RETHINKING YOUTH PRIVACY

Danielle Keats Citron and Ari Ezra Waldman***

Congress and state legislatures are showing renewed interest in youth privacy, proposing myriad new laws to address data extraction, addiction, manipulation, and more. Almost all of their proposals, and youth privacy law in general, follow what we call the parental control model. The model is erected in the name of children, but it mostly ignores their expressed privacy interests. Under the model, parents are asked to provide consent for the collection of children's data, to check on the handling of that data, and to protect children from danger. Because parental control dominates policymaking and scholarly discourse, it goes unquestioned. This Article challenges the status quo. Parental control risks harm to vulnerable children, overburdens caregivers (who are more often women), and denies youth the intimate privacy that they need to grow and develop close relationships, including, ironically, relationships with their parents. The parental control model disserves nearly everyone involved except companies that press for its adoption because it earns them massive advertising profits without costly responsibilities for youth safety and privacy. The time is now to reimagine the youth privacy project. We need to shed the yoke of exclusive parental control and to protect the intimate privacy that youth want, expect, and deserve. Our proposal foregrounds youth

* Jefferson Scholars Foundation Schenck Distinguished Professor of Law, University of Virginia School of Law; Vice President, Cyber Civil Rights Initiative; 2019 MacArthur Fellow.

** Professor of Law and, by courtesy, Professor of Sociology, University of California, Irvine School of Law; Member, Board of Directors, Cyber Civil Rights Initiative. Special thanks to Alice Abrokwa, Anita Allen, Anu Bradford, Naomi Cahn, Ryan Calo, Ellie Citron, Maxine Eichner, Fanna Gamal, Alison Gocke, Woodrow Hartzog, Clare Huntington, Paul Schwartz, Kate Silbaugh, Scott Skinner-Thompson, Mona Sloane, Daniel Solove, Kathy Strandburg, Catharine Ward, and Phil Weiser (who graciously joined UVA Law's Spring 2024 Privacy 1 class to discuss his work on youth privacy). Matthew Hamilton, Ryan Johnston, Zoe Kirsner, Adeline Lee, Olivia Sahid, and Shivani Vikuntam provided outstanding research assistance. Kate Boudouris is a librarian extraordinaire, and Michaela Thompson a superb assistant. The editors of the *Virginia Law Review* went above and beyond in their skilled efforts; we are grateful to Tyler Tidwell, Derek Furr, Olivia Haimerl, and all of the editors who worked on this piece. We thank our respective Deans Leslie Kendrick and Austen Parrish for their support. The authors contributed equally to the Article, so names are listed alphabetically.

voices and intimate privacy interests. It calls for policymakers to address corporate amassing of youth data and to place responsibility on their shoulders, which accords with what young people say they want. Companies are best situated to secure youth privacy and to minimize risks to child safety. Beyond law, parents should be encouraged to act more as partners with their children in the effort to protect their intimate privacy. That personal imperative will redound to parents' and children's benefit and engender trust and love.

INTRODUCTION

The privacy afforded young people is under threat. Social media companies track and share young people's online activities with advertisers, generating billions in profits.[1] Commercial websites trap young people in endless loops of data extraction, data-driven targeted advertisements, and video feeds that manipulate behavior, facilitate addiction, and increase screen time.[2] Surveillance software monitors students' laptop and tablet activities to detect bullying, suicidal ideation, and threats.[3]

Parental supervision has been policymakers' go-to solution to securing youth privacy interests for decades. The Children's Online Privacy Protection Act of 1998 ("COPPA") requires websites and online services to ask parents for permission to handle children's personal data and requires parents to contact those services to stop the further collection and sale of their children's personal data.[4] On January 16, 2025, the Federal Trade Commission ("FTC"), which enforces COPPA, finalized changes to its COPPA Rule to give parents control over advertisements targeted to children.[5] The Kids Online Safety Act, which the Senate passed in June 2024, would enhance parental authority by requiring online platforms to provide controls for parents so they can monitor accounts held by children aged sixteen and younger.[6]

[1] Alfred Ng, Where Parental Snooping Is Becoming the Law, Politico (Apr. 11, 2023, 1:50 PM), https://www.politico.com/news/2023/04/11/social-media-privacy-parents-kids-00091400.

