id.* at 125–32.

43 Marcela Hernandez-de-Menendez, Ruben Morales-Menendez, Carlos A. Escobar & Jorge Arinez, *Biometric Applications in Education*, 15 INT'L J. ON INTERACTIVE DESIGN & MFG. 365, 369 (2021); Shawna De La Rosa, *Biometrics Can Make Schools Safer, but Privacy Concerns Persist*, K-12 DIVE (May 9, 2019), https://www.k12dive.com/news/biometrics-can-make-schools-safer-but-privacy-concerns-persist/554420/ [https://perma.cc/Y2GJ-YP2R]; *Schools and Biometric Technology: A Global Trend*, EDUCATOR AUSTL. (July 25, 2018), https://www.theeducatoronline.com/k12/best-practice/education-technology/schools-and-biometric-technology-a-global-trend/252786 [https://perma.cc/GQV2-5UE8].

44 *See* Zeide, *supra* note 40, at 89, 98; Elana Zeide, *The Limits of Education Purpose Limitations*, 71 U. MIA. L. REV. 494, 518 (2017) [hereinafter Zeide, *Education Purpose Limitations*]; Claire Galligan, Hannah Rosenfeld, Molly Kleinman & Shobita Parthasarathy, *Cameras in the Classroom: Facial Recognition Technology in Schools*, UNIV. OF MICH. GERALD R. FORD SCH. OF PUB. POL'Y (Aug. 25, 2020), https://stpp.fordschool.umich.edu/research/research-report/cameras-classroom-facial-recognition-technology-schools [https://perma.cc/J35Q-F64R]; Danielle Keats Citron, *The Surveilled Student*, 76 STAN. L. REV. 1439, 1458 (2024); Barbara Fedders, *The Constant and Expanding Classroom: Surveillance in K-12 Public Schools*, 97 N.C. L. REV. 1673, 1711 (2018). *See generally* Evan Selinger & Hyo Joo (Judy) Rhee, *Normalizing Surveillance*, 22 N. EUR. J. PHIL. 1 (2021) (explaining "normalization" in the context of surveillance).

45 *See, e.g.*, Pin Lean Lau, *Facial Recognition in Schools: Here Are the Risks to Children*, CONVERSATION (Oct. 21, 2021, 3:04 PM), http://theconversation.com/facial-recognition-in-schools-here-are-the-risks-to-children-170341 [https://perma.cc/HTZ9-SKDT] (for example, a person's "face print").

46 *See generally*, Zeide, *supra* note 22 (discussing how the information pulled from big data-driven education technologies is used to shape institutional decisions).

47 *See* Frank Pasquale & Neil Selwyn, *Education and the New Laws of Robotics*, 5 POSTDIGITAL SCI. EDUC. 206, 211 (2023); Elana Zeide, *Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPs*, 8 DREXEL L. REV. 339, 351 (2016); MIGUEL A. CARDONA, ROBERTO J. RODRIGUEZ & KRISTINA ISHMAEL, U.S. DEP'T OF EDUC., ARTIFICIAL INTELLIGENCE AND THE FUTURE OF TEACHING AND LEARNING: INSIGHTS AND RECOMMENDATIONS 1, 3, 15–16 (2023), https://www2.ed.gov/documents/ai-report/ai-report.pdf [https://perma.cc/TAR2-3NC7].

"objective" machines often reflect historical patterns of bias, amplifying existing inequity.[48] Furthermore, the opacity of many of these algorithms makes it difficult for students, parents, and educators to understand or challenge decisions that may significantly impact a student's future.[49]

College admissions officers may, in the future, employ algorithms to evaluate applications and predict prospective students' interest by, for example, monitoring website browsing patterns and email engagement rates.[50] This may disadvantage students who may not have the knowledge or resources to engage with institutions' online platforms in ways that algorithms deem favorable.

Financial aid departments similarly may, in the future, leverage data analytics to determine scholarship awards.[51] Although this approach may streamline the allocation of limited resources, it also risks reducing complex personal circumstances to data points, potentially overlooking deserving students whose situations do not fit predefined criteria.[52] The use of data analytics in financial aid decisions also prompts concerns about transparency and fairness, as the factors influencing these critical determinations may not be fully disclosed or understood by applicants.[53]

---

48 *See generally* Ryan S. Baker & Aaron Hawn, *Algorithmic Bias in Education*, 32 Int'l J. A.I. Educ. 1052 (2022) (discussing algorithmic bias); Carlo Perrotta, *Advancing Data Justice in Education: Some Suggestions Towards a Deontological Framework*, 48 Learning, Media & Tech. 187 (2023) (same); Chris Gilliard & Neil Selwyn, *Automated Surveillance in Education*, Postdigital Sci. & Educ. (2022) (same); Elana Zeide, *The Silicon Ceiling: How Artificial Intelligence Constructs an Invisible Barrier to Opportunity*, 91 UMKC L. Rev. 403 (2022); *see also* Zeide, *supra* note 40, at 91–95 (discussing bias in proctoring software).

49 *See generally* Zeide, *supra* note 40; Manuela Ekowo & Iris Palmer, The Promise and Peril of Predictive Analytics in Higher Education 36 (2016) (discussing the use of predictive analytics in higher education); Jenna Burrell, *How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms*, Big Data & Soc'y, Jan.–June 2016, at 1–12 (analyzing different types of "opacity" in machine learning algorithms); Nabeel Gillani, Rebecca Eynon, Catherine Chiabaut & Kelsey Finkel, *Unpacking the "Black Box" of AI in Education*, 26 Educ. Tech. & Soc'y 99 (2023) (discussing the role of artificial intelligence in education).

50 *See* Marguerite J. Dennis, *Artificial Intelligence and Recruitment, Admission, Progression, and Retention*, Enrollment Mgmt. Rep., Nov. 2018, at 1, 1; Doug Belkin, *Colleges Mine Data on Their Applicants*, Wall St. J. (Jan. 26, 2019, 8:00 AM), https://www.wsj.com/articles/the-data-colleges-collect-on-applicants-11548507602 [https://perma.cc/2ZKE-U2TZ].

51 *See* Kyle Eric Van Duser & Clifton S. Tanabe, *The Educational Return on Investment Commitment: Using Predictive Analytics and Financial Aid to Leverage Retention*, 23 J. Coll. Student Retention: Rsch., Theory & Prac. 264, 266 (2021).

52 *See generally* Ben Williamson, Sian Bayne & Suellen Shay, *The Datafication of Teaching in Higher Education: Critical Issues and Perspectives*, 25 Teaching in Higher Educ. 351 (2020) (discussing the problem of datafication in education generally); Ann Christin Eklund Nilsen & Ove Skarpenes, *Quantification and Classification in Education: What is at Stake?*, 20 Pol'y Futures in Educ. 120 (2022) (discussing the use of statistics and quantification in the field of education).

53 Liann Herder, *Algorithmic Bias Continues to Negatively Impact Minoritized Students*, Diverse: Issues in Higher Educ. (July 15, 2024), https://www.diverseeducation.com/reports-data/article/15679597/algorithmic-bias-continues-to-impact-minoritized-students [https://perma.cc/NFX4-97D6].

Counselors now rely on early-warning systems that apply predictive algorithms to a wide array of student data, including attendance records, assessment outcomes, disciplinary history, and demographic information, to identify and intervene with struggling students.[54] Although these systems aim to provide timely support, they also risk labeling students based on limited data, potentially creating self-fulfilling prophecies or stigmatizing students flagged by the system.[55]

At the administrative level, technology-gathered data informs crucial decisions about staffing, budgeting, and resource allocation.[56] Although this data-driven approach may improve efficiency, it also risks reducing the complex ecosystem of education to measurable metrics. It may overlook important qualitative factors in favor of quantifiable outcomes.[57]

This integration of technology also facilitated the creation of comprehensive data systems that track students from early education through their careers—and beyond. Statewide longitudinal data systems ("SLDSs") collect attendance, grades, and demographic data from early education programs through high school, college graduation, and even career placement.[58] Contemporary policy initiatives increasingly combine this data with social services and workforce bases to gain

---

54 *See Early Warning System*, PANORAMA EDUC., https://www.panoramaed.com/early-warning-system [https://perma.cc/4KKH-5A48]; *How Early Warning Works*, BRIGHTBYTES, https://wvde.state.wv.us/osp/Graduation/HowItWorks.pdf [https://perma.cc/C466-3N9M]; *see also, e.g.*, *Supporting Early Warning Systems: Using Data to Keep Students on Track to Success*, DATA QUALITY CAMPAIGN (Mar. 2016), https://dataqualitycampaign.org/wp-content/uploads/2016/03/Supporting-Early-Warning-Systems.pdf [https://perma.cc/S92D-2QKV].

55 *See generally* Kyle M.L. Jones, *Advising the Whole Student: eAdvising Analytics and the Contextual Suppression of Advisor Values*, 24 EDUC. INFO. TECH. 1 (Aug. 2018) (discussing why certain advisors have stepped away from using eAdvising tools due to moral and ethical concerns); Hideyuki Matsumi & Daniel J. Solove, *The Prediction Society: AI and the Problems of Forecasting the Future*, 2025 U. ILL. L. REV. 1 (2025) (discussing the issue of algorithmic predictions generally); Priscilla M. Regan, Jolene Jesse & Elsa Talat Khwaja, *Big Data in Education: Developing Policy for Ethical Implementation in the U.S. and Canada*, LAW & SOC'Y ASS'N ANN. CONF. (2017) (providing analysis on the ethical implications of using "big data" in educational environments); Zeide, *Education Purpose Limitations*, *supra* note 44 (discussing the shift to data-driven education tools generally); Zeide, *supra* note 22 (addressing implications of data-driven education).

56 *See* Neil Selwyn, Michael Henderson & Shu-Hua Chao, *'You Need a System': Exploring the Role of Data in the Administration of University Students and Courses*, 42 J. FURTHER & HIGHER EDUC. 46, 47 (2016); Zeide, *supra* note 24, at 3; Marguerite J. Dennis, *Artificial Intelligence and Recruitment, Admission, Progression, and Retention*, 22 ENROLLMENT MGMT. REP. 1, 3 (2018).

57 Dennis, *supra* note 56, at 3.

58 *See, e.g.*, Elana Zeide, *The Proverbial "Permanent Record"*, N.Y.U. INFO. L. INST. 4 (Oct. 2014), https://ssrn.com/abstract=2507326 [https://perma.cc/VCD2-NKEC]; JOEL R. REIDENBERG, JAMELA DEBELAK, ADAM GROSS, LEE A. MAYBERRY, JUDITH SIMMS & ELIZABETH WOODARD, FORDHAM L. SCH. CTR. ON L. & INFO. POL'Y, CHILDREN'S EDUCATIONAL RECORDS AND PRIVACY: A STUDY OF ELEMENTARY AND SECONDARY SCHOOL STATE REPORTING SYSTEMS 1–2 (2009), https://archive.epic.org/apa/ferpa/Fordham%20Center%20Report.pdf [https://perma.cc/ZZ9F-9ZGN].

holistic insights into health, economic, and education outcomes.[59] Although these integrated data systems offer new opportunities for evidence-based policymaking and targeted interventions, they also raise significant privacy and ethical questions about the long-term implications of maintaining such lifelong digital profiles for students.

The trajectory of educational technology points toward even more sophisticated data collection and analysis systems. There is growing interest in the use of generative AI and expanded monitoring methods like gaze tracking[60] that raise fundamental questions about the boundaries between assessment and invasive surveillance.[61] As these capabilities advance, the need for coherent theoretical frameworks to protect student privacy becomes increasingly urgent.

B. The Student Privacy Regulatory Framework and Its Limitations

The rapid technological advancements in education have outpaced the legal frameworks designed to protect student privacy. The legal architecture governing student privacy centers on two aging federal statutes, FERPA and PPRA, which are supplemented by an expanding patchwork of state regulations.[62] This regulatory regime fails to address contemporary challenges not merely due to technological change, but because of fundamental theoretical limitations in how privacy is conceptualized within educational contexts.

Current frameworks do not account for an expansive array of information-based harms or the impact of modern information practices on students' development, wellbeing, and opportunities. As a result, they lack clear normative guidance on the desired balance of competing values such as institutional transparency, pedagogical innovation, and student autonomy. This leads to inconsistent protections and a failure to keep pace with the increasingly complex educational ecosystem.

Enacted in 1974, FERPA governs educational institutions that receive federal funding, including postsecondary institutions accepting federal financial aid.[63] The statute regulates access to and disclosure of personally identifiable information found in "education records," broadly defined as records directly related to a student and maintained

---

59 *See* Reidenberg et al., *supra* note 58, at 1.

60 *See, e.g.*, Andrea Apicella, Pasquale Arpaia, Mirco Frosolone, Giovanni Improta, Nicola Moccaldi & Andrea Pollastro, *EEG-Based Measurement System for Monitoring Student Engagement in Learning 4.0*, 12 Sci. Rep. 5857 (2022); Uzma Samadani, *A New Tool for Monitoring Brain Function: Eye Tracking Goes Beyond Assessing Attention to Measuring Central Nervous System Physiology*, 10 Neural Regeneration Rsch. 1231 (2015).

61 *See supra* Section I.A.

62 *See, e.g.*, Ok Stat. tit. 70, § 3-168 (2022); Colo. Rev. Stat. § 22-16-107 (2022); Ky. Rev. Stat. Ann. § 365.734 (West 2022); Cal. Bus. & Prof. Code § 22584(b)(1)–(2), (b)(4)(A) (West 2024).

63 20 U.S.C. § 1232g.

by an educational agency or institution or by a party acting on their behalf.[64] FERPA provides parents with several rights that transfer to students when they turn eighteen or enter postsecondary education.[65] These include the right to access a student's personally identifiable information record and challenge its accuracy.[66] Although FERPA generally requires schools to obtain parental consent before disclosing personally identifiable information to third parties,[67] numerous exceptions overshadow the rule.[68]

The PPRA, complementing FERPA, focuses on school surveys and evaluations in K-12 education.[69] It requires schools to obtain written parental consent before compelling students to participate in any survey, analysis, or evaluation that seeks to elicit information on eight categories of particularly sensitive information. These include political affiliations, mental or psychological conditions, sexual behavior or attitudes, illegal[70] or self-incriminating activities,[71] and religious beliefs.[72] The PPRA also provides parents with the right to inspect any instructional material used as part of their child's educational curriculum.[73]

FERPA and the PPRA do not strictly prohibit any information practices in particular.[74] Instead, they condition schools' federal funding on compliance with practices specifically approved by these statutes.[75] As a result, these requirements apply exclusively to schools receiving federal funding, including most public K-12 schools and postsecondary

---

64 *Id.* § 1232g(a)(4)(A) (defining "education records").

65 *Id.* § 1232g(d) (transfer of rights to students).

66 *Id.* § 1232g(a)(1)(A) (granting parents "the right to inspect and review the education records of their children"); *id.* § 1232g(a)(4)(B), (g); 34 C.F.R. § 99.3 (2012) (defining education records as "those that are [d]irectly related to a student; and . . . [m]aintained by an educational agency or institution or by a party acting for the agency or institution").

67 20 U.S.C. § 1232g(b).

68 *Id.*; *see infra* Section II.B (discussing the school official exception).

69 U.S. Dep't of Educ., Technical Assistance on Student Privacy for State and Local Educational Agencies when Administering College Admissions Examinations 4 (May 2018), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/TA%20College%20Admissions%20Examinations.pdf [https://perma.cc/5W69-5ATY].

70 20 U.S.C. § 1232h(b).

71 *Id.* § 1232h(c)(2) (providing parents and emancipated students with the right to opt out of directory information).

72 *Id.* § 1232h(c)(1)(B). The same requirements apply to nonemergency, invasive physical examinations or screenings required for attendance. *Id.* § 1232h(c)(2)(C)(iii)(III). Schools must also provide an annual notice informing parents of their rights under the PPRA and any changes in any related information policies at least annually at the beginning of the school year. *Id.* § 1232h(c)(2).

73 *Id.* § 1232h(c)(1)(A)(i), (C)(i).

74 *Id.* §§ 1232g, 1232h.

75 *Id.* § 1232g(a)(2) ("No funds shall be made available under any applicable program [unless statutory requirements are met]."); *id.* § 1232h(c)(1) ("Except as provided in subsections (a) and (b), a local educational agency that receives funds under any applicable program shall develop policies [prescribed in this section].").

institutions that administer financial aid.[76] Although technically voluntary, the financial realities of modern education render compliance essentially mandatory, as few institutions can forgo federal funding in practice.[77]

State legislatures have responded to perceived inadequacies in federal protections by enacting their own student privacy statutes to address more localized concerns about student privacy. Since 2013, legislators in every state have introduced student privacy bills, with nearly 400 signed into law.[78] These statutes commonly provide parents with more transparency about schools' information practices,[79] require consent before the collection of specific sensitive data like biometric identifiers,[80] and prohibit vendors from selling or using student information for targeted advertising.[81] Although these state-level efforts represent important steps toward addressing modern student privacy challenges, they also contribute to a complex and sometimes inconsistent patchwork of regulations. Perhaps as a result, they are rarely enforced.[82]

---

76 *Id.* § 1232g(f).

77 *See Race, Color, or National Origin Discrimination: Frequently Asked Questions*, U.S. DEP'T OF EDUC. OFF. FOR C.R., https://www2.ed.gov/about/offices/list/ocr/frontpage/faq/race-origin.html [https://perma.cc/6HWT-FJVH] ("All public school districts are covered by Title VI because they receive some federal financial assistance. All public colleges and universities and virtually all private colleges and universities are covered because they receive such assistance by participating in federal student aid programs.").

78 *See* DATA QUALITY CAMPAIGN, EDUCATION DATA LEGISLATION REVIEW: 2019 STATE ACTIVITY 3 (2019), https://dataqualitycampaign.org/wp-content/uploads/2019/10/DQC-2019-Education-Data-Legislation-Review.pdf [https://perma.cc/Q9SW-PYCS]; DATA QUALITY CAMPAIGN, EDUCATION DATA LEGISLATION REVIEW: 2020 STATE ACTIVITY 8 (2020), https://dataqualitycampaign.org/wp-content/uploads/2020/11/DQC-Legislative-Summary-2020.pdf [https://perma.cc/ZAB4-CXZA]; DATA QUALITY CAMPAIGN, EDUCATION DATA LEGISLATION REVIEW: 2021 STATE ACTIVITY 2 (2021), https://dataqualitycampaign.org/wp-content/uploads/2021/12/DQC-Legislation-Summary-2021-1.pdf [https://perma.cc/6BLP-P3M5]; DATA QUALITY CAMPAIGN, EDUCATION DATA LEGISLATION REVIEW: WHAT HAPPENED IN 2022? 1 (2022), https://dataqualitycampaign.org/wp-content/uploads/2022/10/DQC-Legislation-Review-2022.pdf [https://perma.cc/8D4S-PQC3]; DATA QUALITY CAMPAIGN, EDUCATION AND WORKFORCE DATA LEGISLATION REVIEW: WHAT HAPPENED IN 2023? 4 (2023), https://dataqualitycampaign.org/wp-content/uploads/2023/10/DQC-Legislation-Summary-2023.pdf [https://perma.cc/58SE-QGQS].

79 *See, e.g.*, OK STAT. tit. 70, § 3-168 (2022) (requiring data breach notifications); COLO. REV. STAT. § 22-16-107 (2022) (same); KY. REV. STAT. ANN. § 365.734 (West 2022) (same).

80 S.B. 820, 86th Leg. (Tex. 2019).

81 CAL. BUS. & PROF. CODE § 22584(b)(1) (targeted advertising prohibition); § 22584(3) (West 2024) (prohibition on direct sale of covered information); *id.* § 22584(b)(2) (noneducational profile prohibition); *id.* § 22584(b)(4)(A) (noneducational disclosure prohibition); *see also* COLO. REV. STAT. § 22-16-107 (2022) (prohibiting the targeted advertising and sale of student information).