[2] Samuel Levine, Bureau of Consumer Prot., Protecting Kids From Stealth Advertising in Digital Media 1–5 (2023), https://www.ftc.gov/system/files/ftc_gov/pdf/p214505kidsadvertisingstaffperspective092023.pdf [https://perma.cc/39DS-KZYF].

[3] Nir Kshetri, School Surveillance of Students via Laptops May Do More Harm Than Good, The 74 (Jan. 19, 2022), https://www.the74million.org/article/school-surveillance-of-students-via-laptops-may-do-more-harm-than-good/ [https://perma.cc/MMX8-79LE].

[4] E.g., Children's Online Privacy Protection Act (COPPA) of 1998, 15 U.S.C. §§ 6501–6506.

[5] Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2025).

[6] Kids Online Safety and Privacy Act, S. 2073, 118th Cong. § 103(b) (as passed by Senate, July 30, 2024); see also H.B. 311, 2023 Gen. Sess., Reg. Sess. (Utah 2023) ("Social Media Usage Amendments"); S.B. 152, 2023 Gen. Sess., Reg. Sess. (Utah 2023) (giving parents power to monitor children's social media accounts without their knowledge or permission).

Under the mandate of law and the hydraulics of social pressure, parents have gotten the message that they should be monitoring their children.[7] According to one study, 90% of parents surveyed try to monitor the digital activities of younger children (aged six through twelve); 40% of parents say that they endeavor to monitor the activities of older children (aged thirteen through seventeen).[8] Utah State Senator Kathleen Riebe, who uses an app to control her son's phone, urges fellow parents to do the same.[9]

The prevailing approach to children's privacy in the United States follows what we call the *parental control model*—the ecosystem of laws, practices, logic, and ideologies that give parents authority over children's privacy interests. That model is erected in the name of children's privacy, but it mostly excludes youth and their privacy interests from the calculus.

Lawmakers are scrambling to tackle profoundly harmful corporate practices that exploit children's data, including the manipulation of young people to consume material that causes self-doubt, depression, and suicide and exposes children to harassment and predation. Policymakers' go-to response—parental control—is a failure. While the parental control model was never well suited to protect children's privacy, it cannot meet this moment.

No parent, no matter how well intentioned and resourced, can ensure that children's privacy is prioritized and protected. No parent can meaningfully curtail corporate data collection, either for themselves or their children.[10] Therefore, the inevitable result of parental authority is

[7] See, e.g., What Parents Should Know About Parental Control Apps, Nat'l Cybersecurity All. (June 28, 2023), https://staysafeonline.org/programs/events/what-parents-should-know-about-parental-control-apps-webinar/ [https://perma.cc/7R48-S727] ("[A]n essential part of parenting in the 21st Century is monitoring your children's digital lives . . . [so] parents can work to keep their kids safe."); Top 10 Best Parental Control Apps (2025), Fam. Online Safety, https://www.familyonlinesafety.com/best-paretnal-control-apps [https://perma.cc/DHT4-5TXT] (last updated Oct. 2025) ("Parental control apps are fast becoming a must have for any parent.").

[8] Microsoft, Global Online Safety Survey 2024, at 38–39 (2024), https://news.microsoft.com/wp-content/uploads/prod/sites/40/2024/02/Microsoft-Global-Online-Safety-Survey-2024.pdf [https://perma.cc/R6WM-LFFY] (explaining that parents surveyed monitored children by receiving activity reports, reviewing friend requests, and reviewing and adjusting children's privacy settings on accounts and devices).

[9] Utah Senate, Senate Floor Audio on S.B. 152, Day 28, 2023 Gen. Sess., at 01:05:58 (Feb. 13, 2023) [hereinafter Utah Senate Audio (Feb. 13, 2023)], https://le.utah.gov/av/floorArchive.jsp?markerID=121381 [https://perma.cc/34RU-SG94] (statement of Sen. Kathleen Riebe).