82 *See* RACHAEL STICKLAND, NETWORK FOR PUB. EDUC. & PARENT COAL. FOR STUDENT PRIV., THE STATE STUDENT PRIVACY REPORT CARD: GRADING THE STATES ON PROTECTING STUDENT PRIVACY 20 (2019), https://studentprivacymatters.org/wp-content/uploads/2019/01/The-2019-State-Student-Privacy-Report-Card.pdf [https://perma.cc/ETG5-JQ4G].

Parents' Bills of Rights ("PBORs") constitute the final component of student information governance.[83] Although these are not generally recognized as "student privacy" laws, they are often implemented by amending student privacy legislation or promoting parents' rights through information policies.[84] Although the focuses and regulatory mechanisms of PBORs vary, they often grant parents a more transparent view of school finances and library offerings, broader access to reviewing their children's information, and more rights to opt out of instruction on controversial topics.[85]

Federal and state laws provide some protections for student privacy, but they have not kept pace with the realities of modern, data-driven education. The digital transformation of schools has created a vast network of data collection and sharing involving educators, parents, students, private companies, and government actors—far beyond what Congress envisioned when enacting FERPA and the PPRA. At the time, schools relied on paper records kept in filing cabinets.[86] These analog-era constraints created natural privacy protections—physical records could not be instantaneously copied, shared with multiple parties, or easily analyzed for patterns or insights beyond their original purpose. These physical constraints inadvertently served as a safeguard against unauthorized access and widespread dissemination of sensitive information and its repurposing for noneducational purposes.[87]

The transition from physical to digital record keeping has fundamentally changed the landscape of student privacy protection. The ease of data collection, storage, and sharing in digital formats has eroded the natural barriers that once limited access to student information.[88] The sheer volume and velocity of data flows in modern educational contexts exceed the cognitive and technical capacities of parents and educators to meaningfully track and control.[89]

These challenges are compounded by the outdated definitions, broad exceptions, and compliance-oriented enforcement models of existing student privacy regimes.[90] The limitations begin with fundamental definitional and structural problems in FERPA's architecture. The statute's core concept of "education records" reflects its analog origins, defining protected information as records "maintained by an

---

83 *See, e.g.*, Parents' Bill of Rights Act of 2021, S. 3218, 117th Cong. (2021); Parents' Bill of Rights Act, H.R. 5, 118th Cong. (2023).

84 *See, e.g.*, H.R. 5 (amending FERPA and the PPRA to provide parents with more control over their children's information and education).

85 *See infra* Section II.A.3.

86 *See* Zeide, *supra* note 47, at 350–55.

87 *See id.*

88 *See id.*

89 *See id.* at 349–50.

90 *See* 20 U.S.C. §§ 1232g, 1232h; 34 C.F.R. § 98 (2023); Zeide, *supra* note 47, at 350–55.

educational agency or institution"[91]—a definition that presumes static and stored data held by schools.

This definition fails to encompass the dynamic nature of modern educational technology, in which data is continuously generated, processed, and analyzed in real time.[92] For example, learning management systems track students' reading patterns, adaptive learning platforms adjust content based on performance metrics, and attendance systems monitor physical movements through campus.[93] These technologies make decisions based on educational data that may never be "maintained" in any traditional sense, potentially placing it outside FERPA's protective scope.[94]

FERPA's exceptions further compromise its efficacy in the digital age. FERPA generally requires schools to obtain parental consent before sharing student information with third parties.[95] However, the "school official" exception permits schools to share personally identifiable student information without parental consent to recipients, as long as the school determines that disclosure serves a "legitimate educational interest[]"[96] and the information remains under the school's "direct control."[97] Importantly, neither the statutes, nor regulation, nor agency guidance clearly define these terms.[98] Schools often broadly interpret the exceptions and thus commonly share information with for-profit education technology vendors.[99] As a result, companies may gain extensive access to sensitive student information without direct accountability to students or parents.[100]

The school official exception is just one example of how FERPA's outdated provisions fail to adequately protect student privacy in the digital age. The "directory information" exception permits schools to designate certain categories of student information, such as name,

---

91 20 U.S.C. § 1232g(a)(4)(A)(ii).

92 *Id.* § 1232g(b)(1)(A) (permitting the release of education records to "school officials"); JARED P. COLE, CONG. RSCH. SERV., R46799, THE FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA): LEGAL ISSUES 7–8 (2021).

93 *See supra* Section I.A.

94 *See supra* Section I.A; 20 U.S.C. § 1232g(a)(4)(A)–(B).

95 20 U.S.C. § 1232g(b)(1), (4).

96 *Id.* § 1232g(b)(1)(A); COLE, *supra* note 92, at 7–8.

97 20 U.S.C. § 1232g(b)(1)(A); 34 C.F.R § 99.31(a)(1)(i)(A), (B)(2).

98 *See* 20 U.S.C. §§ 1232g, 1232h; 34 C.F.R. § 98 (2023); U.S. DEP'T OF EDUC., *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*, *PTAC FAQ* 3 (2014), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Student%20Privacy%20and%20Online%20Educational%20Services%20%28February%202014%29_0.pdf [https://perma.cc/T8GD-J7UE].

99 *See generally* Reidenberg et al., *supra* note 13 (analyzing the relationship between the legal landscape and information sharing practices by educational institutions to third-party cloud service vendors).

100 *See* COLE, *supra* note 92, at 7–8.

address, and date of birth, as "directory information" that can be disclosed without parental consent.[101] Although this exception was originally intended to facilitate the publication of student directories and yearbooks, it now enables the widespread dissemination of student data to third parties, including commercial entities that can easily aggregate and analyze this information.[102]

Beyond these specific exceptions, federal student privacy laws do not directly regulate the education technology vendors that are now integral to today's education environment.[103] Instead, they adopt an indirect approach by placing the responsibility on educational institutions to ensure these vendors adhere to FERPA's constraints on redisclosure and repurposing of student information.[104] Yet, many schools, typically under-resourced and lacking sufficient technical expertise, find it challenging to effectively oversee vendor compliance with privacy requirements.[105] Moreover, the power imbalance between schools and large technology companies can make it challenging for schools to enforce privacy protections or negotiate favorable terms.[106]

The regulatory gaps and practical limitations of the current student privacy regime have created an environment where the students find their most intimate information exposed to myriad actors—from school administrators to law enforcement to commercial data brokers—with little visibility, control, or recourse. Modern educational technologies have far outpaced the protective measures of existing student privacy laws, creating an urgent need for comprehensive legal reform. Unfortunately, the current discourse, focusing on the doctrinal limitations revealed by new technologies, is incomplete.

C. Theoretical Limitations of Current Student Privacy Paradigms

The shortcomings of student privacy protection stem not merely from outdated statutes or technological complexity, but from a deeper theoretical problem: the lack of a coherent normative foundation that articulates the values, principles, and aims that should guide the governance of student data. Existing frameworks remain largely reactive, focusing on procedural safeguards and parental control mechanisms

---

101 20 U.S.C. § 1232g(a)(5)(A) (defining directory information and the exception).

102 *See* Elec. Priv. Info. Ctr., Comment Letter on Proposed Rule to Amend Regulations Under the Family Educational Rights and Privacy Act of 1974 (May 23, 2011), https://epic.org/privacy/student/EPIC_FERPA_Comments.pdf [https://perma.cc/2X5A-RZ7D] (documenting how commercial entities exploit the directory information exception to collect and aggregate student data).

103 *See infra* Sections III.A–.B.

104 Zeide, *supra* note 40, at 369; Amy Rhoades, *Big Tech Makes Big Data out of Your Child: The FERPA Loophole EdTech Exploits to Monetize Student Data*, 9 AM. U. BUS. L. REV. 445, 458–59 (2020).

105 Zeide, *supra* note 40, at 345, 362; Rhoades, *supra* note 104, at 469.

106 Zeide, *supra* note 40, at 345, 362; Rhoades, *supra* note 104, at 469.

rather than grappling with the substantive question of why and how student privacy should be protected in the first place.[107] Simply put, student privacy itself is undertheorized.

Current frameworks do not account for an expansive array of information-based harms or the impact of modern information practices on students' development, wellbeing, and opportunities. Nor is there clarity about student privacy's purposes, priorities, and protective goals. As a result, neither of the prevailing paradigms provides clear normative guidance about the desired balance between competing values such as institutional transparency, pedagogical innovation, and student autonomy.

Privacy theory has evolved significantly since FERPA's enactment, yet student privacy law remains rooted in outdated models. Contemporary scholars consider privacy to be more than merely the "right to be let alone"[108]—or control over personal information. They now recognize privacy as essential infrastructure for intellectual development, identity formation, and democratic participation[109]—all core functions of education itself. Yet, student privacy law continues to operate through mechanisms of individual control and procedural compliance that prove inadequate in modern educational environments.[110]

This Article reconceptualizes student privacy as critical infrastructure for learning and development—not merely a protective shield, but the essential foundation upon which meaningful education depends. Privacy creates the necessary breathing room for intellectual exploration, identity formation, and authentic self-expression.[111] It establishes the conditions where students can take intellectual risks, experiment with ideas, and develop their unique voices without the chilling effects of constant observation and evaluation. Without this infrastructure, core educational functions—questioning, creating, collaborating, and dissenting—become compromised or impossible.[112]

Yet current frameworks remain trapped in a paradigm that overlooks privacy's essential function in education. While they correctly recognize privacy's role in protecting against data misuse and unauthorized disclosures, these frameworks fail to acknowledge privacy as the architectural foundation that enables intellectual exploration and personal development. By focusing almost exclusively on controlling

---

107 *See infra* Part II.

108 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

109 *See, e.g.*, PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES AND PUBLIC POLICY 212–43 (1995); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 103–57 (2009); Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904 (2013).

110 *See* Zeide, *supra* note 47, at 352–53, 386–93; Penney, *supra* note 39, at 1452–63, 1488–513.

111 *See* Cohen, *supra* note 109.

112 *See* Penney, *supra* note 39, at 1452–63, 1488–513.

information flows rather than also fostering the conditions necessary for authentic learning, they implement important but incomplete solutions. This conceptual limitation—recognizing only privacy's protective function while missing its constitutive role in education—explains why student privacy law has struggled to adapt to technological change: It addresses only part of what it aims to protect.

Addressing these theoretical gaps requires more than technical fixes to outdated definitions or exceptions. This Article employs a novel paradigmatic analysis to demonstrate how dominant models of student privacy law not only marginalize the interests of their purported beneficiaries but also fail to theorize privacy's essential role in education itself.[113] Legal paradigms do more than organize doctrinal rules; they shape how problems are perceived, which solutions seem possible, and what interests are recognized as legitimate.[114]

Paradigmatic analysis serves multiple purposes. It elucidates the current state of student privacy protection, providing a clearer understanding of how existing frameworks conceptualize and operationalize privacy in educational contexts.[115] It identifies gaps in existing frameworks, highlighting areas where current approaches fail to address the complexities of modern educational environments.[116] And it lays the groundwork for a more effective approach that better serves the multifaceted interests of students in an increasingly digitized educational landscape.[117]

Examining student privacy through a paradigmatic lens offers analytical advantages that mere doctrinal analysis cannot provide. By identifying the foundational assumptions and normative commitments that shape how we conceptualize and regulate student information, this approach reveals patterns and limitations that remain hidden in conventional legal analysis. This methodology moves beyond specific doctrinal failings to identify the deeper conceptual frameworks that have shaped student privacy governance for decades. It also highlights how these frameworks systematically prioritize certain interests and values while marginalizing others—particularly those of students themselves.

This analysis identifies three critical limitations in current approaches to protecting student privacy. First, current frameworks remain tethered to an individualistic conception of privacy, relying on procedural safeguards and individual rights rather than establishing

---

113 *See infra* Part IV.

114 *See* Julie E. Cohen, *The Regulatory State in the Information Age*, 17 THEORETICAL INQUIRIES L. 369, 374–75 (2016) (noting how legal frameworks can embed and naturalize particular power relations and value hierarchies while excluding alternative perspectives).

115 *See infra* Part II.

116 *See infra* Part III.

117 *See infra* Part IV.

substantive principles that reflect the collective needs of students in educational settings.[118] Second, existing frameworks conceptualize student privacy primarily through the lens of child protection rather than learning and development.[119] This narrow focus on protecting children's personal information overlooks privacy's essential role in supporting students as learners who require intellectual freedom to explore, question, and develop.[120] Rather than recognizing privacy as fundamental infrastructure for education itself, current approaches treat it primarily as a shield against external threats, missing its crucial role in enabling core educational functions.[121] Third, these frameworks fail to account for students' evolving capacities and agency, presenting a static view of students that ignores the developmental trajectory of children and adolescents.[122] This one-size-fits-all approach treats childhood as a monolithic category, vesting privacy decisions entirely in parents or educational institutions. The result is a framework that neither adequately protects students' current privacy interests nor prepares them to manage their own privacy as they mature.[123]

By identifying and critiquing these foundational paradigms, one can begin to construct alternatives that better align with contemporary privacy theory, educational goals, and developmental science. The following Part provides key insights into privacy law's conceptual shortcomings by exposing the descriptive and normative assumptions that undermine existing legal frameworks.[124] It identifies and critiques two dominant paradigms that have shaped student privacy law: the parent-centric paradigm and the school-centric paradigm.

II. The Dominant "Student" Privacy Paradigms

This Part employs paradigmatic analysis to identify and examine the two dominant approaches that have shaped student privacy law: a parent-centric model that positions parents as primary decision-makers over children's educational data, and a school-centric approach that grants educational institutions broad discretion over student information.

The parent-centric paradigm reflects long-standing constitutional principles of family privacy, emphasizing parents' roles as guardians and arbiters of their children's education.[125] This model is evident in statutes

118 *See infra* Section III.D.1.
119 *See infra* Section III.D.2.
120 *See infra* Section III.D.2.
121 *See infra* Section III.D.2.
122 *See infra* Section III.D.3.
123 *See infra* Part III.
124 *See infra* Part II.
125 *See infra* Section II.A.

like FERPA and PPRA that require parental consent for certain disclosures and grant parents access to and control over their children's educational records.[126] PBORs further extend this framework, providing parents greater transparency and oversight regarding educational materials and decisions.[127] By centering parental authority, this paradigm underscores the importance of family involvement in managing children's privacy within the educational context.

The school-centric paradigm, by contrast, places significant discretion in the hands of educational institutions.[128] Rooted in assumptions about institutional expertise and efficiency, this framework allows schools broad control over how student information is collected, managed, and disclosed.[129] Provisions such as FERPA's exceptions to consent requirements exemplify this paradigm, granting schools considerable flexibility in sharing data internally or with third-party vendors.[130] This approach assumes that schools are best positioned to balance educational needs with privacy protections, reflecting a trust in institutional decision-making.

Together, these paradigms constitute the foundation of contemporary student privacy law and shape its application across diverse educational contexts. Although they emphasize different priorities—parental authority versus institutional discretion—both frameworks ultimately view student privacy primarily through a child protection lens, overlooking students' evolving autonomy and distinct privacy interests as learners.

A. The Parent-Centric Paradigm

The parent-centric paradigm in student privacy law positions parents as the primary arbiters of their children's educational information and experiences.[131] This approach, deeply rooted in constitutional notions of family privacy and parental rights, has significantly shaped the development of student privacy legislation and policy in the United States.[132] By examining its historical context, key principles, and manifestations in law, this Article uncovers how this paradigm often prioritizes parental control over their children's development and education.

---

126 *See infra* Section II.A.

127 *See supra* notes 83–85 and accompanying text.

128 *See infra* Section II.B.

129 *See infra* Section II.B.

130 *See infra* Section II.B.1–2.

131 Benjamin Shmueli & Ayelet Blecher-Prigat, *Privacy for Children*, 42 COLUM. HUM. RTS. L. REV. 759, 783–85 (2011).

132 *Id.* at 761–62, 783–85.

1. FERPA's Origins: Promoting Family Privacy

The origins of the parent-centric paradigm can be traced to the social and political context of the early 1970s, a period marked by growing concerns about government surveillance and data collection practices.[133] The standard narrative surrounding the origins of FERPA situates it within broader nationwide apprehension about computer recordkeeping and government surveillance.[134]

By the late 1960s, schools had begun to employ computers to collect more extensive records on students, increasingly including surveys about students' cultural, social, and moral beliefs, as well as personality profiling.[135] These practices drew criticism for their intrusiveness and lack of transparency.[136] In 1969, the Russell Sage Foundation's report on school recordkeeping practices brought to light troubling issues in how schools collected and used student information.[137] The report revealed that schools often collected information without informed consent and used it for noneducational purposes, such as law enforcement.[138] Moreover, schools frequently withheld information about intelligence tests, personality assessments, and teacher-counselor evaluations from parents and students, fearing negative reactions to what might be perceived as critical professional observations of the students.[139]

Beyond recordkeeping concerns, broader societal shifts fueled parental anxieties about education, further driving the push for

---

133 *See Spying on Americans: Infamous 1970s White House Plan for Protest Surveillance Released*, Geo. Wash. Univ. Nat'l Sec. Archive (June 25, 2020), https://nsarchive.gwu.edu/briefing-book/intelligence/2020-06-25/spying-americans-new-release-infamous-huston-plan [https://perma.cc/PE4G-TPYV]; Ben A. Franklin, *Surveillance of Citizens Stirs Debate*, N.Y. Times (Dec. 27, 1970), https://www.nytimes.com/1970/12/27/archives/surveillance-of-citizens-stirs-debate-government-surveillance-of.html [https://perma.cc/CTH2-LV8N].

134 *See, e.g.*, U.S. Dep't of Health, Educ. & Welfare, DHEW Pub. No. (OS) 73–94, Records, Computers, and the Rights of Citizens 12, 28–30 (1973); Vance Packard, The Naked Society 135–63 (Ig Publ'g 2014) (1964); Alan F. Westin, Privacy and Freedom 3–4, 195–210 (1967).

135 *See generally* David A. Goslin & Nancy Bordier, *Record-Keeping in Elementary and Secondary Schools*, *in* On Record: Files and Dossiers in American Life 29 (Stanton Wheeler ed., 1969) (discussing recordkeeping in educational institutions); Angelika Hoyman, *Personality Testing by the Schools: A Possible Invasion of Privacy*, 4 IUSTITIA 26, 27–28 (1976) (discussing the use of personality tests on schoolchildren).

136 *See* Goslin & Bordier, *supra* note 135, at 55; Hoyman, *supra* note 135, at 27, 35–38.

137 *See generally* Russell Sage Found., Guidelines for the Collection, Maintenance & Dissemination of Pupil Records: Report of a Conference on the Ethical & Legal Aspects of School Record Keeping (1969) (providing a detailed analysis and recommendations for the handling of school records).

138 *See* Goslin & Bordier, *supra* note 135, at 64–65; *see also* Russell Sage Found., *supra* note 137, at 14, 31 (1969) (noting that many schools handled access by nonschool personnel on an ad hoc basis and had no formal policies governing access by law enforcement, courts, potential employers, colleges, and researchers).