[10] See Geoffrey A. Fowler, Your Kids' Apps Are Spying on Them, Wash. Post (June 9, 2022), https://www.washingtonpost.com/technology/2022/06/09/apps-kids-privacy/ (noting

more corporate monetization of children's data.[11] As for safety, even if parents could minimize or prevent some hazards, exclusive parental responsibilities mean exclusive parental burdens, and parents are ill-equipped to shoulder them. Also, not all parents are well meaning: youth have been thrown out of their homes or beaten after adults discovered children's emerging LGBTQ+ identities by accessing their private online activities.[12]

The parental control model has a perverse downside: it undermines the very privacy that young people need to grow, mature, and thrive. In this Article, we use the term *youth intimate privacy* to refer to the privacy that young people claim, expect, and deserve.[13] Youth intimate privacy involves others' access to, and information about, minors' bodies, thoughts, health, sex, gender, sexual orientation, sexual activities, and close relationships, whether in physical or digital activities or spaces.[14] Youth need intimate privacy for maturation, self-esteem, and close

that by the time a person turns thirteen, "online advertising firms hold an average of 72 million data points" on them).

[11] Press Release, Fed. Trade Comm'n, FTC Staff Report Finds Large Social Media and Video Streaming Companies Have Engaged in Vast Surveillance of Users with Lax Privacy Controls and Inadequate Safeguards for Kids and Teens (Sept. 19, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-staff-report-finds-large-social-media-video-streaming-companies-have-engaged-vast-surveillance [https://perma.cc/UUT7-RFES] (detailing "the data collection and use practices of major social media and video streaming services" to "incentivize[] mass collection of user data to monetize, especially through targeted advertising").

[12] Jamie Gorosh & Chris Wood, LGBT Tech & Future of Priv. F., Student Voices: LGBTQ+ Experiences in the Connected Classroom 7 (2023) (noting a 2020 survey by the Trevor Project that found "29% of LGBTQ+ youth have experienced homelessness, been kicked out of their homes, or have run away" (citation omitted)); see also Anne Collier, Why I Struggle Mightily with the New Utah Law, Net Fam. News (Mar. 30, 2023), https://www.netfamilynews.org/why-i-struggle-mightily-with-the-new-utah-law [https://perma.cc/L2AG-NDHR] (arguing that laws giving parents control over children's online accounts "could end up supporting abusive parents who use it to monitor and punish children who use social media to get help").

[13] See generally Danielle Keats Citron, The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age, at xii–xiii (2022) [hereinafter Citron, Fight for Privacy]. Intimate privacy is a capacious privacy interest that is critical to identity development, self-esteem, and love; it has special importance because it helps youth learn the skills of autonomy, independence, and relationship building, which are essential for adulthood. See infra Section III.B. We focus on youth intimate privacy for practical and normative reasons. Much of what law regulates implicates youth intimate privacy, and the privacy that most matters to human flourishing involves the privacy around our intimate lives. See generally infra Part III. Because of its importance and because even prosaic personal data becomes intimate data when amassed, we use the phrase youth intimate privacy interchangeably with youth privacy unless we signal otherwise.

[14] Citron, Fight for Privacy, supra note 13, at xii.

relationships.[15] Intimate privacy is a prerequisite for autonomy and maturation.[16] Only with privacy can children grow and develop into democratic citizens, an oft-stated goal of parenting, education, and socialization.[17]

Current privacy law ignores all of this and damages youth intimate privacy. It also frays parent-child relationships rather than enhances them.[18] Because children under parental surveillance feel that their trust has been betrayed, they do their best to hide their online activities from their parents.[19] This puts youth at greater risk from the very hazards that rightly worry parents and policymakers.[20]

In short, the parental control model is a wolf in sheep's clothing. It is an empowering facade that leaves parents unable to protect children and undermines the intimate privacy that youth need to thrive. It is bad for parents, children, and parent-child relationships. And it is bad for the pursuit of equality. The parental control model places impossible burdens on caregivers, many of whom are women.[21] It does the opposite of what

[15] Danielle Keats Citron, The Surveilled Student, 76 Stan. L. Rev. 1439, 1457–60 (2024) [hereinafter Citron, Surveilled Student].