139 *See* Russel Sage Found., *supra* note 137, at 8, 13–15.

increased parental control.[140] Parents grew increasingly worried about education policy, research, and reforms implemented in the wake of social upheaval in the late 1960s and early 1970s.[141] Some parents resisted school integration, while others fought against novel pedagogical approaches.[142] Many worried about educators implementing programs that sought to influence children's worldviews and emotions as part of the "whole child" movement.[143]

At the same time, courts and scholars increasingly recognized minors' rights in schools and children's rights as being distinct from—and sometimes in opposition to—those of their parents.[144] In *Tinker v. Des Moines Independent Community School District*,[145] the Supreme Court recognized students' right to free speech in schools.[146] These developments undermined traditional authority structures, stoking parents' fears about losing control over their children's education and upbringing.[147] In response to these concerns, parental rights advocates created the National Committee for Citizen Education ("NCCE"),[148] which mobilized to circulate information about appalling school recordkeeping practices and aimed to promote grassroots demand for reform.[149] Informed in part by this campaign, former New York City Board of Education member Diane Divoky published several exposés in the early 1970s.[150] In one article, she wrote:

> [B]y 1970, almost any government agent could walk into a school, flash a badge and send a clerk scurrying to produce a file containing

---

140 *See generally* Ben Brodinsky, *Something Happened: Education in the Seventies*, 61 PHI DELTA KAPPAN 238 (1979) (discussing several 1970s-era events affecting society's view of education).

141 *See* Elisabeth Lewis Crutchfield, The National Committee for Citizens in Education: A Descriptive Analysis 7–12 (1977) (M.A. thesis, College of William & Mary), https://dx.doi.org/doi:10.21220/s2-m9qf-3h81 [https://perma.cc/K39K-7GRP] (noting that school consolidation and the emergence of nonpartisan schools, less subject to the political process, moved control over education further away from parents).

142 Brodinsky, *supra* note 140, at 239–41.

143 Diane Divoky, *How Secret Records Can Hurt Your Child*, PARADE, Mar. 31, 1974, at 14; *see* 88 CONG. REC. 23,071–81 (1962) (statement of Rep. Ashbrook).

144 Martha Minow, *What Ever Happened to Children's Rights?*, 80 MINN. L. REV. 267, 277 (1995) ("The Supreme Court, and thus the law of the land, began to recognize children as distinct individuals deserving a direct relationship with the state under a legal regime protecting liberties against both public and private authorities.").

145 393 U.S. 503 (1969).

146 *Id.* at 503.

147 Crutchfield, *supra* note 141, at 8–11.

148 *Id.* at 2–3.

149 *Id.* at 2–4.

150 Divoky, *supra* note 143, at 14. Buckley cited Divoky's articles when he introduced FERPA, 120 CONG. REC. 13,951 (1974), as did Congressmen Koch, Edwards, and McKinney. Amelia Vance & Casey Waughn, *Student Privacy's History of Unintended Consequences*, 44 SETON HALL LEGIS. J. 515, 518 n.18 (2020) (first citing S. REP. No. 93-11, at 14,580 (1974); then citing 120 CONG. REC. 36,529 (1974); and then citing H.R. REP. No. 93-7, at 71, 84, 90 (1974)).

> the psychiatric and medical records of a former student. It was unlikely that the student would even know about the intrusion into his private life. A mother could be coolly informed that she had *no right* to see the records that resulted in her [child] being transferred to a class for the mentally retarded. A father attending a routine parent-teacher conference about his outgoing son could discover in the boy's anecdotal record comments that he was "strangely introspective" in the third grade, "unnaturally interested in girls" in the fifth, and had developed "peculiar political ideas" by the time he was 12—judgments that the father could neither retroactively challenge nor explain.[151]

Policymakers finally responded. Senator James Buckley contacted the NCCE to collaborate on what would become FERPA.[152] He introduced FERPA as a floor amendment titled "Protection of the Rights and Privacy of Parents and Students" to the General Education Provisions Act ("GEPA"),[153] an education funding bill.[154]

FERPA's original scope was remarkably broad. It protected a laundry list of information[155] and applied to "any State or local educational agency, any institution of higher education, any community college, any school, agency offering a preschool program, or any other educational institution" receiving federal funds.[156]

Initially, FERPA required parents' written consent for nearly all disclosures of personally identifiable student information,[157] with exceptions to facilitate student admissions, financial aid applications, school compliance with federal and state educational audits, and judicial subpoenas.[158] It also made an exception for instances when

---

151 Diane Divoky, *Cumulative Records: Assault on Privacy*, 2 LEARNING 18 (1973), *reprinted in* 120 CONG. REC. 36,529 (1974).

152 Crutchfield, *supra* note 141, at 19.

153 20 U.S.C. §§ 1221–1233.

154 120 CONG. REC. 13,951–53 (1974).

155 These included:

> [A]ll official records, files, and data directly related to their children, including all material that is incorporated into each student's cumulative record folder, and intended for school use or to be available to parties outside the school or school system, and specifically including, but not necessarily limited to, identifying data, academic work completed, level of achievement (grades, standardized achievement test scores), attendance data, scores on standardized intelligence, aptitude, and psychological tests, interest inventory results, health data, family background information, teacher or counselor ratings and observations, and verified reports of serious or recurrent behavior patterns.

Education Amendments of 1974, Pub. L. No. 93-380, § 513, 88 Stat. 484, 571–72 (codified as amended at 20 U.S.C. § 1232g).

156 *Id.*

157 *Legislative History of Major FERPA Provisions*, U.S. DEP'T OF EDUC. (2002), https://student-privacy.ed.gov/resources/legislative-history-major-ferpa-provisions [https://perma.cc/7ZUV-FEJY].

158 Education Amendments of 1974, Pub. L. No. 93-380, § 513, 88 Stat. 484, 572 (codified as amended at 20 U.S.C. § 1232g).

schools shared information with "other school officials, including teachers within the educational institution or [school district] who have legitimate educational interests."[159] Parents had the right to inspect and review these records.[160] They also had the right to challenge the content of their children's education records to ensure that they were not "inaccurate, misleading or otherwise" in violation of students' privacy rights, and provide opportunity to correct the information.[161]

To ensure compliance, FERPA tied adherence to its provisions directly to federal funding.[162] The Act stipulated that no funds would be made available to educational institutions that denied or prevented parents from exercising their rights under the Act.[163] This financial leverage created a powerful incentive for educational institutions to rapidly and comprehensively implement FERPA's requirements, regardless of any administrative burdens or operational challenges they might pose.[164]

Buckley's aims extended beyond mere regulation of school record-keeping.[165] He also sought to address "the dangers of ill-trained persons trying to remediate the alleged personal behavior or values of students," which included "poorly regulated testing, inadequate provisions for the safeguarding of personal information, and ill-devised or administered behavior modification programs."[166]

FERPA's very title—the *Family* Educational Rights and Privacy Act—underscores its parent-centric approach. FERPA was designed to protect families.[167] Indeed, FERPA extends beyond mere protection of family information from schools; it serves to protect against educators potentially intruding into parents' oversight of their children's values and moral development.[168] Although this approach originally aimed to protect family privacy and parental rights, it also set the stage for ongoing tensions between parental control, student autonomy, and institutional needs in the realm of modern educational privacy.

2. The PPRA: Pushing for Parental Oversight

The PPRA further entrenched a parent-centric approach to governing information in education. The statute's evolution illustrates

---

159 *Id.* § 513, 88 Stat. at 571.

160 *Id.* § 513, 88 Stat. at 572.

161 *Id.*; *see also* Crutchfield, *supra* note 141, at 8–11.

162 Education Amendments of 1974, Pub. L. No. 93-380, § 513, 88 Stat. 484, 571 (codified as amended at 20 U.S.C. § 1232g).

163 *Id.*

164 *See* 20 U.S.C. § 1232g(a)(2) ("No funds shall be made available under any applicable program [unless statutory requirements are met].").

165 120 CONG. REC. at 14,580–81 (1974) (statement of Sen. James Buckley).

166 *Id.*

167 *Id.*

168 *See id.*

how student privacy law has increasingly prioritized parental rights, reflecting growing parental anxieties about educational innovation and a desire to assert control over curriculum content. Like FERPA, the PPRA began as a floor amendment to the GEPA education funding bill in 1974.[169] Representative Jack Kemp introduced the law on March 27, days after Diane Divoky's *Parade* exposé.[170] The initial amendment was called "Protection of Pupil Rights" and required schools to allow parents to inspect instructional material used "in connection with any research or experimentation program," defined as those "designed to explore or develop new or unproven teaching methods or techniques."[171]

Senator Orrin Hatch drastically expanded the amendment four years later in response to escalating concerns regarding schools' use of personality and psychological tests for various purposes, including diagnosing problems, shunting students into specialized programs, and prompting therapeutic interventions.[172] The amendment reflected a growing discomfort among parents and policymakers with what they perceived as intrusive educational practices.[173] This discomfort was not limited to data collection but extended to concerns about how such information might be used to shape students' educational experiences without parental input or consent.[174]

Parents and policymakers saw educators' use of personality and psychological tests as intruding on family privacy—not just in asking about intimate personal details such as family dynamics, ethical beliefs, and self-image, but in encroaching on parents' prerogatives over their children's upbringing.[175] Some parents even worried that asking questions about suicide, for example, might give their children dangerous ideas.[176] These issues came to public attention in 1973, when a mother successfully sued to enjoin a school from administering a personality test to her eighth-grade child.[177] The survey probed into

---

169 Education Amendments of 1974, Pub. L. No. 93-380, 88 Stat. 574; Elementary and Secondary Education Amendments of 1967, Pub. L. No. 90-247, 81 Stat. 783, *amended by* 92 Stat. 2355 (1978). These were also amendments to GEPA.

170 *See* 120 CONG. REC. at 8,505 (1974) (statement of Rep. Jack Kemp).

171 Education Amendments of 1974, Pub. L. No. 93-380, § 514, 88 Stat. 574.

172 *See* Hoyman, *supra* note 135, at 27–28; Michael J. Zdeb, *A Student Right of Privacy: The Developing School Records Controversy*, 6 LOY. U. L.J. 430, 433 (1975).

173 Bert I. Greene & Marvin Pasch, *The Hatch Amendment Regulations: Lessons for Social Studies Educators*, 77 SOC. STUD. 111, 114 (1986).

174 *Id.*

175 *See* Meyer v. Nebraska, 262 U.S. 390, 396 (1923) (striking down a state law prohibiting foreign language instruction); Pierce v. Soc'y of Sisters, 268 U.S. 510, 534–35 (1925) (striking down a state law requiring attendance at nonparochial school).

176 Greene & Pasch, *supra* note 173, at 113–14.

177 Merriken v. Cressman, 364 F. Supp. 913, 918 (E.D. Pa. 1973). The court noted that:

> The questionnaire would have asked "whether the student's family is 'very close, somewhat close, not too close, or not close at all,' . . . whether [his parents] told him how 'much

his family life to identify future drug users and "deviant[s]" to send to mandatory therapy.[178]

Senator Hatch's 1978 amendment to the PPRA emerged as a direct response to these mounting concerns, with the Senator's frequent reference to his amendment as the "parental consent amendment" underscoring its fundamental aim of expanding parental oversight of educational practices.[179] Indeed, the amendment expanded the purview of parental control, extending beyond experimental educational materials to encompass a wide range of educational activities and content.[180] It required schools to obtain written parental consent before surveying students if the survey's primary purpose was to obtain information about any of seven controversial subjects, including family, political affiliation, mental health, sexual behavior, finances, and illegal behavior.[181] By requiring affirmative parental consent, the amendment positioned parents as gatekeepers, able to prevent their children's exposure to or participation in certain types of information-gathering activities within schools.[182]

The PPRA's scope expanded further in 1984 when new regulations added another layer of parental control.[183] Parents were concerned about educators discussing values that diverged from their own, particularly on sensitive or controversial topics, such as nonheteronormative identities[184] and "psychological topics and techniques . . . includ[ing]: death education; curricula pertaining to alcohol and drugs; instruction in nuclear war; one-world government or globalism curricula; discussions of witchcraft and the occult; political affiliations and beliefs of student and family; autobiography assignments, and sociograms."[185] Additionally, the regulations gave parents the right to access any instructional material used in research or experimentation programs "designed to explore or develop new or unproven teaching methods or techniques."[186]

---

they loved him[],' . . . whether his parents 'seemed to know what [his] needs or wants [were],' . . . and whether the student '[felt] that he is loved by his parents.'"

Id.

178 *Id.* at 916. Students who were identified as potential drug users, deviants, or "emotionally handicapped" would be required to undergo therapy to change their "cognitive and affective domains." *Id.* at 915–17.

179 124 CONG. REC. 27,423 (1978).

180 *See id.* (requiring written parental consent before a secondary or elementary student "is subjected to psychiatric, behavior probing or other nonscholastic and nonaptitude testing").

181 Lynn M. Daggett, *Student Privacy and the Protection of Pupil Rights Act as Amended by No Child Left Behind*, 50 U.C. DAVIS J. JUV. L. & POL'Y 51, 65 (2008).

182 *See, e.g.*, Beth Garrison, *Children Are Not Second Class Citizens: Can Parents Stop Public Schools from Treating Their Children Like Guinea Pigs?*, 169 VALPARAISO U. L. REV. 147, 168–69 (2004).

183 Greene & Pasch, *supra* note 173, at 111, 113, 115.

184 *See id.* at 113.

185 *Id.* at 114.

186 34 C.F.R. § 98.3(a)(b) (providing access to all instructional material used in a research or experimentation program, defined as "any program or project in any program").

The most significant expansion of the PPRA occurred in 2002 as part of the No Child Left Behind Act ("NCLB").[187] Representative Todd Tiahrt introduced this expansion as the "Parental Freedom of Information" amendment with the stated goal of "plainly and unambiguously defin[ing] the rights parents have under the law."[188] The NCLB amendments introduced a series of opt-out requirements for additional school activities.[189]

The NCLB amendments to the PPRA centered around three key categories of opt-out rights for parents.[190] First, parents could now remove their children from any "nonemergency, invasive physical examination or screening," addressing concerns about health surveys or screenings not directly related to immediate student safety.[191] Second, they gained the right to opt their children out of activities involving "[t]he collection, disclosure, or use of personal information collected from students for the purpose of marketing," responding to growing unease about the commercialization of education and potential misuse of student data.[192] Third, parents could exempt their children from participating in any survey that explored sensitive topics, regardless of the survey's funding source.[193]

In addition to these opt-out rights, the NCLB amendments substantially expanded parental access rights. Parents were now entitled to review instructional materials and surveys used in routine educational activities, not just experimental or sensitive materials.[194] This broadened access meant that parents could examine a much wider range of educational content that their children might encounter, from textbooks and supplementary reading materials to classroom handouts and digital resources.[195]

The evolution of the PPRA from its inception to its most recent amendments reflects a consistent trend toward increasing parental control, further cementing the parent-centric paradigm in student privacy law. Each amendment has broadened the range of educational activities and information subject to parental oversight, reflecting a broader

---

187 No Child Left Behind Act of 2001, Pub. L. No. 107-110, 115 Stat. 1425 (2002) (codified as amended in scattered Sections of 20 U.S.C.).

188 147 CONG. REC. H2577-01 (daily ed. May 23, 2001) (statement of Rep. Todd Tiahrt); *see also id.* (statement of Rep. Bob Schaffer) ("Mr. Chairman, this is a good amendment because at its core it empowers parents, and that really should be what we are all about here in Congress, is finding ways to empower parents to the greatest extent possible.").

189 20 U.S.C. § 1232h(c)(2)(C).

190 *Id.*

191 *Id.*

192 *Id.* § 1232h(c)(1)(E).

193 *Id.* § 1232h(b).

194 *Id.* § 1232h(c)(1)(A)(i), (C)(i).

195 *Id.*; *see also* 34 C.F.R. § 98.3; Daggett, *supra* note 181, at 91–92.

societal push to prioritize family values and autonomy among evolving educational methodologies and priorities.[196]

3. Parental Rights Laws: Imposing Moral Values

Contemporary manifestations of the parent-centric paradigm have grown even more expansive. Illustratively, the recent PBOR state legislation extends parental control into previously private spaces of student life.[197] Such legislative efforts build upon the foundation laid by earlier federal laws, continuing to reshape education by increasing parental control over their children's educational experiences and information access.[198] This recent emphasis on parental authority across the country also signals a broader national trend that goes beyond controlling information flows in schools to reshaping education along tightly controlled, traditional lines.[199] These laws seek to codify and expand parental rights in education, often using the language of transparency and accountability to establish increased parental oversight.[200]

A prime example is the federal Parents Bill of Rights Act, passed in 2023 in the U.S. House of Representatives.[201] The bill seeks to amend FERPA and the PPRA to significantly broaden the scope of parental rights in education.[202] One of its key provisions aims to give parents expansive access to educators' instructional and administrative information, beyond the access rights initially granted by FERPA or the PPRA.[203]

One of the most significant aspects of the proposed federal Parents Bill of Rights Act is its potential impact on schools' use of educational technology.[204] The bill would require schools to notify parents and provide justification when disclosing personally identifiable student information to technology vendors and others outside the school system.[205] It would also narrow the definition of appropriate "legitimate educational purpose[s]" for data sharing to "the exclusive purpose of developing, evaluating, or providing educational products or services for, or to, students or schools."[206] This provision would effectively eliminate

---

196 *See* Daggett, *supra* note 181, at 73–108.

197 *See, e.g.*, Parents' Bill of Rights, H.B. 2161, 55th Leg., 2d Reg. Sess. § 15-117 (Ariz. 2022).

198 *See id.*

199 *See* Jeremy C. Young, Jonathan Friedman & Kasey Meehan, Pen America, America's Censored Classrooms 2023 (2023), https://pen.org/report/americas-censored-classrooms-2023 [https://perma.cc/W3LY-ESWH].

200 *See, e.g.*, Parents' Bill of Rights, H.B. 2161, 55th Leg., 2d Reg. Sess. § 15-117 (Ariz. 2022).

201 *See* Parents Bill of Rights Act, H.R. 5, 118th Cong. (2023).

202 *See id.*

203 *See id.* at §§ 104, 201, 202.

204 *See id.* § 201(k).

205 *See id.*

206 *Id.* § 202(f)(A).

FERPA's school official exception.[207] The implications of this change could be substantial. Given the difficulties of adapting instructional content and technology choices to each parent's privacy preferences, educators might abandon certain teaching materials or technologies altogether.[208]

Beyond technology use, the House bill would expand parents' access to school records—including not only instructional but also administrative, training, and budget information.[209] It aims to give parents the right to know what their children are being taught, information about school budgets and spending, and knowledge of any violent activity at school.[210]

States have enacted similar statutes that give parents even more control over what ideas children are exposed to and more access to educators' information.[211] Virginia law, for example, protects the right of parents to review any audiovisual materials used in the classroom to ensure that they align with the family's values.[212] Texas's SB 393 requires explicit parental permission for students to receive instruction about or participate in clubs related to gender and sexual identity.[213] It also provides parents with more oversight over their children by requiring educators to disclose information regarding their child's physical or mental health.[214] New Hampshire creates a right for parents to inquire if their child is being referred to by a name or gender different from their official records.[215] Parents may not be physically at hand in the classroom, but the implementation of such policies will, in essence, make them omnipresent in their child's life.

B. The School-Centric Paradigm

The school-centric paradigm emerged as a powerful counterweight to parental control, reflecting both practical necessities and deeper assumptions about institutional expertise in the digital age.[216] This shift in focus repositioned educational institutions as the primary decision-makers regarding student data and privacy.[217] This framework,

---

207 *See id.*; 20 U.S.C. § 1232g(b)(1)(A) (school official exception).

208 *See* H.R. 5, 118th Cong. § 202(b) (providing parents with rights to notice and consent to schools' use of classroom technology).

209 *See id.* §§ 102, 104.

210 *See id.* § 104 (providing a list of parents' rights to information about their child's education).

211 *See id.* §§ 102, 104, 202.

212 VA. CODE ANN. § 22.1-207.2 (2020).

213 S.B. 393, 88th Leg. § 26.016(b) (Tex. 2023).

214 *Id.* § 26.0083(a)(1).

215 S.B. 272, 2023 Leg., Ch. 189-B:3(I)(u)–(v) (N.H. 2023).

216 *See infra* Section II.B.1.

217 *See infra* Sections II.B.1–.3.

which has evolved through legislative changes, agency interpretations, and institutional practices, stands in stark contrast to the parent-centric model discussed in the prior section.[218] At its core, the school-centric approach is predicated on the belief that educational institutions are best positioned to make informed decisions about student data use and disclosure given their unique understanding of educational contexts and needs.

1. FERPA's Exceptions: Granting Schools Discretion

The school-centric paradigm emerged in the immediate aftermath of FERPA's enactment in 1974.[219] Although the original statute granted parents unprecedented rights—including the right to access their children's records, challenge the content of these records, and require consent for the release of personally identifiable information,[220] this robust protection of parental rights was short-lived.[221]

President Gerald Ford signed FERPA into law on August 21, 1974, and it became effective ninety days later.[222] A coalition of educational institutions and professional associations immediately mobilized, critiquing the law as unworkable for three primary reasons.[223] First, they criticized the requirement that they give parents detailed notice as being impossibly burdensome, potentially overwhelming schools with paperwork and impeding their ability to function efficiently.[224] Second, they complained that providing parents and eligible students

---

218 *See infra* Sections II.B.1–.3.

219 *See infra* notes 223–32 and accompanying text.

220 FERPA originally required schools to obtain written consent before every disclosure of covered information. *See supra* note 157 and accompanying text.

221 *See infra* notes 223–32 and accompanying text.

222 *Legislative History of Major FERPA Provisions*, U.S. DEP'T OF EDUC. (June 2002), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/ferpaleghistory.pdf [https://perma.cc/VC8F-KPMM].

223 120 CONG. REC. 39,862 (1974) (noting that the educational community pointed to "certain ambiguities . . . contained in the language and provisions—that because there was none of the normal legislative history, it means that [the U.S. Department of Health, Education, and Welfare] does not have an adequate record . . . to develop the necessary regulations.").

224 *See* ALFRED B. FITT, A SPECIAL REPORT FROM THE WASHINGTON OFFICE OF THE COLLEGE ENTRANCE EXAMINATION BOARD (1975), *reprinted in* HIGHLAND CAVALIER, Jan. 27, 1975, at 2–3 (discussing the additional steps taken by Senators to correct technical errors in the Act to assuage universities' concerns); *see also* Edward B. Fiske, *School Data Law Draws Criticism*, N.Y. TIMES, Oct. 13, 1974, at 46, https://www.nytimes.com/1974/10/13/archives/school-data-law-draws-criticism-alarm-voiced.html [https://perma.cc/S2C9-5AKT] (discussing how chief executives at six major higher education institutions requested delaying FERPA's effective date in order to provide time for hearings to prevent unintended consequences); Carole M. Mattessich, Recent Development, *The Buckley Amendment: Opening School Files for Student and Parental Review*, 24 CATH. U. L. REV. 588, 596–99 (1975) (discussing the lobbying efforts by a postsecondary educational association to delay the implementation of FERPA due to legal concerns over the Act's effect on confidentiality).

too much control over educators' use—and disclosure—of information would interfere with schools' practical and pedagogical needs.[225] Third, higher education institutions objected that granting students complete access to their education records, including confidential recommendation letters, would undermine the integrity of the admissions process, potentially discouraging candid evaluations and hindering institutions' ability to make informed decisions about applicants.[226] These objections reflect a fundamental conflict between the ideal of students' and families' privacy rights and the practical realities of operating an educational institution.[227]

Congress responded by postponing FERPA's effective date[228] and sent the bill to the committee for revisions.[229] The resulting Joint Amendment, introduced by Senator Buckley and Senator Claiborne Pell in December 1974, marked a pivotal shift toward the school-centric paradigm.[230] The rationale behind these changes, as articulated by Senators Buckley and Pell, was to address concerns that the original statute's restrictions were "too narrow and, if strictly applied, would seriously interfere in the operation of educational institutions."[231] The measure passed and was applied retroactively to the statute's original effective date.[232]

These amendments focused on three areas: the scope of protected information, the introduction of "directory information," and the expansion of the school official exception.[233] First, the amendment broadened the concept of protected information by introducing the term "education record[]" covered by FERPA, replacing the original law's specific list of protected documents.[234] This change gave schools greater latitude to determine what information falls under FERPA's protection, effectively allowing them to define the boundaries of

---

225 Fitt, *supra* note 224, at 2–3; *see also* Fiske, *supra* note 224; Mattessich, *supra* note 224, at 597.

226 Fiske, *supra* note 224.

227 Fitt, *supra* note 224, at 2–3; *see also* Fiske, *supra* note 224; Mattessich, *supra* note 224, at 597.

228 *See* Mattessich, *supra* note 224, at 588–89.

229 *See* S. REP. NO. 93-1409, at 10 (1974) (Conf. Rep.) (noting that FERPA, as originally enacted, "contain[ed] a laundry list of items which are to be available to parents and students and ma[de] inconsistent references to 'personally identifiable information, school records,' etc.," and explaining that the new amendment "uses the generic designation, 'education records' and defines that term."); 120 CONG. REC. 40,549 (1974) (same).

230 *See* Mattessich, *supra* note 224, at 588–89, 599.

231 120 CONG. REC. 39,863 (1974) (Joint Statement in Explanation of Buckley/Pell Amendment).

232 *Id.* at 39,863, 39,866.

233 S. REP. NO. 93-1409, at 3–8 (1974) (Conf. Rep.).

234 *Id.* at 5; 120 CONG. REC. 40,548. Specifically, the amendment defined "education records" as "those records, files, documents, and other materials which (i) contain information directly related to a student; and (ii) are maintained by an educational agency or institution or by a person acting for such agency or institution." *Id.*

student privacy protection.[235] The amendment also clarified that the right of parental challenges to records was not a broad right to contest educators' professional opinions or assessments like grades.[236]

Building on this redefinition, the amendment addressed concerns that the original statute might prevent schools from publishing routine information, such as football players' weights or students' names in a school play.[237] To resolve this issue, the Joint Amendment created an exclusion for "directory information."[238] This new provision allowed schools to share a wide range of personal information about students that "would not generally be considered harmful or an invasion of privacy if disclosed."[239] This data includes, but is not limited to "the student's name; address; telephone listing; electronic mail address; photograph; date and place of birth; . . . weight and height of [athletes]; . . . and awards received."[240] Because of this change, schools can unconditionally share whatever they define as directory information unless a parent opts out in advance.[241]

Perhaps most significantly, the Joint Amendment drastically reduced the constraints of the original statute's school official exception.[242] Instead of requiring written consent for every disclosure of covered information, schools could share information with any recipient who "[p]erforms an institutional service or function" that the school determines serves "legitimate educational interests."[243] They did not have to formally designate information recipients as "school officials," specify what legitimate educational purposes a disclosure served, or track who requested or obtained access to students' records and for what purpose.[244] This broad exception allowed schools to share student information with a wide range of individuals and entities without parental consent as long as they could plausibly articulate an educational purpose.[245]

---

235 *See* S. REP. NO. 93-1409, at 10 (1974) (Conf. Rep.); 120 CONG. REC. 40,549.

236 The amendment clarified the right to challenge records, specifying that this was "to insure that the records are not inaccurate, misleading, or otherwise in violation of the privacy or other rights of students, and to provide an opportunity for the correction or deletion of any such inaccurate, misleading, or otherwise inappropriate data contained therein." 120 CONG. REC. 39,864 (1974) (Joint Statement in Explanation of Buckley/Pell Amendment).

237 *See* 34 C.F.R. §§ 99.3, 99.31(a)(11), 99.37 (2023) (establishing the "directory information" exception).

238 *Id.*; *Frequently Asked Questions*, U.S. DEP'T OF EDUC., https://www.ed.gov/about/contact-us/faqs [https://perma.cc/7AL8-5SLV].

239 34 C.F.R. § 99.3.

240 *Id.*

241 *See id.* §§ 99.31 (a)(11), 99.37.

242 *See* 120 CONG. REC. 39,863 (1974).

243 34 C.F.R. § 99.31(a)(1)(i)(A).

244 *Id.*

245 *See* 34 C.F.R. § 99.31(a)(1)(i)(A).

2. *FERPA's Modern Exceptions: Promoting Technocratic Reform*

The changes did not stop there. FERPA amendments continued to give educators more discretion over student information disclosure to facilitate technology use in schools.[246] In the early 2000s, educators increasingly relied on vendors to provide classroom technology for students, teachers, and administrators.[247] The law's initial focus on physical records and limited disclosure scenarios did not account for digital recordkeeping or the involvement of third-party technology providers in educational services.[248]

When FERPA was initially enacted, schools primarily used the school official exception to share personally identifiable student information with substitute teachers and parent volunteers.[249] As schools entered the digital era, however, they were unsure about whether—or when—they could share personally identifiable student information with technology vendors[250] and questioned whether email or records stored on cloud-based services should even be considered part of students' education records.[251]

This uncertainty prompted a series of regulatory changes that further solidified the school-centric approach to student privacy.[252] The Department of Education amended the regulations related to the school official exception in 2008 and again in 2011 to support outsourcing to technology vendors, sharing data with researchers, and creating SLDSs.[253] These changes facilitated schools' ability to outsource work to technology providers in two significant ways. First, they allowed schools to share student data with third-party service providers without obtaining parental consent.[254] Second, the 2011 amendments allowed for the

---

246 *See infra* notes 252–70 and accompanying text.

247 *See generally* Zeide, *supra* note 47 (providing examples of technology provided by private vendors that are widely used in classrooms).

248 *See id.* at 373.

249 *See id.* at 360.

250 *See, e.g.*, *Family Educational Rights and Privacy Act: Section-by-Section Analysis*, WRIGHT'S LAW 5 (Dec. 2008), https://www.wrightslaw.com/law/ferpa/finalrule.sec.analysis.08.pdf [https://perma.cc/F9VJ-9USA] (noting that the pre-amendment regulations did not clarify the extent of the school officials exception); Family Educational Rights and Privacy, 76 Fed. Reg. 75,604, 75,607 (proposed Dec. 2, 2011).

251 *Cf.* REIDENBERG ET AL., *supra* note 13, at 1–7, 17, 24–25 (discussing the various ways schools across the country treat cloud-based data and how this treatment implicates privacy rights under FERPA and other privacy statutes).

252 *Cf.* WRIGHT'S LAW, *supra* note 250 (explaining the 2008 FERPA amendments); Family Educational Rights and Privacy, 76 Fed. Reg. at 75,607.

253 *See generally* WRIGHT'S LAW, *supra* note 250 (explaining 2008 FERPA amendments); Family Educational Rights and Privacy, 76 Fed. Reg. at 75,607.

254 Family Educational Rights and Privacy, 73 Fed. Reg. 74,806, 74,852 (Dec. 9, 2008).

nonconsensual disclosure of student data for audits, evaluations, or enforcement of education programs.[255]

The 2008 amendments marked a particularly significant expansion of the school-centric paradigm. They expanded the definition of "school officials" to include "contractor[s], consultant[s], volunteer[s]," and "other part[ies] to whom an [educational] agency or institution has outsourced institutional services or functions" that it would otherwise use employees to perform.[256] This amendment was explicitly designed to facilitate schools' ability to share student data with technology vendors without obtaining parental consent.[257]

In an attempt to address potential privacy concerns, the regulations required schools to use "reasonable methods" to exercise "direct control" over these newly defined school officials.[258] However, the Department of Education has provided little concrete guidance on what constitutes either "reasonable methods" or "direct control."[259] The Department's guidelines only note that "reasonableness" should correspond to the magnitude of harm presented by different types of information and should reflect the customary practices of similarly situated institutions.[260] In fact, agency guidance repeatedly responds to questions with "it depends."[261] This lack of specific guidance gives schools considerable discretion in determining what constitutes appropriate safeguards when sharing data with third-party providers.[262] The legitimate educational interest standard thus nominally limits school power, but in practice, it does not restrict schools' collection, use, and disclosure of student data.[263]

In 2011, the Department further amended FERPA regulations again to facilitate compliance with reporting requirements for outside research and to create SLDSs.[264] These 2011 exceptions further relaxed restrictions, relying on contractual guarantees rather than requiring

---

255 Family Educational Rights and Privacy, 76 Fed. Reg. at 75,618; JOHN MORAN, CONN. GEN. ASSEMB. OFF. OF LEGIS. RSCH., FERPA, RECENT CHANGES IN FEDERAL REGULATIONS, AND STATE COMPLIANCE, 2014-R-0127, at 5 (2014), https://www.cga.ct.gov/2014/rpt/pdf/2014-R-0127.pdf [https://perma.cc/JH7P-WFP7].

256 34 C.F.R. § 99.31(a)(1)(i)(B) (2015); Family Educational Rights and Privacy, 73 Fed. Reg. at 74,852.

257 *See generally* WRIGHT'S LAW, *supra* note 250 (explaining 2008 FERPA amendments).

258 *See* 34 C.F.R. § 99.31(a)(1)(i)(B)(2)–(a)(1)(ii).

259 *See* U.S. DEP'T OF EDUC. PRIV. TECH. ASSISTANCE CTR., GUIDANCE FOR REASONABLE METHODS AND WRITTEN AGREEMENTS 4–6 (2015), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Guidance_for_Reasonable_Methods%20final_0_0.pdf [https://perma.cc/N7B3-9RXF].

260 *See id.*

261 *See, e.g.*, U.S. DEP'T OF EDUC., *supra* note 98.

262 Zeide, *supra* note 47, at 343; Zeide, *supra* note 40, at 105.

263 Zeide, *supra* note 47, at 339; Zeide, *supra* note 40, at 105.

264 *See* U.S. DEP'T OF EDUC. PRIV. TECH. ASSISTANCE CTR., *supra* note 259, at 4–6.

parental consent or even the school official exception covered above.[265] Specifically, these amendments expanded the definition of "authorized representative" to include any individual or entity designated by a state or local educational authority or federal official to conduct audit, evaluation, enforcement, or compliance activities relating to education programs.[266] This broadened definition allowed for more extensive sharing of student data with researchers and state agencies without parental consent.[267]

Additionally, the amendments expanded the definition of "education program" to encompass any program "principally engaged in the provision of education, including . . . early childhood education, elementary and secondary education, postsecondary education, special education, job training, career and technical education, and adult education."[268] This expansion facilitated the aforementioned creation of SLDSs, allowing for more comprehensive tracking of student outcomes across educational levels.[269] These amendments fundamentally altered the balance of power in educational privacy governance.

The evolution of FERPA from its original focus on parental rights and student privacy to a more permissive stance on data sharing reflects broader changes in educational philosophy and technology.[270] The law's transformation has enabled the growth of data-driven educational practices and research, but it has also weakened the privacy protections at the core of FERPA's initial purpose. This tension between data utility and individual privacy rights continues to be a central challenge in interpreting and applying FERPA in the modern educational landscape.

At present, educators exercise expansive discretion to share covered information with any technology provider, web service, or mobile app, absent an additional local or state requirement.[271] These amendments reflect a broader trend toward data-driven decision-making in education, prioritizing institutional efficiency and research potential over

---

265 Family Educational Rights and Privacy, 76 Fed. Reg. 75,604, 75,617 (Dec. 2, 2011).

266 34 C.F.R. § 99.35(a) (2012).

267 States reacted to the expansion by creating their own protections for student information. *See, e.g.*, CAL. BUS. & PROF. CODE § 22584(b)(1) (West 2016) (prohibiting targeted advertising); *id.* § 22584(3) (prohibiting the direct sale of covered information); *see also* COLO. REV. STAT. § 22-16-107 (2022) (prohibiting targeted advertising and sale of student information).

268 34 C.F.R. § 99.3.

269 *See* ZEIDE, *supra* note 58, at 4.

270 *See supra* notes 247–69 and accompanying text.

271 *See* CONSORTIUM FOR SCH. NETWORKING, STUDENT DATA PRIVACY TOOLKIT PART 2: PARTNERING WITH SERVICE PROVIDERS 12, 30 (2023) (discussing that if the provider will be using FERPA-protected information, schools and districts should exercise caution when entering into click-wrap agreements that allow for amendment without notice given FERPA's requirement to maintain "direct control" over the use and maintenance of the information under the school official exception).

individual privacy concerns.[272] Although proponents argue that these changes enhance educational outcomes, critics worry about the erosion of student privacy protections in an increasingly digital learning environment.[273]

3. Enforcement: Reinforcing the School-Centric Paradigm

The enforcement history of student privacy laws in the United States reveals a persistent school-centric paradigm that prioritizes institutional interests over stringent protection of individual privacy rights. This approach to enforcement, established by FERPA and reinforced through subsequent legal interpretations and administrative practices, has created an environment where the convenience of educational institutions often takes precedence over robust privacy protections for students.[274]

FERPA's structural design as a spending clause statute reveals fundamental tensions between its protective aims and institutional implementation. FERPA's primary enforcement tool is the withholding of federal funds from noncompliant institutions.[275] This reliance on conditional funding, rather than outright prohibition, constrains the effectiveness of FERPA's privacy safeguards.[276] The enforcement mechanism creates a paradox because withdrawing funds will harm students just as much, if not more, than poor privacy practices.[277] The extreme nature of the penalty—the complete loss of federal funding—makes it an impractical tool for addressing privacy violations, and the Department of Education has never invoked this "nuclear" option of withdrawing federal funding for FERPA violations in the statute's fifty-year history.[278]

The pre-2002 era of FERPA enforcement saw some federal circuits recognizing FERPA as protecting individual rights, creating a more diverse enforcement landscape. For example, in *Fay v. South Colonie Central School District*,[279] the Second Circuit upheld a district court's

---

272 *See supra* notes 247–69 and accompanying text.

273 *See, e.g.*, Zeide, *supra* note 58, at 5.

274 *See supra* Sections II.B.1–.2.

275 20 U.S.C. § 1232g(b)(1).

276 *See* Zach Greenberg & Adam Goldstein, *Baking Common Sense into the FERPA Cake: How to Meaningfully Protect Student Rights and the Public Interest*, 44 J. OF LEGIS. 22, 24–33 (2017) (explaining FERPA's origin and its enforcement shortfalls).

277 *See id.* at 31–32 ("Despite having the power to reduce schools to financial ruin by terminating their federal funding, the Office of the Chief Privacy Officer's reluctance to even attempt to take this step has rendered FERPA a meaningless deterrent.").

278 Zeide, *supra* note 47, at 368; *see* 20 U.S.C. § 1232g(b)(1) (describing the fund withholding provision); Letter from LeRoy S. Rooker, Director, Fam. Pol'y Compliance Off., to Dr. Hunter Rawlings III, President, Cornell Univ. (Feb. 28, 2000).

279 802 F.2d 21, 33 (2d Cir. 1986).

award of nominal damages under 42 U.S.C. § 1983 when the school denied a father access to his child's education records.[280] However, even then, courts showed a marked reluctance to impose severe penalties on educational institutions.[281]

The Supreme Court's landmark 2002 decision *Gonzaga University v. Doe*[282] rejected this interpretation, holding that FERPA does not create enforceable individual rights.[283] In this case, a former student sued Gonzaga University claiming that the school had violated his FERPA rights by disclosing information about alleged sexual misconduct to the state's teachers' certification agency.[284] Like the plaintiff in *Fay*, he sued the school under 42 U.S.C. § 1983, seeking damages for the claimed FERPA violation.[285]

The Court's reasoning focused on the specific language of FERPA, which states that federal funding shall be withheld from institutions with a "policy or practice" of permitting release of student records.[286] Chief Justice Rehnquist, writing for the majority, emphasized that this language was directed at institutional policies rather than individual instances of disclosure.[287] The Court concluded that such language did not confer individual rights enforceable under § 1983.[288]

In the wake of *Gonzaga*, administrative enforcement by the Department of Education has become the sole mechanism for ensuring school compliance with FERPA.[289] The investigation process typically begins with a complaint filed by a parent, eligible student, or in some cases, a third party who believes a violation has occurred.[290] The Student Privacy Policy Office, formerly the Family Policy Compliance Office, within the Department of Education then reviews the complaint, requests information from the school in question, and conducts interviews or site visits in more complex cases.[291] Most cases, however, are resolved without full investigations, and no proceedings have been initiated to withhold funding.[292]

---

280 *See Fay*, 802 F.2d at 34 (finding Fay could state a claim under 42 U.S.C. § 1983 for FERPA violations). These courts also held, however, that FERPA did not itself create a private right of action. *Id.* at 33; *Tarka*, 917 F.2d at 891.