[16] See, e.g., Maxine Wolfe, Childhood and Privacy, *in* Children and the Environment 175, 189 (Irwin Altman & Joachim F. Wohlwill eds., 1978) (explaining that "children's experiences with privacy feed back into their sense of self-esteem and help define the range, limits, and consequences of individual autonomy"); Ross D. Parke, Children's Home Environments: Social and Cognitive Effects, *in* Children and the Environment, supra, at 33, 66–68 (explaining how children's need for privacy increases with age and varies by situation and activity).

[17] See W. Va. Bd. of Educ. v. Barnette, 319 U.S. 624, 637 (1943) ("That [public schools] are educating the young for citizenship is reason for scrupulous protection of Constitutional freedoms of the individual . . . .").

[18] Valerian J. Derlega & Alan L. Chaikin, Sharing Intimacy: What We Reveal to Others and Why 15 (1975) (explaining that children can and occasionally will claim zones of privacy and that when parents disrespect those zones, children lose the trust necessary for close relationships).

[19] For a recent example, see Denise Witmer, Why Teens Need Privacy From Their Parents, Yahoo (July 29, 2024, 11:36 AM), https://www.yahoo.com/lifestyle/why-teens-privacy-parents-153635430.html [https://perma.cc/U2Q2-DNNV]. Part IV explores the rich social science literature in detail.

[20] Ng, supra note 1 ("Researchers have found that parental monitoring apps . . . were associated with *increased* chances of teen online victimization, compared to teens whose parents didn't use monitoring services."); see Citron, Fight for Privacy, supra note 13, at 14–15 (explaining that some health apps pose risks to young women and girls' health privacy and safety); Ari Ezra Waldman, Privacy as Trust: Information Privacy for an Information Age 62–78 (2018) [hereinafter Waldman, Privacy as Trust].

[21] Microsoft, supra note 8, at 39 (identifying mothers as more active in monitoring their children's online activities).

it purports to do—it hurts parents and children, and it does not lead to greater privacy protections. Indeed, the central beneficiaries of parental control are the companies that earn massive profits from exploiting children's data and endangering their safety.

Policymakers must reckon with the inadequacies of the current approach. They should reject exclusive parental control and choose a structural and collaborative posture to youth intimate privacy for the good of children, parents, families, and democracy. We propose a new model to do just that. Our approach foregrounds youth voices and interests, prioritizes legal reform focused on corporate responsibility, encourages parental-child collaboration, and supports young people and their parents.

Now is the time to rethink youth intimate privacy. Federal proposals are being introduced and debated. States are filling the void, but their work is just beginning. Plus, the risks are undeniable: the advertising-driven information economy invades young people's privacy at alarming rates.[22] Rapidly advancing artificial intelligence metastasizes those privacy risks by increasing demand for data about individuals.[23] Adolescents, particularly young women, face the dangers of image-based sexual abuse and pornographic deepfakes.[24]

In developing this argument, this Article makes several contributions to legal scholarship. We challenge the conventional approach that automatically associates parental privacy control with youth privacy. We interrogate the often-ignored step of relying upon parents to the exclusion, and sometimes to the detriment, of children themselves. We unearth legislative history showing that many so-labeled youth privacy laws were drafted to empower parents to dictate young peoples' activities, rather than to directly secure youth privacy interests. We highlight youth perspectives on intimate privacy, drawn from state legislative testimony, which have been left out of scholarly discussion in the United States. Our vision of youth privacy law charts a more straightforward, inclusive, and

[22] Katie Joseff, Behavioral Advertising Harms: Kids and Teens, Common Sense Media 2–3 (2022), https://www.commonsensemedia.org/sites/default/files/featured-content/files/behavioral_-surveillance-advertising-brief.pdf [https://perma.cc/N2S7-XFTK] (noting that the advertising technology industry has at least seventy-two million data points about each child before they are thirteen).

[23] E.g., Harry Surden, Artificial Intelligence and Law: An Overview, 35 Ga. St. U. L. Rev. 1305, 1315–16 (2019).

[24] Natasha Singer, Teen Girls Confront an Epidemic of Deepfake Nudes in Schools, N.Y. Times (Apr. 8, 2024), https://www.nytimes.com/2024/04/08/technology/deepfake-ai-nudes-westfield-high-school.html.

productive path. It begins with structural reform because individualized efforts are ineffective, burdensome, and isolating. It calls for the involvement of all parties (including youth, parents, and schools) in securing youth privacy interests. Adjusting parental control at the margins or shifting domination from parents to young people or schools is insufficient.

This Article has four parts. Part I shows the breadth of the parental control model. It surfaces the tradition of parental privacy authority in youth privacy law, from the rules governing the collection and processing of children's data by digital platforms to data concerning youth as students.

Part II uncovers the prevailing rationales for the parental control model, filling a gap left by existing privacy scholarship that has, for the most part, assumed that parental control is obvious and acceptable. Those explanations involve distinct but interrelated categories: social science, norms, and legal policy. First, we show that the parental control model depends on a particular view of childhood development that sees maturity, defined by age, as a prerequisite for making informed choices about privacy. Second, the parental control model is based on legal rationales borrowed from consumer privacy, including the rationality demands of the "notice-and-consent" approach whereby adults are presumed to read privacy policies and make choices about online disclosure.[25] Last, it reflects norms of the family in which adults inculcate children with their values and ideals.

Part III challenges these rationales, finding them uninformed, overinclusive, and discriminatory. This Part highlights how exclusive parental control over youth privacy is not supported by the social science literature, which emphasizes the importance of privacy to childhood development. It explores how social norm-based rationales for parental control are based on an overly romanticized conception of the family, in terms of both gender roles and the relationship between caregivers and youth. Relying on this vision of the family sweeps aside the reality that many young people, including LGBTQ+ children, grow up without that romanticized family dynamic. Finally, this Part shows how the legal

[25] The literature on notice-and-consent is voluminous. For discussions specifically connecting notice-and-consent with the presumption of rationality, see, e.g., Ari Ezra Waldman, Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power 52–63 (2021); Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New Technologies 35–36 (2018).

rationales border on the absurd: a long line of studies shows that adults are incapable of bearing the burden of privacy self-management and effectuating their own privacy preferences,[26] and yet current law expects them to do so not only for themselves but also for their children.

Part IV offers a new model for youth intimate privacy based on four principles: respect for youth voices, structural reform, collaboration, and support. Lawmakers and regulatory authorities should step in to ensure that youth intimate privacy interests are secured in the information economy—the time is now to regulate the very companies whose data-extractive practices undermine youth intimate privacy and endanger child safety. Lawmakers can and should collaborate with and listen to young people about their privacy expectations and needs. Schools and youth can support parents, alleviating parental isolation from systems of support and bearing some of the burdens. We consider this piece a first step, not a precise road map. We want to encourage the development of a youth intimate privacy project that can evolve to meet new challenges and accommodate different interests.

I. ILLUSTRATING THE PARENTAL CONTROL MODEL

This Part proves our descriptive claim that youth privacy law is, in fact, parental control. It focuses on two critical regulatory arenas. The first involves consumer privacy laws addressing corporate handling of children's data and social media regulation. The second concerns the laws and practices governing student privacy. This Part demonstrates the model's hold on our legal imagination. It shows how most privacy scholars either have failed to acknowledge the lack of youth interests in youth privacy law or have adopted the parental control model without interrogating it.

A. Examples of the Law and Practice of Parental Control

U.S. privacy laws reflexively treat parents as their children's exclusive privacy authorities. As the consumer protection and student contexts show, children's own privacy interests are absent from the legal calculus.

[26] See, e.g., Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 Harv. L. Rev. 1880, 1882–93 (2013).

1. Consumer Privacy and Social Media Laws and Practices

Sector-specific and comprehensive laws regulating the commercial handling of children's data overwhelmingly rely on parental control.[27] The paradigmatic example is COPPA.[28] Certain websites and online services must provide privacy notices to parents and ask them for "verifiable consent" before collecting personal information from children who are under thirteen years old.[29] Parents must be able to request a description of the types of personal information collected from children and ask covered entities to stop the further use or collection of a child's personal information or to delete the information entirely.[30] Once parents revoke their consent, children may no longer be able to use the online service.