281 *See Fay*, 802 F.2d at 27.

282 536 U.S. 273 (2002).

283 *Id.* at 276–77 (holding that FERPA does not create individual rights and thus cannot be enforced under 42 U.S.C. § 1983).

284 *Id.* at 277.

285 *Id.* at 276–77, 283; *Fay*, 802 F.2d at 33; *Tarka*, 917 F.2d at 891.

286 *Gonzaga*, 536 U.S. at 276.

287 *Id.* at 276, 288–91.

288 *Id.* at 287–88.

289 *See* Greenberg & Goldstein, *supra* note 276, at 32–33

290 *See* 34 C.F.R. § 99.63 (2023).

291 *See id.* §§ 99.64–66.

292 *See* Greenberg & Goldstein, *supra* note 276, at 31–32.

This small office is tasked with investigating complaints, providing technical assistance, and ensuring compliance across the nation's educational system.[293] The limited resources allocated to this office inherently constrain its ability to conduct proactive investigations or engage in rigorous enforcement actions.[294]

The Department of Education's Office of Inspector General's 2018 report illuminated systemic deficiencies in FERPA's enforcement infrastructure.[295] The investigation revealed chronic institutional inefficiency, with some complaints remaining unresolved for years.[296] Results of the inquiry also demonstrated the absence of a documented process for tracking complaints and monitoring the progress of investigations.[297]

Although the Department subsequently implemented new processes to prioritize complaints based on their severity and impact and began coordinating with other Department offices to develop more effective remediation strategies, these administrative adjustments have yet to yield substantive changes in enforcement patterns.[298]

The College Board's practices illustrate this problem. For years, it was standard procedure for the company to collect sensitive information from students under thirteen years old through pretest surveys and sell this data to colleges, universities, and scholarship services for marketing.[299] This routine practice occurred without obtaining the parental consent required by federal privacy laws.[300] The Department of Education's Privacy Technical Assistance Center did not address these practices until 2018, when it finally issued a Technical Assistance Letter warning schools that minor students' consent was not enough share this information under FERPA and PPRA.[301] Even then, it took another six

---

293 *See* Lynn M. Daggett, *FERPA in the Twenty-First Century: Failure to Effectively Regulate Privacy for All Students*, 58 CATH. U. L. REV. 59, 91 (2008).

294 *See id.* (explaining that the Family Policy Compliance Office's limited staff is responsible for enforcing FERPA and PPRA and "deal[ing] with complaints asserting violations, provides model policies and other technical assistance, and takes on special tasks").

295 OFF. OF INSPECTOR GEN., U.S. DEP'T. OF EDUC., ED-OIG/A09R0008, OFFICE OF THE CHIEF PRIVACY OFFICER'S PROCESSING OF FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT COMPLAINTS 5 (2018).

296 *Id.* at 12–13.

297 *Id.* at 20–21.

298 *See* OFF. OF MGMT., U.S. DEP'T OF EDUC., IMPROVING THE EFFECTIVENESS AND EFFICIENCY OF FERPA ENFORCEMENT 2–3 (2018).

299 PRIV. TECH. ASSISTANCE CTR., U.S. DEP'T OF EDUC., PTAC-FAQ-10, TECHNICAL ASSISTANCE ON STUDENT PRIVACY FOR STATE AND LOCAL EDUCATIONAL AGENCIES WHEN ADMINISTERING COLLEGE ADMISSIONS EXAMINATIONS 1 (2018), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/TA%20College%20Admissions%20Examinations.pdf [https://perma.cc/D7M9-C8M5].

300 *Id.* at 9.

301 *Id.* at 1.

years for any meaningful enforcement, when New York finally secured a $750,000 settlement from the College Board in 2024.[302]

State-level enforcement of student privacy laws reinforces the school-centric paradigm. Many states have enacted seemingly strong privacy laws, but these often lack effective enforcement mechanisms, rendering them more symbolic than substantive.[303] These laws, although appearing to offer strong protections, often fail to provide meaningful recourse for individual privacy violations.[304] This is the case even with bright-line policies, such as requiring parental consent before schools collect biometric identifiers,[305] record students on video,[306] or share information internally or with local school districts.[307] Accordingly, both federal and state student privacy laws provide no accountability when schools fail to act as faithful data stewards.

This comprehensive overview of the enforcement landscape reveals a persistent school-centric paradigm in student privacy law. From FERPA's spending clause foundation to the post-*Gonzaga* emphasis on administrative remedies, the enforcement mechanisms consistently prioritize institutional interests and overall attempts at compliance over individual privacy rights.

The lack of robust enforcement at both federal and state levels underscores a fundamental tension in student privacy law: the balance between protecting individual privacy rights and maintaining institutional flexibility. This tension is exacerbated by rapid technological changes in education, which often outpace legal and regulatory frameworks.[308] It is increasingly clear that neither the parent-centric nor the school-centric approach fully addresses the multifaceted needs of students, parents, and educational institutions.

B. Competing Adult Priorities: Tensions Between the Parent-Centric and School-Centric Approaches

The parent-centric and school-centric paradigms, although distinct in their theoretical foundations and normative commitments, do not operate in isolation. Rather, they intersect and collide in ways that generate friction, inconsistencies, and even contradictions in student privacy

---

302 Press Release, Off. of the New York State Att'y Gen., *Attorney General James and NYSED Commissioner Rosa Secure $750,000 from College Board for Violating Students' Privacy* (Feb. 13, 2024), https://ag.ny.gov/press-release/2024/attorney-general-james-and-nysed-commissioner-rosa-secure-750000-college-board [https://perma.cc/UY7L-5WP2].

303 *See, e.g.*, S.B. 393, 88th Leg. § 26.016(e) (Tex. 2023); H.B. 1372, 2016 Sess. (N.H. 2016); La. Stat. Ann. § 17:3914 (2023).

304 *See* Zeide, *supra* note 47, at 343.

305 S.B. 393, 88th Leg. § 26.016(e) (Tex. 2023).

306 H.B. 1372, 2016 Sess. (N.H. 2016).

307 La. Stat. Ann. § 17:3914 (2023).

308 *See* Zeide, *supra* note 47, at 372–73.

governance.[309] This conflict extends beyond mere disagreements over data management practices, reflecting deeper societal debates about the nature of education, the boundaries of parental and institutional authority, and the balance between individual rights and collective goals in a democratic society.[310] As Justin Driver argues, schools have been "the single most significant site of constitutional interpretation within the nation's history," and the debates over student privacy law are no exception to this pattern.[311]

At their core, the parent-centric and school-centric approaches reflect fundamentally different perspectives on who should control student data, with rationales rooted in competing legal doctrines.[312] The parent-centric view draws strength from the constitutional doctrine of parental rights that affirm parents' fundamental right to direct their children's upbringing and education.[313] In contrast, the school-centric approach aligns with the doctrine of *in loco parentis* and the state's interest in educational institutions as a means to shape societal values and promote collective welfare.[314]

---

309 *See infra* notes 313–27 and accompanying text.

310 Justin Driver, *The Public School as the Preeminent Site of Constitutional Law*, 98 NEB. L. REV. 777, 781–82, 786 (2019) [hereinafter Driver, *Public School as Site*] (explaining that students and families must resist "not only the wishes of local educators but also the norms of their surrounding communities" to effect change); *see also* JUSTIN DRIVER, THE SCHOOLHOUSE GATE: PUBLIC EDUCATION, THE SUPREME COURT, AND THE BATTLE FOR THE AMERICAN MIND 7–28 (2018) [hereinafter DRIVER, SCHOOLHOUSE GATE] (discussing how schools are a microcosm for many of the issues facing society at large); WALTER LIPPMANN, AMERICAN INQUISITORS 22–23 (1928) (explaining that historically "the struggles for the control of the schools [have been] among the bitterest political struggles which . . . divide nations"); Brown v. Bd. of Educ., 347 U.S. 483, 493–94 (1954) (explaining how "education is perhaps the most important function of state and local governments . . . [and] is a right which must be made available to all on equal terms"); Hillary Rodham, *Children Under the Law*, 43 HARV. EDUC. REV. 487, 498 (1973) ("From the first confrontations between parents and the state, education has been the subject of continuous and often bitter struggles, primarily over the proper social role of education and the proper treatment of children within the schools.").

311 Driver, *Public School as Site*, *supra* note 310, at 780. *See generally* DRIVER, SCHOOLHOUSE GATE, *supra* note 310 (analyzing social change as enacted through litigation involving education); *see also* James E. Ryan, *The Supreme Court and Public Schools*, 86 VA. L. REV. 1335 (2000) (analyzing the Supreme Court's "public school[] jurisprudence"); Betsy Levin, *Educating Youth for Citizenship: The Conflict Between Authority and Individual Rights in the Public School*, 95 YALE L.J. 1647 (1986) (discussing the relationship children have with law and authority); Anne Proffitt Dupre, *Should Students Have Constitutional Rights? Keeping Order in the Public Schools*, 65 GEO. WASH. L. REV. 49 (1996) (discussing how different Supreme Court approaches to conceptualizing public schools affect school discipline and order); TYLL VAN GEEL, THE COURTS AND AMERICAN EDUCATION LAW (Phillip G. Altbach ed., 1987) (analyzing the contemporary transformation of American educational law).

312 *See supra* Part II.

313 *See* Meyer v. Nebraska, 262 U.S. 390, 396 (1923); Pierce v. Soc'y of Sisters, 268 U.S. 510, 510 (1925).

314 *Brown*, 347 U.S. at 493–94; Susan Stuart, *In Loco Parentis in the Public Schools: Abused, Confused, and in Need of Change*, 78 U. CIN. L. REV. 969 (2010).

This fundamental disagreement manifests in several key areas of tension. First, they conflict over the balance between individual and collective interests in education.[315] The parent-centric approach prioritizes the preferences and values of individual families, arguing that parents are best positioned to make decisions about their children's privacy and educational experiences[316] and seeking to protect family autonomy from state intrusion.[317] Conversely, the school-centric paradigm emphasizes the collective benefits of standardized educational practices and data-driven decision-making.[318]

Second, the two paradigms adopt conflicting approaches to consent and data governance. The parent-centric paradigm generally favors explicit, opt-in consent models for data collection and use, arguing that parents should have granular control over their children's information, as reflected in laws like the PPRA, which requires schools to obtain written parental consent before administering surveys on sensitive topics such as political affiliations, mental health, or sexual behavior.[319]

In contrast, the school-centric approach often relies on broader, opt-out consent models or institutional discretion in data handling.[320] This is exemplified by FERPA's provisions on "directory information," which allow schools to disclose certain student data without explicit parental consent.[321] Under this model, schools can share information such as a student's name, address, and academic honors unless a parent specifically requests that this information be withheld.[322]

Third, the paradigms clash over the role of educational technology and innovation. Parent-centric advocates often object to what they perceive as the surveillance overreach by educational institutions and the privacy-eroding influence of commercial education technology providers, calling for more robust consent requirements, data minimization principles, and parental oversight mechanisms.[323] School-centric proponents, in turn, argue for the importance of administrative flexibility, centralized coordination, and research and evaluation capacity to improve educational outcomes and equitable service delivery.[324]

---

315 *See supra* Part II.

316 Sonia Livingstone & Jasmina Byrne, *Challenges of Parental Responsibility in a Global Perspective*, *in* DIGITALLY CONNECTED: GLOBAL PERSPECTIVES ON YOUTH AND DIGITAL MEDIA 26, 28 (Urs Gasser & Sandra Cortesi eds., 2015).

317 *See* WESTIN, *supra* note 134, at 166.

318 *See* SONIA LIVINGSTONE ET AL., *supra* note 361, at 8–9.

319 *See* 20 U.S.C. § 232h(c)(2).

320 *See supra* Section II.B.

321 20 U.S.C. § 1232g(b)(1).

322 *See* 34 C.F.R. §§ 99.3, 99.31, 99.37 (2023).

323 Allen, *supra* note 352, at 752.

324 *See supra* Section II.B.

These conflicting perspectives create significant challenges for policymakers attempting to craft effective student privacy legislation. The tension between granular parental control and institutional flexibility makes it difficult to establish clear, universally acceptable standards for data collection and use in educational settings.[325] This tension often leads to legislative gridlock or the passage of laws that fail to adequately address the complexities of modern student privacy challenges.[326] When lawmakers attempt to satisfy both parent-centric and school-centric constituencies, the resulting legislation can be vague, internally inconsistent, or difficult to implement effectively.

The inBloom controversy illustrates how these competing paradigms can fuel legal and political conflicts that ultimately undermine student privacy interests. In 2013, inBloom, a nonprofit funded by the Gates Foundation, offered schools and districts a standardized database to collect and analyze information from various student information sources.[327] The inBloom system provided better security and privacy protections than many existing school data systems, including advanced encryption and more granular control over data sharing.[328] School administrators embraced these features, exercising their institutional discretion to adopt the system.[329]

However, the company's school-centric vision of data-driven personalized learning and cross-institutional data integration ran headlong into parent-centric concerns about consent, transparency, and commercialization.[330] Alarmist media reports stoked public outrage, and the company became a focal point for parents' fears about schools' surveillance of students, reliance on for-profit technology providers, and use of big data.[331] The inBloom controversy became a proxy for broader

---

325 *See, e.g.*, U.S. Dep't of Educ. Privacy Tech. Assistance Ctr., *supra* note 259, at 4–5.

326 *See, e.g.*, 76 Fed. Reg. 75,604, 75,607 (proposed Dec. 2, 2011).

327 Leonie Haimson, *Part IV of the InBloom Saga Through FOILed Emails: InBloom Is Born, Faces Increasing Controversy, and Dies*, N.Y.C. Pub. Sch. Parents (Jan. 4, 2016), https://nycpublicschoolparents.blogspot.com/2016/01/part-iv-of-inbloom-saga-through-foiled.html [https://perma.cc/VK4S-4ZCE].

328 *See* Monica Bulger, Patrick McCormick & Mikaela Pitcan, *The Legacy of inBloom*, 3, 6 (Data & Soc. Rsch. Inst., Working Paper No. 02.02.2017, 2017), https://datasociety.net/pubs/ecl/InBloom_feb_2017.pdf [https://perma.cc/XJ9N-ZPS8] (discussing the inBloom controversy).

329 *See id.* at 19–20.

330 *See id.* at 4, 13–19.

331 *Id.* at 15–16 ("In conjunction with negative press about corporate and government malfeasance and questionable use of data, inBloom was caught in a riptide of criticism about a wide range of education reform initiatives."); Tanya Roscorla, *Congress Urged to Update Student Data Privacy Law*, Ctr. for Digit. Educ. (June 27, 2014), http://www.centerdigitaled.com/news/congressurged-to-update-student-data-privacy-law.html [https://perma.cc/FPW9-44AD] (discussing general fears over schools using third-party cloud service providers); Khaliah Barnes, *Student Data Collection Is out of Control*, N.Y. Times: Room for Debate (Dec. 19, 2014, 12:33 PM), http://www.nytimes.com/roomfordebate/2014/09/24/protecting-student-privacy-in-online-learning/

debates over federal overreach in education, standardization, and the role of technology in schools.[332] Politicians, responding to parent-centric advocacy, began withdrawing support for the project.[333] Within a year of its launch, inBloom announced its closure, unable to reconcile its school-centric vision of data-driven education with the parent-centric demands for data control and privacy.[334]

The aftermath of the inBloom controversy exemplifies the problems stemming from the tension between these paradigms. The subsequent wave of state "student privacy" legislation addressed concerns about federal overreach and the nature of school reforms more than schools' information practices.[335] They tended to prioritize parental control and ideological battles over centralized reform to create a coherent, student-centered privacy framework.[336]

This pattern illustrates how the evolution of student privacy laws has often been reactive, shaped by high-profile scandals like inBloom rather than by a proactive, comprehensive understanding of students' privacy needs. The reactive approach has produced regulatory frameworks that focus almost exclusively on individual rights and procedural safeguards instead of clear, substantive boundaries outlining students' privacy needs.[337]

Contradictory requirements and coverage gaps created compliance quagmires for educational institutions, uneven protections for students, and a fractured normative foundation for digital education governance.[338] This misalignment led to regulations that conflicted with other educational mandates and did not protect student privacy in an effective manner. For example, state laws that required parental consent before sharing information prevented students from being nominated for scholarships.[339] Other laws that required parental consent before video recording interfered with schools' ability to provide accommodations to disabled students as required by the Individuals with Disabilities Education Act.[340] Many of these laws have been amended multiple times, and some are not enforced at all.[341]

---

student-data-collection-is-out-of-control [https://perma.cc/7KBV-576B] (discussing a lawsuit against the Department of Education for allowing companies to access student data).

332 *See* Bulger et al., *supra* note 328, at 15–16, 25–28; Roscorla, *supra* note 331.

333 Natasha Singer, *InBloom Student Data Repository to Close*, N.Y. TIMES: BITS (Apr. 21, 2014, 1:21 PM), http://bits.blogs.nytimes.com/2014/04/21/inbloom-student-data-repository-to-close/ [https://perma.cc/PZ92-R26R].

334 *Id.*

335 Vance & Waughn, *supra* note 150, at 535–36.

336 *See* discussion *supra* Sections III.A.3–.4.

337 *See supra* Part II.

338 Vance & Waughn, *supra* note 150, at 535–56.

339 *Id.*

340 Individuals with Disabilities Education Act, 20 U.S.C. §§ 1400–1482 (2006); Vance & Waughn, *supra* note 150, at 537–38.

341 Vance & Waughn, *supra* note 150, at 536–47.

The inBloom case serves as a cautionary tale about the consequences of failing to recognize or reconcile parent-centric and school-centric approaches to student privacy. It further demonstrates how the tension between paradigms, especially when inflamed by misunderstandings and broader educational debates, can lead innovative educational initiatives to fail, spark reactive and problematic legislation, and ultimately fail to serve the best interests of students. The controversy underscores the need for a new approach to student privacy that balances the legitimate concerns of parents with the data needs of educational institutions while simultaneously prioritizing the educational and privacy interests of students themselves.

The tensions between the parent-centric and school-centric paradigms reveal fundamental problems in how student privacy has been conceptualized and regulated. Neither approach adequately centers students themselves nor provides a coherent theoretical foundation for understanding privacy's role in education. Part III examines these limitations in detail, critiquing each paradigm individually before identifying their shared shortcomings. This critical assessment will demonstrate why a new approach is needed—one that recognizes students as primary stakeholders with evolving capabilities and distinct privacy interests as learners in increasingly data-rich educational environments.

III. Deconstructing Dominant Paradigms: Critiquing Parent-Centric and School-Centric Approaches

The parent-centric and school-centric paradigms not only fail to adequately protect student privacy but are built on fundamentally flawed theoretical foundations that marginalize students' own interests. This Part examines how these dominant approaches to student privacy governance systematically neglect students as evolving rights-bearers with distinct privacy interests. Neither framework adequately theorizes privacy's role in education nor accounts for students' developmental trajectory.

Despite originating from legitimate concerns about parental rights and institutional efficiency, both frameworks lack coherent conceptual and normative foundations for privacy protection. The following analysis exposes their conceptual limitations, the tensions between their underlying values and commitments, and their inability to address the complex realities of privacy in contemporary educational institutions.