COPPA's drafters and supporters underscored the importance of parental control. The bill's cosponsor, Senator Richard Bryan, explained

[27] U.S. data privacy law is "sectoral," especially at the federal level. Rather than by a single comprehensive privacy law, data is regulated only in some industries or parts of the economy, including health, financial, and, most relevant for this Article, children's data. Even where personal data is regulated, the law only protects certain data in certain circumstances. See, e.g., Paul M. Schwartz, Preemption and Privacy, 118 Yale L.J. 902, 904–05 (2009). This stands in contrast to a more comprehensive or "omnibus" approach, exemplified by the General Data Protection Regulation ("GDPR") in the European Union, which applies generally to almost all platforms that collect and process data. Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1, 37–38 [hereinafter GDPR].

[28] The only parts of COPPA that do not empower parents are sections that place duties on websites and online services to collect only personal information that is "reasonably necessary [for children] to participate" in a game or competition; maintain the confidentiality, security, and integrity of information collected from children; and retain children's personal information for only as long as necessary to fulfill the purpose for which it was collected. 15 U.S.C. § 6502(b)(1)(C), (2)(D); 16 C.F.R. § 312.7–.8, .10 (2025).

[29] Websites and online services covered by COPPA are those targeted to children, based either on their subject matter, visual content, use of animated characters, and other appeals to children, or on their actual knowledge that they are collecting personal information directly from children. 16 C.F.R. § 312.2 (2025). Regarding notice, see id. § 312.4; Complying with COPPA: Frequently Asked Questions, Fed. Trade Comm'n (Jan. 2025) [hereinafter Complying with COPPA], https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions [https://perma.cc/YWS9-APYQ]. Regarding "verifiable consent," see 15 U.S.C. § 6501(9); 16 C.F.R. § 312.5 (2025). In July 1998, Senators John McCain and Richard Bryan introduced S. 2326, which defined anyone under sixteen as a child; the bill that was passed in the House and Senate and signed into law lowered the age of children to under thirteen. Phyllis Marcus, Children's Privacy in the United States, *in* Children's Privacy and Safety 5, 8–9 (Kalinda Raina ed., 2022).

[30] 16 C.F.R. § 312.6 (2025).

that COPPA would "enhance parental involvement in a child's online activities" and condition "the collection of personal information from children" on "parental consent."[31] Then-FTC Chair Robert Pitofsky urged lawmakers to place parents in charge of the handling of their children's data.[32] The FTC's COPPA compliance guide explains that the law was drafted with the "primary goal" of "plac[ing] parents in control."[33] To that end, the FTC has investigated and sued sites that failed to obtain verifiable parental consent before collecting children's data.[34]

[31] 144 Cong. Rec. 12787 (1998) (statement of Sen. Richard Bryan).

[32] Consumer Privacy on the World Wide Web: Hearing Before the Subcomm. on Telecomms., Trade & Consumer Prot. of the H. Comm. on Com., 105th Cong. (1998) (statement of Robert Pitofsky, Chairman, FTC). FTC staff member David Medine testified that there needed to be some degree of parental choice over the disclosure of personal information about children. Privacy in Electronic Communications: Hearing Before the Subcomm. on Cts. & Intell. Prop. of the H. Comm. on the Judiciary, 105th Cong. 9–10 (1998), https://play.google.com/books/reader?id=_OsnAAAAMAAJ&pg=GBS.PP7&hl=en [https://perma.cc/LSV4-6QG7] (statement of David Medine, Assoc. Dir. for Credit Pracs., Bureau of Consumer Prot., FTC); see also Internet Privacy: Hearing Before the Subcomm. on Cts. & Intell. Prop. of the H. Comm. on the Judiciary, 105th Cong. (1998), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-internet-privacy/privacy.pdf [https://perma.cc/HN3Y-NPRH] (statement of David Medine, Assoc. Dir. for Credit Pracs., Bureau of Consumer Prot., FTC) (highlighting the need for sites to "allow parents to have control over the collection, disclosure, and use of their children's information"). In March 1998, the FTC surveyed 1,402 commercial websites, including 212 sites directed to children, and found that 90% of sites directed to kids were collecting extensive information from and about children, 23% of those sites asked parents for permission before collecting children's data, and only three sites required parental consent before collecting children's information. Marcus, supra note 29, at 7. The results of this survey animated lawmakers to require parental consent for the handling of children's data. Id. at 8.

[33] Complying with COPPA, supra note 29.

[34] E.g., First Amended Complaint for Permanent Injunction & Other Equitable Relief at 3, 5, FTC v. Toysmart.com, LLC, No. 00-cv-11341, 2000 WL 34575570 (D. Mass. July 21, 2000) (seeking to enjoin Toysmart's collection of children's data without parental consent); Complaint for Civil Penalties, Permanent Injunction & Other Equitable Relief at 9–10, United States v. Musical.ly, No. 19-cv-01439, 2019 WL 976734 (C.D. Cal. Feb. 27, 2019) (seeking monetary civil penalties and to enjoin Musical.ly's collection and use of children's data without parental notice or consent); Press Release, Fed. Trade Comm'n, Developer of Apps Popular with Children Agrees to Settle FTC Allegations It Illegally Collected Kids' Data Without Parental Consent (June 4, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/06/developer-apps-popular-children-agrees-settle-ftc-allegations-it-illegally-collected-kids-data [https://perma.cc/D6EB-47BU] (settling for $150,000 and agreeing to delete children's data collected without parental consent); Stipulated Order for Permanent Injunction, Civil Penalty Judgment & Other Relief, United States v. Amazon.com, Inc., No. 23-cv-00811 (W.D. Wash. July 19, 2023) (stipulating to a permanent injunction resolving charges of failing to delete children's data at the request of parents).

Legislative proposals to amend COPPA, if passed, would augment parental control over youth privacy even as those proposals recognize that minors have privacy interests of their own. Consider the Kids Online Safety and Privacy Act ("KOSPA"), which passed the Senate on July 30, 2024.[35] KOSPA would expand parental control by requiring platforms to give parents tools to control the privacy and account settings of children who are under seventeen years old.[36] In a modest shift away from the parental control model, KOSPA would also require websites and online services to ask thirteen- to seventeen-year-olds themselves (not their parents) for consent before collecting personal information from them.[37] On balance, the bill empowers parents. Senator Richard Blumenthal underscored this point: "Parents are asking for tools and safeguards that give them a measure of control," and KOSPA would give them that "power."[38] In short, proposed amendments to COPPA would give parents "greater control."[39]

Other federal proposals follow in lockstep with the parental control model. The Verifying Kids' Online Privacy Act would extend the rights secured to parents under COPPA to parents whose children are fifteen years old and younger.[40] The AI Shield for Kids Act would require parental consent before a platform could let minors use an "artificial intelligence feature."[41] The Parental Data Rights Act would require social media companies to notify parents when minor children create accounts and enable parents to delete "an account maintained with the social media company by a minor child."[42]

[35] S. 2073, 118th Cong. (2024). For procedural reasons not relevant to the substantive discussion, the Kids Online Safety Act ("KOSA") and the Children and Teens' Online Privacy Act ("COPPA 2.0") were both added to a House amendment to S. 2073, the Eliminate Useless Reports Act of 2024. As a result, the final vote taken was to align the House amendment to S. 2073 as amended by the Senate's addition of KOSA and COPPA 2.0. Id. That newly amended bill was renamed the Kids Online Safety and Privacy Act ("KOSPA"). Title I of KOSPA is KOSA, Title II is COPPA 2.0, and Title III is titled the Eliminating Useless Reports Act. Id.

[36] Id. § 103(a)(1)–(b).

[37] Id. § 201(a)(4).

[38] 170 Cong. Rec. S5562–63 (daily ed. July 30, 2024) (statement of Sen. Richard Blumenthal).