This critique demonstrates how the parent-centric paradigm imposes unrealistic burdens on parental oversight, treats childhood as a static category rather than a developmental process, and ultimately subordinates students' privacy interests and autonomy to parental prerogatives.[342] The school-centric approach, meanwhile, grants educa-

342 *See infra* Section III.A.

tional institutions expansive discretion without adequate safeguards, neglects the critical importance of intellectual privacy for learning, enables practices that amplify existing inequities, and lacks meaningful transparency and accountability mechanisms.[343]

Crucially, both paradigms share fundamental shortcomings: They fail to protect *students'* privacy from parents and schools themselves; they focus on students as children requiring protection rather than as learners engaged in intellectual development; and they overlook privacy's essential role in the educational process. Although each framework reflects important values—parental rights and institutional expertise, respectively—their conceptual architectures prove fundamentally inadequate for protecting student privacy in contemporary educational environments.[344]

A. Parental Control and Its Limitations

The parent-centric paradigm frames privacy as an extension of parental authority, emphasizing control and consent mechanisms to protect students from external threats.[345] This approach positions parents as the principal decision-makers and guardians of not only their children's information privacy but also their moral upbringing. It reflects principles embedded in both the constitutional and literal concepts of "family privacy."[346] Although these serve important functions in protecting family independence from state overreach,[347] they fail to account for the evolving and complex nature of privacy in contemporary educational contexts.

Before proceeding to critique, it is crucial to acknowledge the legitimate interests that underpin the parent-centric approach. Parents, as primary caregivers and guardians, have a valid stake in their children's well-being, education, and development. American law recognizes this parental interest as a fundamental right.[348] The desire to protect children from harm, guide their moral and intellectual growth,

---

343 *See infra* Section III.B.

344 *See infra* Sections III.A.3, III.B.2.

345 *See supra* Section II.A.

346 Smith v. Org. of Foster Fams. for Equal. & Reform, 431 U.S. 816, 845 (1977) (acknowledging the right of "family privacy" recognized in constitutional law and stemming from "intrinsic human rights"). The Supreme Court has recognized parents' rights as being grounded in the concept of "family privacy." *Id.* For over a century, the Court has recognized parents' role as primary decision-makers in their children's moral and intellectual development, setting a precedent for parental authority in educational matters. Meyer v. Nebraska, 262 U.S. 390, 400, 403 (1923) (striking down a state law prohibiting foreign language instruction); Pierce v. Soc'y of Sisters, 268 U.S. 510, 534–35 (1925) (striking down a state law requiring attendance at nonparochial school).

347 *See Meyer*, 262 U.S. at 403; *Pierce*, 268 U.S. at 534–36.

348 *See Meyer*, 262 U.S. at 392–403; *Pierce*, 268 U.S. at 530, 534.

and maintain familial bonds are valid considerations in education and privacy.

This Section examines three fundamental limitations of the parent-centric paradigm: its unrealistic expectations for parental privacy management in complex digital environments, its static conception of childhood that disregards students' evolving capabilities, and its subordination of students' own privacy interests to parental control. Each limitation reveals how this paradigm, despite its aim to protect children, ultimately fails to serve students' educational and developmental needs.

1. Unrealistic Burden of Privacy Management

The paradigm's reliance on parental oversight reflects fundamental limitations in its conceptualization of information governance. The volume of educational technologies, complexity of privacy policies, and technical nature of data practices overwhelm even the most dedicated parents, rendering consent a procedural formality rather than meaningful protection.

This consent-based framework places unrealistic burdens on parents given the sheer volume of information and the technical complexity of privacy policies.[349] Digital literacy often correlates with factors such as age, education level, and socioeconomic status, creating patterns of differential privacy protection that reflect and reproduce broader social inequities.[350]

2. Disregard for Students' Evolving Capabilities and Autonomy

The parent-centric paradigm also reflects a static conception of childhood that fails to engage with contemporary understandings of student development. This manifests in provisions that give parents access to or mandate disclosure of information that children might prefer to be private, such as internet browsing habits or actions that reveal they are questioning their gender identity.[351] As Anita Allen aptly observed, the parental consent provision in FERPA "purports to protect children's informational privacy by investing parents with the right to bar certain disclosures of information to third parties," an approach that is both paternalistic and authoritarian.[352] This paternalistic approach neglects a growing body of research demonstrating that independence

---

349 Colleen McClain, Michelle Faverio, Monica Anderson & Eugenie Park, Pew Rsch. Ctr., How Americans View Data Privacy (2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/ [https://perma.cc/VD6N-5M5R] (noting only thirty-seven percent of United States adults feel overwhelmed by managing their online privacy).

350 Danhua Peng & Zhonggen Yu, *A Literature Review of Digital Literacy over Two Decades*, 2022 Hindawi Educ. Rsch. Int'l, May 17, 2022, at 1, 3.

351 Warren & Markey, *supra* note 35, at 5–7; Laird, et al., *supra* note 35, at 21.

352 *See* Anita L. Allen, *Minor Distractions: Children, Privacy and E-Commerce*, 38 Hous. L. Rev. 751, 755 (2002).

from parents plays a pivotal role in fostering healthy identity formation and autonomy.[353]

At its core, the parent-centric paradigm treats children as extensions of parental authority rather than as individuals with their own developmental trajectory. It risks stifling the developmental processes essential for privacy self-management, which helps students navigate adolescence and prepares them for autonomous adulthood.[354]

Insights from developmental psychology and children's rights movements challenge traditional concepts of childhood and its regulation, emphasizing the importance of permitting even young children to have some degree of control over their lives.[355] In *The New Law of the Child*, for example, Anne C. Dailey and Laura A. Rosenbury argue that children have distinct privacy, free expression, identity, and reputational interests worthy of consideration, and their interests are not just derivatives of parental prerogatives.[356]

Internationally, children have rights separate from their parents, including the rights to survival, development, protection, and participation.[357] These rights extend to digital environments, as highlighted by the United Nations Convention on the Rights of the Child ("UNCRC"), which includes rights to participation, education, play, and family life online.[358] The UNCRC's General Comment No. 25 further advocates for legislative and policy measures to safeguard children's digital rights by enhancing digital literacy, creating safe online spaces for children, and supporting children's rights to education, participation, and freedom of expression.[359]

Although the United States has not ratified the UNCRC,[360] this global perspective offers valuable insights for rethinking the balance between parental control and children's rights concerning student privacy laws. For example, research shows that digital technology provides opportunities as well as risks.[361] It facilitates self-directed learning and

---

353 *See* Shmueli & Blecher-Prigat, *supra* note 131, at 763; *see also, e.g.*, Allen, *supra* note 352, at 772.

354 *See* Shmueli & Blecher-Prigat, *supra* note 131, at 763; *see, e.g.*, Allen, *supra* note 352, at 772.

355 *See, e.g.*, Anne C. Dailey & Laura A. Rosenbury, *The New Law of the Child*, 127 YALE L.J. 1448, 1510 (2018).

356 *Id.* ("Children have independent interests—not derivative of third-party interests or rights—in developing and maintaining relationships with nonparental figures, such as other relatives, foster parents, stepparents, siblings, and other children.").

357 U.N. Convention on the Rights of the Child arts. 6, 13, 31, Nov. 20, 1989, 1577 U.N.T.S. 3.

358 U.N. Comm. on the Rights of the Child, *General Comment No. 25 on Children's Rights in Relation to the Digital Environment*, U.N. Doc. CRC/C/GC/25, ¶ 16 (Mar. 2, 2021).

359 *See id.* ¶¶ 9, 11, 16, 56.

360 *Ratification Status for CRC - Convention on the Rights of the Child*, U.N. HUM. RTS. TREATY BODIES, https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?Treaty=CRC [https://perma.cc/36HW-TDYH].

361 *See, e.g.*, SONIA LIVINGSTONE, DANIEL KARDEFELT-WINTHER & MARIUM SAEED, GLOBAL KIDS ONLINE COMPARATIVE REPORT 6–7 (2019), https://www.unicef-irc.org/publications/1059-global-kids-online-comparative-report.html [https://perma.cc/RFH9-TMPA].

offers support that children may lack at home or school.[362] Digital spaces can be invaluable tools that can help youth address their needs in ways that their parents may be ill-equipped to address.[363] In light of this new understanding of children's rights outside and within digital spaces, scholars must reevaluate existing legal frameworks to better align with the realities of children's lives and developmental needs.

3. Subordination of Students' Interests to Parental Control

The parent-centric paradigm often subordinates students' interests to parental prerogatives. Student privacy laws that rely on parental consent reflect an outdated model of family structure and dynamics, assuming a unity of interest between parents and their children—or simply subordinate children's interests to those of their parents.[364] This assumption becomes increasingly problematic as students mature and develop distinct privacy needs.[365] It fails to recognize the potential for intrafamilial privacy conflicts and the need, at times, to protect children's privacy from, rather than through, parental authority.[366]

Feminist scholarship has exposed how "privacy" has been used to protect some men from the consequences of abusing family members.[367] Although outdated notions of the family unit being paternal "property" have faded,[368] the legal framework surrounding family privacy still places children under parental control without consideration for cases in which a parent's intentions may conflict with a child's best interests.[369] Further, students may have valid reasons to keep medical, disciplinary, or counseling information private from their parents.[370] Parental rights bills that require teachers to "out" students' sexual or gender identities to their parents[371] put youth with unaccepting parents at risk of eviction

362 *See, e.g.*, DANAH BOYD, IT'S COMPLICATED: THE SOCIAL LIVES OF NETWORKED TEENS 176–98 (2014).

363 *See supra* notes 361–62 and accompanying text.

364 Shmueli & Blecher-Prigat, *supra* note 131, at 776.

365 *See* Anne C. Dailey & Laura Rosenbury, *The New Parental Rights*, 71 DUKE L.J. 75, 83 (2021).

366 *See id.*

367 *See, e.g.*, Riva B. Siegel, "*The Rule of Love": Wife Beating as Prerogative and Privacy*, 105 YALE L.J. 2117, 2152–53 (1996) (describing how courts used the concept of marital privacy to effectively immunize wife beaters from prosecution).

368 *See* Shmueli & Blecher-Prigat, *supra* note 131, at 768 n.39; Barbara Bennett Woodhouse, *Hatching the Egg: A Child-Centered Perspective on Parents' Rights*, 14 CARDOZO L. REV. 1747, 1756 (1993).

369 *See, e.g.*, Dailey & Rosenbury, *supra* note 365, at 92; Barbara Bennett Woodhouse, *Who Owns the Child:* Meyer *and* Pierce *and the Child as Property*, 33 WM. & MARY L. REV. 995, 1113–14 (1991) (discussing the focus on parental control in jurisprudence concerning parental rights).

370 *See, e.g.*, Klein & Sarit, *supra* note 8.

371 *See, e.g.*, H.B. 1522, 68th Legis. Assemb. (N.D. 2023); S.F. 496, 90th Gen. Assemb. § 14 (Iowa 2023); H.B. 1608, 123rd Gen. Assemb., 1st Sess. § 4 (Ind. 2023); S.B. 49, 2023 Sess. § 115C-76.45(a)(5) (N.C. 2023); S.B. 184, 2022 Leg., Reg. Sess. § 5 (Ala. 2022).

or abuse.[372] Moreover, the parent-centric paradigm can stifle children's intellectual exploration and limit access to beneficial resources and supportive communities by permitting parental access to students' digital communication and browsing histories.[373]

In summary, the parent-centric paradigm's focus on parental authority negates students' privacy rights and evolving capacity for autonomy and independence. Imposing parental preferences can undermine children's agency, intellectual freedom, and access to resources that support their welfare.

B. Institutional Power and its Consequences

The school-centric paradigm conceptualizes privacy as an institutional responsibility, emphasizing compliance and administrative efficiency over the intellectual and developmental needs of students.[374] It draws strength from the doctrine of *in loco parentis*, a legal principle that positions schools as acting in the place of parents during school hours, granting them significant authority over students. The school-centric paradigm also reflects the broader state interest in educational equity.[375]

Again, it is crucial to acknowledge the legitimate interests and practical considerations that underpin the school-centric approach.[376] From a practical standpoint, the school-centric approach addresses the logistical challenges of data management in educational settings. Requiring teachers to obtain individual parental consent for every use of data by schools would overwhelm schools, hinder collective instruction,[377] and undermine the idea of education as a public good.[378]

A fundamental flaw in this paradigm, however, lies in its implicit assumption that the greatest risks to student privacy come from external threats, rather than from within the educational system itself.[379] This misplaced focus is evident in regulations, such as FERPA, that primarily address data disclosure to outside parties while paying insufficient attention to internal data practices and potential misuses.[380] These limitations

---

372 Jonah DeChants, Myeshia N. Price, Amy E. Green & Carrie Davis, The Trevor Project, Homelessness and Housing Instability Among LGBTQ Youth 4, 5 (2021), https://www.thetrevorproject.org/wp-content/uploads/2022/02/Trevor-Project-Homelessness-Report.pdf [https://perma.cc/8BH8-UVY5].

373 Deborah Lupton & Ben Williamson, *The Datafied Child: The Dataveillance of Children and Implications for Their Rights*, 19 New media & Soc'y 780, 788–89 (2017).

374 *See supra* Section II.B.

375 347 U.S. 483 (1954); *see id.* at 493–94.

376 *See* Zeide, *supra* note 47, at 384–86.

377 *Id.* at 384.

378 *See id.* at 385–86.

379 *See id.* at 375–76.

380 *See, e.g.*, 20 U.S.C. § 1232g.

manifest in four critical ways: the expansive institutional discretion that lacks adequate safeguards, the neglect of students' intellectual privacy essential for learning, the amplification of existing biases affecting marginalized populations, and the absence of meaningful due process mechanisms for contesting data-driven decisions. Together, these shortcomings demonstrate how educators' priorities systematically override student interests in current privacy frameworks.

1. Expansive Institutional Discretion in Data Governance

The school-centric paradigm grants educational institutions expansive latitude in managing student data without clear guidelines or sufficient accountability.[381] This approach is manifest in FERPA's broad exceptions, such as the school official and audit exceptions and the directory information exclusion.[382] This flexibility, although potentially beneficial for institutional operations, can lead to inconsistent interpretations and applications of the law, potentially exposing student data to unnecessary access or misuse.

Furthermore, educators, like parents, frequently struggle to oversee the complex information flows in modern education and effectively monitor vendors' information and privacy practices. In Virginia, for example, the Fairfax County Public School District has had multiple incidents in which school administrators mistakenly shared thousands of sensitive records—including information about students' alleged sexual assault complaints and suicidal ideation—with parents.[383] The lack of clear, consistent standards for data use and disclosure creates an environment where student information may be shared more widely than necessary, potentially exposing sensitive data to unauthorized access or misuse.

2. Neglect of Students' Intellectual Privacy and Autonomy

The school-centric paradigm, in its focus on institutional prerogatives, often neglects the critical importance of intellectual privacy and autonomy for student development. By constructing student privacy primarily as a matter of legal compliance rather than as a vital condition for learning and growth, it fails to recognize the chilling effects

---

381 *See* Zeide, *supra* note 47, at 361–62.

382 *See supra* Section II.B.3.

383 Linda Jacobson, *Exclusive: Virginia's Fairfax Schools Expose Thousands of Sensitive Student Records*, THE 74 (Nov. 1, 2023), https://www.the74million.org/article/exclusive-virginias-fairfax-schools-expose-thousands-of-sensitive-student-records/ [https://perma.cc/S9PW-L5JV]; Michelle C. Reid, *Message from the Superintendent: Update on FERPA Disclosure*, FAIRFAX CNTY. PUB. SCH. (Dec. 12, 2023), https://www.fcps.edu/news/update-ferpa-disclosure [https://perma.cc/D3G7-84L4].

that pervasive monitoring, dataveillance, and algorithmic assessment practices can have on students' willingness to explore ideas, express themselves authentically, and cultivate their identities.[384]

This omission ignores the psychological, pedagogical, and material harms inflicted on students by extensive school data collection and surveillance.[385] Extensive surveillance practices can have chilling effects on student expression and exploration.[386] Recording class sessions may discourage students from participating honestly or articulating what they perceive as unpopular views.[387] Constant monitoring of students during digital instruction or remote exams can increase their anxiety levels, which negatively impacts academic performance.[388] Similarly, schools monitoring students' internet browsing and social media can chill intellectual exploration.[389] Researchers such as Alan Rubel and Kyle M.L. Jones demonstrate that extensive school surveillance reduces students' willingness to seek help, trust educators, and engage civically.[390]

3. Bias Amplification and Institutional Power

The school-centric paradigm's theoretical architecture enables and reinforces institutional power asymmetries that systematically disadvantage certain student populations. Students receiving disability accommodations or social welfare benefits must provide extensive documentation, which increases their vulnerability to privacy intrusion.[391] Schools with sizeable nonwhite student populations are disproportionately subject to invasive surveillance technologies.[392] This increased scrutiny can lead to criminalization for minor infractions that might otherwise be addressed through internal school disciplinary processes.[393]

---

384 *See infra* notes 386–90 and accompanying text.

385 *See generally*, Elana Zeide & Helen Nissenbaum, *Learner Privacy in MOOCs and Virtual Education*, 16 THEORY & RES. EDUC. 280 (2018) (discussing the harm to children's educational experiences caused by overuse of technology in the classroom).

386 LAIRD ET AL., *supra* note 35, at 22.

387 *See* RICHARDS, *supra* note 39, at 95–122; Jon W. Penney, *Understanding Chilling Effects*, 106 MINN. L. REV. 1451, 1452–55 (2022); Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 490–92, 501–06 (2015).

388 Elana Zeide, Credentialing Effects: Psychological Implications of Ubiquitous Capture and Constant Assessment, Remarks at the Privacy Law Scholars Conference (June 3, 2016) (draft on file with author).

389 LAIRD ET AL., *supra* note 35, at 4, 22.

390 *See generally, e.g.*, Alan Rubel & Kyle M.L. Jones, *Student Privacy in Learning Analytics: An Information Ethics Perspective*, 32 INFO. SOC'Y 143, 147 (2016) (critiquing surveillance in schools); Alan Rubel & Kyle M.L. Jones, *The Temptation of Data-Enabled Surveillance*, COMMC'NS. ASS'N COMPUTING MACH., Apr. 2020, at 22, 22 (same).

391 Fanna Gamal, *The Private Life of Education*, 75 STAN. L. REV. 1315, 1348–54 (2023).

392 *Id.* at 1335–37.

393 *See, e.g.*, Nance, *supra* note 1, at 780–81.

FERPA's limited scope of protection, which excludes medical records, illustrates the potential for school misuse of student data.[394] The loophole allows schools to disclose students' sensitive health information, such as visits to women's health clinics, to their parents without student consent.[395] Even more alarmingly, universities can disclose student-plaintiffs' mental health records against them in legal proceedings.[396] Such practices not only violate student privacy but also potentially deter students from seeking necessary medical or mental health care.[397]

The trust placed in educational institutions under this paradigm sometimes extends to problematic interactions with law enforcement, often to the detriment of marginalized communities.[398] A striking example of this occurred in Pasco County, Florida, where the school district shared student information, including grades and disciplinary records, with local law enforcement to create a predictive policing model to "label schoolchildren potential criminals."[399] The police visited and harassed these students at home.[400]

At the core of this problem lies the creation and maintenance of biased data in student records. Najarian Peter's research provides a compelling illustration of this issue, highlighting how Black students' records often reflect subjective assessments by educators that are discriminatorily slanted against them.[401] This bias occurs in the very process of observing, assessing, and judging students—tasks performed by both human teachers and increasingly by technological tools.[402] The result is a corpus of student data tainted by racial and other biases, which then forms the basis for future educational decisions and opportunities.[403]

---

394 Lynn M. Daggett, *The Myth of Student Medical Privacy*, 14 HARV. L. & POL'Y REV. 467, 480–82 (2019).

395 Lynn M. Daggett, *Female Student Patient "Privacy" at Campus Health Clinics: Realities and Consequences*, 50 U. BALT. L. REV. 77, 80–81 (2020).

396 Marin Dell, *The Campus Litigation Privacy Act of 2015: In Support of a FERPA Amendment Closing the Privacy Gap for University Student Litigants' Counseling Records*, 19 APPALACHIAN J.L. 187, 187–88 (2019).

397 *See* Daggett, *supra* note 395, at 144–45.

398 *See, e.g.*, Kathleen McGrory & Neil Bedi, *Pasco's Sheriff Created a Futuristic Program to Stop Crime Before It Happens. It Monitors and Harasses Families Across the Country*, TAMPA BAY TIMES (Sept. 3, 2020), https://projects.tampabay.com/projects/2020/investigations/police-pasco-sheriff-targeted/intelligence-led-policing/ [https://perma.cc/8A94-5UJB].

399 *Id.*

400 *Id.*

401 Najarian R. Peters, *The Golem in the Machine: FERPA, Dirty Data, and Digital Distortion in the Education Record*, 78 WASH. & LEE L. REV. 1991, 1995, 2001 (2021); *see* Gamal, *supra* note 391, at 1335–36.

402 *See* Peters, *supra* note 401, at 1995; Zeide, *supra* note 40, at 92–93.

403 *See* Gamal, *supra* note 391, at 1335–36.

The school-centric paradigm exacerbates this issue by granting educational institutions significant discretion in adopting new technologies without requiring due diligence to evaluate their accuracy, efficacy, and impact on students' privacy and educational equity.[404] This has led to the widespread implementation of systems that can perpetuate and amplify existing biases, creating a self-reinforcing cycle of disadvantage for already marginalized students.[405] For example, early alert systems that identify "at-risk" students can create self-fulfilling prophecies, potentially reinforcing existing biases and limiting student opportunities.[406] Similarly, advisory systems offering personalized recommendations based on educational records can discourage students from pursuing their desired career paths.[407]

These algorithmic profiling systems often reflect embedded biases.[408] Online proctoring software, for instance, has been found to disproportionately flag neurodivergent students for "suspicious" behavior during remote exams, simply because they do not conform to typical behavioral patterns.[409] Cheating detection tools have similarly been criticized for disproportionately flagging nonnative English speakers.[410] Schools lack robust protocols for students to contest algorithmic inferences,[411] leaving students at the mercy of opaque systems.[412] This not only subjects students to faulty technology but also perpetuates existing inequities.

4. Insufficient Mechanisms for Transparency and Redress

While the previous Section addressed the excessive authority granted to schools through the regulatory framework, this Section focuses on the procedural barriers that prevent students and families from effectively exercising their theoretical rights or contesting privacy

---

404 *See* Hannah Quay-de la Vallee & Natasha Duarte, Algorithmic Systems in Education: Incorporating Equity and Fairness When Using Student Data, Ctr. for Democracy & Tech. 20–21 (Aug. 2019), https://cdt.org/wp-content/uploads/2019/08/2019-08-08-Digital-Decision-making-Brief-FINAL.pdf [https://perma.cc/SQA5-X3VT].

405 *See id.* at 4–6, 12–15, 19–21; Zeide, *supra* note 40, at 92–93.

406 Ekowo & Palmer, *supra* note 49, at 13–15.

407 *See* Alan Rubel & Kyle Jones, *Data Analytics in Higher Education: Key Concerns and Open Questions*, 11 U. St. Thomas J.L. & Pub. Pol'y 25, 32 (2017); Ekowo & Palmer, *supra* note 49, at 14–15.

408 *See* Zeide, *supra* note 40, at 92–93.

409 *Id.* at 92–93, 123–24.

410 *See* Weixin Liang, Mert Yuksekgonul, Yining Mao, Eric Wu & James Zou, *GPT Detectors Are Biased Against Non-Native English Writers*, CellPress Open Access: Patterns, July 14, 2023, at 1, https://www.cell.com/action/showPdf?pii=S2666-3899%2823%2900130-7 [https://perma.cc/SLG2-UQ4A].

411 Zeide, *supra* note 40, at 102.

412 *Id.* at 102–04; Liang et al., *supra* note 410, at 1.

violations. The problem extends beyond the grant of discretion to the absence of meaningful checks on that power. Although many states mandate transparency through parental notifications,[413] these notices typically contain vague legal jargon that provides little meaningful information.[414] Schools often lack formal protocols for students to contest algorithmic inferences,[415] leaving them at the mercy of opaque systems that often flag innocuous activity as possible academic misconduct.[416]

FERPA theoretically gives parents and students the power to inspect and challenge information in their records,[417] but the complexity of modern data systems undermines this right's practical utility.[418] Today's student records have evolved beyond simple paper files into extensive digital dossiers, with information dispersed across multiple systems that parents and students struggle to navigate.[419] The barriers particularly impact marginalized communities.[420] Families of color, for example, often lack the social capital to participate meaningfully in their children's education.[421] When parents or students seek to challenge inaccurate or misleading information in school records, FERPA requires schools to hold formal hearings.[422] As Gamal notes, however, these hearings offer little meaningful recourse because the school administrators who serve as arbiters are often the same officials—or their colleagues—who created the contested records, leaving families without access to truly independent review.[423] These barriers are particularly pronounced for marginalized communities who may lack the resources, knowledge, or social capital to navigate complex administrative procedures.

The school-centric paradigm's flaws—expansive institutional discretion, neglect of intellectual privacy, bias amplification, and inadequate accountability—create an environment where student privacy interests are subordinated to administrative priorities. While these

---

413 *See, e.g.*, OKLA. STAT. tit. 70 § 3-168 (2022); *see also* COLO. REV. STAT. § 22-16-107 (2016).

414 *See generally* Zeide, *supra* note 40 (discussing problems with due process concerning online proctoring systems).

415 *Id.* at 104–15.

416 *Id.* at 100–03.

417 *Id.* at 107.

418 *Id.* at 114–15.

419 *See, e.g.*, Drew Keller, *FERPA Records Requests Reveal Little*, RICE THRESHER (Jan. 28, 2015), http://www.ricethresher.org/news/ferpa-records-requests-reveal-little/article_41fcdeb4-a764-11e4-b6c5-eb934024235d.html [https://perma.cc/C8FC-UHEK]; Kevin J. Cimino, *Student Education Records: Understanding FERPA and Its Intricacies in Order to Obtain Records from Educational Institutions Efficiently*, W. VA. LAW., Spring 2020, at 37, 39 (discussing the difficulty of locating and requesting student records).

420 *See, e.g.,* LaToya Baldwin Clark, *The Problem with Participation*, 9 MOD. AM. 20, 20–27 (2013).

421 *See id.*

422 *See* Gamal, *supra* note 391, at 1319.

423 *Id.* at 1339.

limitations differ from those of the parent-centric approach, they share a fundamental characteristic: Both paradigms fail to recognize students as primary stakeholders with distinct privacy needs essential to their learning and development. The following Section examines these shared shortcomings and explains why they necessitate a fundamental reconceptualization of student privacy.

C. Shared Shortcomings and the Need for a Student-Centric Approach

The critique of the parent-centric and school-centric paradigms reveals not only their specific limitations but their shared misconception about privacy's role in education. Both frameworks subordinate students' interests to adult priorities—whether parental authority or institutional efficiency—and fail to recognize that students may need privacy from these very stakeholders. This reflects a narrow, individualistic conception of privacy that fails to account for its deeply relational and contextual nature in educational settings.

The preceding analysis reveals three critical flaws that prevent the paradigms from addressing the privacy needs of learners in digital environments. First, both paradigms marginalize students as agents in their own right. Second, they impose static frameworks on the fluid reality of childhood and adolescence. Third, they fail to recognize privacy's constitutive role in education itself.

Compounding these conceptual limitations is a dearth of attention to the changing technological realities of education in the digital age. Both the parent-centric and school-centric approaches remain tethered to anachronistic assumptions about the nature of information flow and control that no longer hold in an era of pervasive data collection, algorithmic decision-making, and embedded learning technologies.[424] They struggle to adapt to a world where the boundaries between home and school, public and private, and online and offline are increasingly blurred, and where traditional notions of individual consent and institutional custody are strained to the breaking point. The following Sections examine each of these shared shortcomings in depth, revealing how they manifest across both paradigms and creating a foundation for the student-centric approach proposed in Part IV.

1. Failure to Center Students as Primary Stakeholders and Marginalizing Students' Privacy Interests

Both paradigms marginalize students' privacy interests, treating them primarily as objects of protection rather than as active agents

---

424 *See supra* Parts I–II; Zeide, *supra* note 47, at 345–53.

with evolving needs and rights.[425] This shared blind spot stems from entrenched notions of students as passive recipients of education rather than active participants in their own learning and development.[426]

The parent-centric paradigm subordinates students' privacy to parental authority, framing students as extensions of the family unit whose privacy rights are exercised through parental control.[427] Conversely, the school-centric paradigm subsumes student privacy under institutional priorities, often emphasizing compliance or efficiency over individual agency.[428] Neither approach adequately recognizes students as the primary stakeholders in privacy governance, resulting in their shared failure to adapt to students' developmental trajectories or to account for privacy's critical role in intellectual and personal growth.

This marginalization is compounded by the increasing use of surveillance technologies in schools.[429] These tools are often implemented to enhance safety or efficiency; however, they frequently undermine students' intellectual privacy—the freedom to explore ideas and develop identities without fear of external judgment or interference.[430] Parental monitoring technologies exacerbate this issue[431] with features that allow parents to track their children's digital activities in ways that may stifle intellectual curiosity or discourage independent exploration.[432] For example, monitoring students' search histories or online communications can deter them from engaging with ideas that challenge familial expectations, hindering both personal and intellectual development.[433]

The failure to center students as primary stakeholders also prevents privacy governance from fostering critical developmental skills. Students are rarely given opportunities to participate in privacy-related decision-making or to develop the competencies necessary for navigating complex digital environments.[434] As scholars like Shmueli and Blecher-Prigat argue, recognizing children's evolving capacities and granting them autonomy rights in stages are each essential for their growth as self-determined individuals.[435] Without such opportunities, students remain passive recipients of privacy protections, unprepared for the challenges they will face as adults in datafied societies.

---

425 *See supra* Sections III.A.3, .B.2.

426 *See supra* Sections III.A.3, .B.2.

427 *See supra* Section III.A.3.

428 *See supra* Section III.B.2.

429 *See supra* Section I.A.

430 *See supra* Section III.B.2.

431 *See supra* Section I.A.

432 *See supra* Section III.A.

433 *See supra* Section III.A.

434 *See* Shmueli & Blecher-Prigat, *supra* note 131, at 782–85.

435 *See id.* at 787–95.

Similarly, the school-centric model prioritizes institutional interests in data collection and analysis over students' autonomy and privacy rights.[436] This approach might offer controlled opportunities for engagement with technology, but it often fails to prepare students for navigating less restricted environments.[437] Privacy, as Neil Richards argues, is essential for the development of autonomous individuals capable of exercising freedom of thought and expression.[438] Yet both paradigms neglect this foundational role of privacy.[439]

2. Conflating Children with Learners

Both paradigms frequently conflate students with children, overlooking the evolving capacities and needs of learners across developmental stages.[440] This conflation reflects a narrow understanding of "student privacy" as synonymous with child protection, focusing on shielding youth from perceived external threats rather than fostering intellectual growth and autonomy.

The parent-centric paradigm portrays students as impressionable youth in need of parental oversight, emphasizing threats to familial privacy or moral development.[441] Similarly, the school-centric model relies on a paternalistic framework, viewing schools as guardians against online risks, commercial exploitation, or emotional harm.[442] This protective stance prioritizes safeguarding over empowering students as active participants in their own privacy decisions. The result is an implicit focus on students' perceived vulnerabilities as children rather than their broader identity as learners. For instance, controversies over comprehensive sex education often reflect concerns about children's innocence rather than a commitment to equipping learners with critical knowledge.[443] Similarly, the focus on protecting students from targeted marketing using their data emphasizes vulnerabilities of youth while neglecting privacy's role in intellectual exploration and personal growth.[444]

---

436 *See id.* (explaining how children's autonomy over their privacy interests should be considered when determining how to best protect children's privacy in "the contemporary digital era").

437 *See supra* Section III.B.

438 *See* RICHARDS, *supra* note 39, at 95–122.

439 *Id.* at 318.

440 *See supra* Sections III.A.2, .B.2.

441 *See supra* Section III.A.

442 *See supra* Section III.B.

443 *See, e.g.*, Kate Payne, *Florida Officials Pressure Schools to Roll Back Sex Ed Lessons on Contraception and Consent*, ASSOCIATED PRESS (Sept. 23, 2024, 6:14 PM), https://apnews.com/article/florida-sex-education-curriculum-5b1a46f5a73e3122f4815cf1d439aef0 [https://perma.cc/B6FE-2YNS].

444 *See supra* Section III.B.

This misalignment perpetuates a narrow, compliance-driven understanding of student privacy. By prioritizing protection over participation, these paradigms fail to cultivate environments where students can develop the intellectual and ethical skills essential for navigating privacy challenges. As a result, both approaches neglect the collective and developmental dimensions of privacy that enable expansive learning and self-discovery.

3. Neglecting Privacy's Constitutive Role in Education

Perhaps most critically, both paradigms overlook privacy's crucial role in core educational values. They fail to recognize how privacy functions not just as a protective measure but as an essential component of the learning process itself.[445] Neither approach adequately protects what Neil Richards terms "intellectual privacy"—the freedom to explore ideas and develop new thoughts without constant surveillance or judgment.[446]

This neglect undermines education's fundamental purpose as a space for intellectual growth. Privacy creates the conditions necessary for intellectual exploration, creative expression, and the development of critical thinking skills—all fundamental to the educational mission.[447] Yet current frameworks provide insufficient space for maturing students to engage in these crucial processes of identity formation and intellectual exploration.[448] These shortcomings not only leave students vulnerable to immediate privacy harms, but also ill-equipped to navigate the complex privacy landscape they will face as adults.

IV. Toward a Student-Centric Paradigm

This Part develops core principles for a student-centric paradigm which recognizes privacy's essential role in education while also accounting for students' evolving autonomy and the realities of modern learning environments. These principles respond directly to the theoretical shortcomings identified above: They center students as primary rights-holders rather than subordinating their interests to parents or institutions; they conceptualize privacy as constitutive of education rather than merely protective; and they account for students' developmental trajectory rather than treating childhood as a static category.

---

445 *See supra* Sections III.A–.B.

446 Richards, *supra* note 39, at 95–108; Neil Richards, Why Privacy Matters 74–75 (2021).

447 Richards, *supra* note 39, at 95–122.

448 *Id.*

A. Core Principles for Student-Centric Privacy

The student-centric approach to privacy advanced by this Article begins by recognizing students as primary stakeholders in their own privacy interests while simultaneously acknowledging their evolving capacities. This framework builds on recent developments in privacy theory, children's rights scholarship, and learning sciences to articulate six core principles that should guide student privacy governance.

This preliminary articulation aims to spark further discussion and research, serving as a foundation for reimagining student privacy that centers students' interests while balancing students' interests with the complex web of relationships and power structures in educational settings. Substantial work remains to elaborate these concepts, grapple with potential obstacles, and explore their contextual application.

1. Recognizing Students' Evolving Autonomy

This principle acknowledges that students' capacity for privacy self-management evolves as they mature.[449] It draws on developmental perspectives on children's rights and the "new law of the child" to recognize that privacy frameworks should create graduated zones of privacy that expand with age and maturity. It aligns with Benjamin Shmueli and Ayelet Blecher-Prigat's advocacy for an independent privacy right for children that recognizes their developing autonomy interests.[450] By incorporating agency-enhancing mechanisms that increase with age, this principle ensures that privacy protections prepare students for adult privacy management rather than simply deciding for them.

Importantly, this principle does not dismiss legitimate concerns about children's vulnerability or need for protection. Rather, it rejects the false dichotomy between protection and autonomy that characterizes current approaches.[451] Similarly, John Eekelaar's concept of "dynamic self-determinism" demonstrates how frameworks can balance appropriate protection with recognition of children's growing capacity for self-determination.[452]

In practice, a student-centric approach to data collection practices would establish age-appropriate tiers of protection: parental consent for elementary students, limited autonomy for middle school, and

---

449 *See supra* Section III.A.

450 *See* Shmueli & Blecher-Prigat, *supra* note 131, at 762–63.

451 *Martha Minow, Rights for the Next Generation: A Feminist Approach to Children's Rights*, 9 HARV. WOMEN'S L.J. 1, 3–5 (1986) (critiquing binary approaches to children's rights and advocating for recognition of children's evolving capacity).

452 John Eekelaar, *The Emergence of Children's Rights*, 6 OXFORD J. LEGAL STUD. 161, 170–71 (1986) (developing the concept of "dynamic self-determinism" as a framework for children's rights).

broader independence for high school students over their own information, restricting parental oversight to only the most sensitive domains. Rather than leaving children to navigate complex privacy decisions alone, this principle calls for scaffolded opportunities to develop privacy management skills as an essential component of education.

2. Safeguarding Intellectual Privacy

Privacy protection must extend beyond personal information to safeguard the intellectual activities essential to learning and development. This principle acknowledges that learning necessitates a certain degree of risk-taking, experimentation, and even failure—processes that are inhibited when students know their every thought and action is subject to observation and judgment.[453] It positions privacy not merely as protection against external threats but as a necessary condition for meaningful learning, connecting directly to education's mission of fostering critical thinking and independent inquiry.

Recent developments in critical pedagogy emphasize the importance of creating safe spaces for intellectual exploration, particularly for marginalized students.[454] In practice, this might involve creating surveillance-free zones in schools—such as libraries or discussion areas—where students can engage in intellectual activities without monitoring and protecting the confidentiality of students' digital explorations including search histories and communications.[455]

Crucially, this principle demands protecting students' intellectual privacy from undue parental scrutiny, acknowledging that as students mature, they require confidential spaces to explore their identities and beliefs. Although young learners' privacy must be balanced with their need for protection and guidance, a student-centric approach calls for carefully tailored frameworks that minimize privacy intrusions, respect students' burgeoning autonomy, and provide robustly private spaces for intellectual and personal growth.

Implementing this principle would require a significant reimagining of privacy practices in educational settings, restricting the collection, use, and retention of student information. This might involve, as mentioned, creating surveillance-free zones in schools, such as libraries, art rooms, or designated discussion areas, where students can engage in

---

453 *See, e.g.*, Diane Ali, *Safe Spaces and Brave Spaces: Historical Context and Recommendations for Student Affairs Professionals*, Nat'l Ass'n of Student Pers. Admins. Pol'y & Prac. Series, Oct. 2017, at 1, 3–8, https://www.naspa.org/files/dmfile/Policy_and_Practice_No_2_Safe_Brave_Spaces.pdf [https://perma.cc/N37A-PBLR].

454 *Id.*

455 *See, e.g.*, Alexandra Walsh, Mary Moynihan & Elizabeth Yin, *Fixing FERPA to Protect Marginalized Students*, Regul. Rev. (Oct. 29, 2022), https://www.theregreview.org/2022/10/29/saturday-seminar-fixing-ferpa-to-protect-marginalized-students/ [https://perma.cc/KXZ3-GR5E].

intellectual activities without fear of monitoring. It would also necessitate the development of policies that protect the confidentiality of students' intellectual explorations, including their online searches, reading habits, and communication.

3. Promoting Educational Equity

Student privacy protections must actively promote educational equity rather than reinforce existing disparities. This principle recognizes that privacy harms and benefits are not distributed equally, with marginalized students often bearing the brunt of intensive surveillance while simultaneously receiving fewer privacy protections. It connects privacy to broader questions of educational justice, challenging the false neutrality of existing frameworks.

Unlike existing paradigms that treat privacy as value-free infrastructure, this principle explicitly addresses how information practices can either challenge or reinforce structural inequities. It recognizes that meaningful autonomy[456] and intellectual privacy[457] are unequally distributed in current educational environments, requiring affirmative measures to ensure all students benefit from privacy protections regardless of race, class, disability status, or other factors that have historically shaped differential treatment.

This approach requires particular attention to how surveillance and data practices disproportionately impact marginalized students. Privacy frameworks should recognize and address how information collection and use can amplify structural inequities, from biased early warning systems to discriminatory monitoring practices. It necessitates implementing data governance measures that not only ensure equitable privacy protections for all learners but also leverage data to identify and redress educational inequities.

4. Guaranteeing Technological Due Process

As educational institutions increasingly rely on algorithmic systems for decision-making,[458] students need robust procedural protections and meaningful opportunities to challenge automated determinations. This principle operationalizes the previous three by establishing the mechanisms through which evolving autonomy, intellectual privacy, and educational equity are secured in increasingly data-driven environments.

By requiring transparency about how student data is collected and used, clear procedures for contesting inaccurate information or unfair

---

456 *See supra* Section IV.A.1.

457 *See supra* Section IV.A.2.

458 *See supra* notes 46–49 and accompanying text.

inferences, and accountability mechanisms for algorithmic systems, this principle creates the procedural infrastructure needed to realize the substantive values articulated in the first three principles. These mechanisms must be developmentally appropriate, providing simpler processes for younger students while offering more sophisticated engagement opportunities for older learners. Due process in the algorithmic context requires not just formal complaint procedures but substantive protections that ensure data-driven systems serve educational goals rather than administrative convenience.

5. Promoting Democratic Values

Privacy protection in education must serve broader democratic aims by preparing students to participate meaningfully in an increasingly data-driven society. This principle connects individual privacy practices to collective democratic governance, recognizing that privacy education is essential for civil participation in the digital age. It extends intellectual privacy[459] into the civic sphere, acknowledging that the freedom to explore and develop ideas is fundamental to democratic discourse.[460]

Furthermore, the student-centric paradigm emphasizes student voice and agency in shaping educational privacy policies and practices. Rather than treating students as passive subjects of data collection and analysis, this approach calls for their active involvement in decisions about how their information is gathered, used, and shared. This could involve establishing student privacy advisory boards, conducting participatory design sessions with students to develop privacy-enhancing educational technologies, or creating opportunities for students to cocreate data governance guidelines for their schools. By centering students' perspectives and experiences in the development of privacy policies, schools can foster a more democratic and responsive approach to student data management.

6. Practicing Responsible Data Stewardship

The final principle calls for a fundamental reorientation of how educational institutions and their partners approach student data, moving from compliance-based management to substantive, ethically grounded stewardship. This principle integrates the previous principles by establishing institutional responsibilities that honor students'

---

459 *See supra* Section IV.A.2.

460 *See* Jesse Stommel, *Critical Digital Pedagogy: A Definition*, Hybrid Pedagogy (Nov. 7, 2014), https://hybridpedagogy.org/critical-digital-pedagogy-definition/ [https://perma.cc/D4NA-K4AS] (arguing for a critical approach to digital pedagogy that empowers students to shape their digital environments).

evolving autonomy, safeguard their intellectual privacy, promote educational equity, ensure technological due process, and foster democratic values.

By articulating heightened duties of care, loyalty, and confidentiality, this principle addresses the power asymmetries inherent in educational data practices while establishing a governance framework that can adapt to emerging technologies. This principle draws inspiration from the "information fiduciary" discourse on commercial entities' possible obligations to consumers but tailors it specifically to the educational context.[461] It would require entities handling student data to be held to heightened duties of care, loyalty, and confidentiality, reflecting the power asymmetries, information inequalities, and trust-based vulnerabilities inherent in contemporary learning environments. Although the exact nature and extent of reforms are beyond the scope of this Article, this concept fundamentally reframes the relationship between students and the institutions that collect and use their data.[462]

This fiduciary ethic goes beyond strict compliance with legal requirements to demand that educational data holders subordinate their own interests to those of the students whose information they collect and use. It requires data practices to be demonstrably aligned with students' academic, developmental, and future success and a default prioritization of learners' privacy and wellbeing over administrative efficiency, commercial exploitation, or other institutional imperatives.

Part of ensuring responsible student data stewardship extends beyond the schools themselves, requiring direct regulation of the education technology vendors that have become essential in today's learning environments. This recognition paves the way for a comprehensive approach through which the burden of oversight is not solely placed on educational institutions but is shared with the technology providers that serve them.

Collectively, these six principles establish the normative and theoretical underpinnings for a new student-centric approach to information governance in education. They offer a holistic and equity-conscious conceptualization of student privacy that centers learners' developmental needs, evolving capacities, and intellectual agency while addressing the institutional responsibilities that shape educational data practices.

---

461 *See, e.g.*, Matthew T. Bodie, *Employers as Information Fiduciaries*, 63 SANTA CLARA L. REV. 35, 39–49 (2023); Claudia E. Haupt, *Platforms as Trustees: Information Fiduciaries and the Value of Analogy*, 134 HARV. L. REV. F. 34, 34–41 (2020); David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 498–520 (2019); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1205–34 (2016).

462 *See* Balkin, *supra* note 461, at 2109 ("An information fiduciary is a person or business who, because of their relationship with another, has taken on special duties with respect to the information they obtain in the course of the relationship.").

Beyond specific practices, the student-centric paradigm opens up a rich agenda for future research at the intersection of education, law, and technology. It calls for empirical studies that more closely examine the actual privacy experiences, expectations, and concerns of students across diverse educational contexts and developmental stages. It invites legal scholars to explore the doctrinal and theoretical implications of recognizing students as autonomous rights-holders and data subjects within educational institutions. And it challenges learning scientists and educational technologists to develop new pedagogical and design frameworks that prioritize student agency, equity, and privacy as core affordances of digital learning environments. As educators, policymakers, and scholars continue to navigate the uncharted territories of data-driven learning, this student-centric approach offers a promising roadmap for reclaiming educational privacy as an enabler of intellectual exploration, social equity, and civic empowerment.

B. Limitations and Challenges

The implementation of the student-centric paradigm in educational practice presents a complex set of challenges and opportunities. Realizing a student-centric approach will require confronting significant obstacles posed by existing legal frameworks, institutional structures, resource constraints, and entrenched power dynamics within the educational system. The work of operationalizing student-centric principles across diverse educational contexts, developing effective implementation strategies, and building the necessary capacity and infrastructure to support student-centric privacy practices is substantial and multifaceted.

1. Legal and Policy Challenges

One significant challenge to implementing the student-centric paradigm lies in the existing legal and policy frameworks governing student privacy. Many current laws and regulations[463] were developed in a predigital era and are ill-suited to address the complex privacy issues raised by the widespread collection and use of student data in modern educational contexts.[464] These frameworks often prioritize parental rights and institutional interests over student autonomy and agency, creating barriers to student-centric approaches.[465]

Updating these legal frameworks to better reflect the realities of data-driven education and the evolving capacities of students will

---

463 Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506; *see supra* note 21.

464 *See supra* Section I.B.

465 *See supra* Part II.

require significant policy reform efforts at the federal and state levels.[466] This may involve amending existing student privacy laws and regulations to better align with the realities of contemporary data-driven education and the evolving capacities of students as digital natives. Policymakers will need to move beyond the dominant parent-centric and school-centric frameworks to develop more nuanced, developmentally appropriate, and equity-conscious approaches to student data governance.

This Article contributes to growing discussions about how powerful entities misuse privacy law as a pretext, shield, or weapon. For example, companies use the General Data Protection Regulation and schools use FERPA to object to discovery requests and evade accountability.[467] By examining how schools and companies invoke privacy laws to evade accountability or restrict access to information, this analysis reveals how seemingly neutral privacy protections can reinforce existing power imbalances.[468]

2. Institutional Barriers and Power Dynamics

Implementing a student-centric approach will also require navigating complex institutional barriers and entrenched power dynamics within the educational system.[469] Schools, education technology companies, and other stakeholders may resist changes that challenge their authority or disrupt established data practices. Overcoming these obstacles will require not only policy reforms but also cultural shifts in how educational institutions and actors understand and prioritize student privacy.

Realizing a student-centric paradigm necessitates addressing the structural inequities that shape students' privacy experiences. Marginalized student populations, particularly those from low-income backgrounds, are disproportionately subject to invasive surveillance and data-driven interventions that can perpetuate discriminatory tracking and stigmatization.[470]

---

466 *See supra* Section III.D.

467 *See* Neil Richards, *The GDPR as Privacy Pretext and the Problem of Co-Opting Privacy*, 73 HASTINGS L.J. 1511, 1513 (2022); Steve Zansberg, *Removing FERPA's "Invisibility Cloak" from Records Showing Public Employees Behaving Badly*, AM. BAR. ASS'N (Mar. 16, 2022), https://www.americanbar.org/groups/communications_law/publications/communications_lawyer/2022-winter/removing-ferpas-invisibility-cloak-records-showing-public-employees-behaving-badly/ [https://perma.cc/762T-B4HV].

468 *See supra* Part II.

469 *See supra* Parts I–III.

470 *See supra* Section III.B.3.

3. Technological and Infrastructural Constraints

Implementing student-centric privacy practices also requires overcoming technological and infrastructural constraints within educational institutions. Many schools, particularly those serving low-income and marginalized communities, lack the necessary technical infrastructure, data management systems, and trained personnel to support robust privacy protections and data governance practices. Addressing these resource and capacity gaps will require significant investments in school infrastructure, professional development, and support services. Ensuring that student-centric principles are embedded in the design and deployment of these technologies will require close collaboration between educators, technologists, and legal experts, as well as the development of new technical standards and ethical frameworks for responsible data use in education.

4. Addressing Potential Objections

Defenders of the status quo might object that this critique undervalues the legitimate roles of parents and schools in protecting children's interests. Some might argue that children lack the maturity to make important privacy decisions, necessitating adult oversight.[471] Others might contend that educational institutions require significant discretion to operate efficiently in an increasingly complex technological environment.[472]

The student-centric paradigm does not deny children's need for protection or guidance. Rather, it recognizes that protection and autonomy exist on a continuum that evolves with development, not in binary opposition. As Emily Buss argues, frameworks that acknowledge children's evolving capacities can provide appropriate protections while still respecting their growing autonomy.[473] Similarly, Benjamin Shmueli and Ayelet Blecher-Prigat demonstrate that graduated approaches to children's privacy rights can balance protection with recognition of developing agency.[474]

These objections ultimately reinforce rather than refute this Article's analysis. They exemplify the binary thinking that characterizes current approaches—assuming that either parents or institutions must exercise primary control with little consideration for students' evolving capacities or the distinctive privacy needs of learners. A more nuanced

---

471 *See* Shmueli & Blecher-Prigat, *supra* note 131, at 788–95 (discussing arguments for parental control over children's privacy based on children's limited capacity and vulnerability).

472 *See supra* Part II and Sections III.A–.C.

473 *See generally* Emily Buss, *Developmental Jurisprudence*, 88 Temple L. Rev. 741 (2016) (discussing how the law can help facilitate children's growth and individual autonomy).

474 *See* Shmueli & Blecher-Prigat, *supra* note 131, at 783–85.

approach would recognize that protecting students' privacy interests often requires creating spaces free from both parental surveillance and institutional monitoring, particularly as students mature. It would also acknowledge that respecting students' intellectual privacy can enhance rather than undermine educational outcomes by fostering the conditions necessary for authentic learning and development.

C. Implications and Future Directions

The student-centric paradigm has significant implications for educational privacy but also for broader debates about child privacy and digital rights in the twenty-first century.[475] This Section explores these implications and charts future directions for research, policy, and practice.

1. Implications and Benefits of the Student-Centric Paradigm

The novel student-centric paradigm has the capacity to impact educational equity and democratic citizenship in the digital age. By prioritizing the privacy rights and developmental needs of all students, particularly those from marginalized and vulnerable communities, the student-centric approach can help mitigate the disparate impacts of educational surveillance and data-driven decision-making on historically disadvantaged groups. It can also empower students to exercise greater control over their own data and digital identities, preparing them to participate as informed and critical citizens in an increasingly data-driven society.

By fostering a culture of trust, transparency, and accountability around educational data practices, the student-centric paradigm can help build public confidence in educational institutions and support the democratic mission of education. It can create spaces for students to engage in critical dialogues about privacy, ethics, and technology, developing the skills and dispositions necessary for lifelong learning and civic engagement.

The student-centric privacy paradigm advanced in this Article also contributes to present debates about children's privacy and digital rights. As young people increasingly live, learn, and socialize in digital environments, policymakers and scholars have grappled with how to balance the need to protect children from online harms with the importance of respecting their autonomy and agency as digital citizens.

---

475 *See* Katherine A. Hild, Leave Me Alone: Protecting Children's Privacy in the Digital Age, 17–18 (Apr. 11, 2017) (M.A., thesis, Georgetown University) (on file with author), https://repository.library.georgetown.edu/handle/10822/1043835 [https://perma.cc/NG6D-4XA9].

Dominant approaches to child privacy have often relied on paternalistic frameworks that prioritize parental control and consent over children's own evolving capacities and preferences. These frameworks, while well-intentioned, can have the unintended consequence of limiting children's opportunities to learn, explore, and participate meaningfully in the digital world.[476] They may also fail to account for the diverse contexts and developmental stages that shape children's privacy needs and experiences online.

The student-centric paradigm offers an alternative approach that recognizes children's rights to privacy, participation, and protection as interdependent and mutually reinforcing. By emphasizing the importance of intellectual privacy, age-appropriate agency, and contextual transparency, this approach seeks to empower children to make informed choices about their data and digital identities while still providing appropriate safeguards and support structures. It also highlights the role of educational institutions in fostering digital literacy and critical thinking skills that enable children to navigate the complexities of privacy in a data-driven world.

Moreover, the student-centric paradigm underscores the importance of including children's voices and perspectives in the development of privacy policies and practices that affect them. Rather than treating children as passive subjects of adult decision-making, this approach calls for participatory and inclusive processes that engage young people as active stakeholders in the governance of their own data. This kind of collaborative and contextual approach to child privacy can help ensure that policies and practices are responsive to the actual needs, experiences, and concerns of young people in diverse digital contexts.

Although the student-centric paradigm is grounded in the specific context of educational privacy, its core principles and values have broader relevance for child privacy debates beyond the schoolhouse gate. As policymakers and scholars continue to grapple with the challenges of ensuring children's safety, autonomy, and privacy in an increasingly data-driven world, this paradigm offers a valuable approach for empowering young people to become active and informed participants in shaping their digital futures.

2. Future Directions for Research and Policy

The student-centric paradigm provides promising avenues for future research and policy development. From an empirical perspective, there is a need for more research on students' privacy experiences, expectations, and concerns across diverse educational contexts and developmental stages. This research can inform the design of more

476 *See supra* Part III.

effective and equitable privacy policies and practices, as well as the development of new pedagogical approaches and technological tools that prioritize student agency and autonomy.

This reorientation of student privacy also encourages interdisciplinary collaboration and knowledge sharing between educators, legal scholars, technologists, and policymakers. From a practical perspective, translating these principles into operational practices requires careful consideration of implementation strategies. The student-centric approach would transform how schools handle consent by establishing age-appropriate tiers that evolve with students' development. When addressing algorithmic decision-making systems, a student-centric framework would require rigorous pre-implementation testing for bias and ongoing monitoring of disparate impacts, with meaningful opportunities for students and families to challenge determinations affecting educational opportunities.

Beyond specific practices, the student-centric paradigm opens up a rich agenda for future research at the intersection of education, law, and technology. It calls for empirical studies that more closely examine students' actual privacy experiences, invites legal scholars to explore the doctrinal implications of recognizing students as autonomous rights-holders, and challenges educational technologists to develop new pedagogical frameworks that prioritize student agency, equity, and privacy as core affordances of digital learning environments. This research agenda recognizes that student privacy is not merely a specialized subfield but a critical site for understanding broader social, legal, and technological developments that affect education and democratic society.[477]

Ultimately, realizing the full potential of the student-centric paradigm will require ongoing collaboration and dialogue between diverse stakeholders, including educators, policymakers, legal scholars, technologists, parents, and students themselves. By working together to navigate the complex challenges and opportunities of educational privacy in the digital age, these stakeholders can chart a path toward a future in which the privacy and flourishing of all students are recognized as essential to the mission of education and the health of our democracy.

Conclusion

This Article's fundamental contribution lies in exposing a fundamental incongruity: Despite their labels, student privacy laws systematically fail to center students themselves. Current frameworks marginalize students in favor of adult stakeholders, representing not merely an implementation problem but a theoretical limitation

---

477 *See supra* Section IV.B.

embedded in the conceptual architecture of student privacy law. By exposing the descriptive and normative assumptions that have shaped privacy governance in education, this work provides both a diagnosis of existing shortcomings and a prescription for more effective protection.

The student-centric approach advanced here represents a fundamental reconceptualization of privacy in educational contexts. Rather than treating students as passive objects of protection or as extensions of their parents, it recognizes them as evolving rights-bearers with distinct privacy interests essential to their learning and development. This shift in perspective has profound implications not only for privacy law but for how we conceive of education itself: as a space where students develop both knowledge and the capacity for autonomous decision-making, including decisions about their own privacy.

Through paradigmatic analysis, this Article illuminates the shortcomings of parent-centric and school-centric approaches, demonstrating that they provide insufficient data protections and neglect privacy's vital role in learning and growth. In response, it has offered a normative and theoretical framework for reorienting educational privacy around six core principles: student autonomy, intellectual privacy, educational equity, technological due process, promotion of democratic values, and responsible data stewardship. Together, these principles provide a blueprint for reenvisioning student privacy as an essential infrastructure for learning, creating the conditions necessary for students to experiment, question, and develop as autonomous and critically engaged citizens.

The student-centric paradigm creates the conditions for students to explore, experiment, and develop their authentic selves without fear of stigma or repercussion. It emphasizes the importance of providing students with age-appropriate opportunities to exercise agency over their own data and to cultivate the skills and dispositions necessary for critical engagement with the technologies that shape their lives. It also highlights the responsibility of educational institutions to model ethical data practices that align with the democratic purposes of education.

Furthermore, this Article contributes to ongoing debates in legal theory about the nature and function of rights in contemporary society. As Jamal Greene argues, rights have increasingly shifted from being a bulwark against government oppression to a tool for embedding fundamental values and policy preferences.[478] The student-centric paradigm reflects this understanding by reconceptualizing student privacy rights not merely as a matter of individual control or parental authority but as

---

478 *See generally* JAMAL GREENE, HOW RIGHTS WENT WRONG: WHY OUR OBSESSION WITH RIGHTS IS TEARING AMERICA APART (2021) ("Rights in a modern constitutional democracy are not the glass we break in the emergency of a government captured by bigots or morons. They are the predictable byproducts of ordinary governance in a pluralistic society in which we disagree with one another about important matters.").

a means of promoting collective values and policy preferences related to education, child development, and democratic citizenship in the digital age.

Ultimately, the work of building a student-centric privacy framework is not merely a matter of technical implementation but of fundamental social transformation. It demands confronting the structural inequities that shape students' informational lives, dismantling power asymmetries between youth and the institutions that serve them, and radically reimagining the meaning and practice of privacy in learning. This reveals privacy not as a barrier to innovation but as the foundation upon which meaningful education depends.

As stakeholders continue to grapple with the profound challenges and opportunities of student privacy in the digital age, this Article offers a roadmap for centering the voices, needs, and aspirations of students themselves. It calls for collaborative action to ensure that student data governance serves the interests of learners, communities, and democracy, ultimately unlocking the transformative potential of education in the twenty-first century and beyond.