[39] Maya C. Miller, Senate Passes Child Online Safety Bill, Sending It to an Uncertain House Fate, N.Y. Times (July 30, 2024), https://www.nytimes.com/2024/07/30/us/politics/senate-child-online-safety-bill-house.html (quoting Speaker of the U.S. House of Reps. Mike Johnson).

[40] H.R. 7534, 118th Cong. § 2(a) (2024).

[41] S. 1626, 118th Cong. § 2(b) (2023).

[42] S. 564, 118th Cong. § 2(b)(2), (c) (2023); see also Protecting Kids on Social Media Act, S. 1291, 118th Cong. § 5 (2023) (requiring "affirmative consent of a parent or guardian to

As with Congress, state lawmakers see parental control as *the* answer to concerns about children's privacy and online safety. Sponsors of Utah's sweeping youth social media law[43] described the parental privacy control approach as obvious ground truth.[44] The law would have "give[n] full administrator-level access to parents, so that they can see everything that their children are doing, or receiving, or seeing on social media."[45] Parental control is so logical and acceptable, the sponsors argued, that it would be unusual for social media to be treated differently than other areas where parents control minors' activities.[46]

The same is true of state comprehensive data privacy laws, which treat children's data as sensitive and choose parental control as the solution.[47] Some states secure more opportunities for parental control, requiring parental consent for a platform's processing of information *about* children, including but not limited to information collected *from* children, which is the COPPA approach.[48] Other state comprehensive privacy laws

create an account for" anyone under eighteen years old); Sammy's Law of 2023, H.R. 5778, 118th Cong. § 4(a)(1) (requiring social media companies to have "third-party-accessible real-time application programming interfaces" so third-party software providers could monitor and manage the content, interactions, and account settings of youth under seventeen years old on behalf of a parent or guardian).

[43] H.B. 311, 2023 Gen. Sess., Reg. Sess. (Utah 2023) ("Social Media Usage Amendments"); S.B. 152, 2023 Gen. Sess., Reg. Sess. (Utah 2023). After both pieces of legislation were challenged with several lawsuits, see, e.g., Complaint for Declaratory & Injunctive Relief at 37, 39, NetChoice, LLC v. Reyes, No. 23-cv-00911, 2024 WL 3510919 (D. Utah July 22, 2024), the legislature passed S.B. 194, Social Media Regulation Amendments, and H.B. 464, Social Media Amendments, to replace the original legislation. Effective as of October 2024, social media companies must adopt privacy protective defaults for minors (anyone under eighteen) and enable minors to ask companies to delete their personal data. Parental control remains part of the law, but only to the extent that privacy protections afforded to minors cannot be changed without verifiable parental consent. This is an important difference, as Part IV discusses. S.B. 194, 2024 Gen. Sess., Reg. Sess. § 13-71-204 (Utah 2024); H.B. 464, 2024 Gen. Sess., Reg. Sess. (Utah 2024).

[44] Utah Senate Audio (Feb. 13, 2023), supra note 9, at 01:17:00–01:18:42 (statement of Sen. Daniel McCay).

[45] 5 Questions with Family Studies: Clare Morell on Utah's Social Media Law, Inst. for Fam. Stud. (Apr. 17, 2023) [hereinafter 5 Questions with Family Studies], https://ifstudies.org/blog/5-questions-with-family-studies-clare-morell-on-utahs-social-media-law [https://perma.cc/9YKY-WXCY].

[46] Utah Senate Audio (Feb. 13, 2023), supra note 9, at 01:19:34–01:20:04 (statement of Sen. Daniel McCay).

[47] This mirrors the approach of GDPR, which classifies children as particularly "vulnerable" to information economy harms. GDPR, supra note 27, at rec. 75; 2016 O.J. (L 119/37–38) art. 8 (extending parental control to data about children under sixteen years old).

[48] See, e.g., Colorado Privacy Act, Colo. Rev. Stat. §§ 6-1-1301(24)(c), 6-1-1304(7) (2023) (treating children's data as "[s]ensitive" and requiring parental consent before processing

mimic COPPA's requirement of parental consent for information collected *from* children under thirteen years of age.[49]

In sum, the current approach to protecting the privacy of young consumers, embodied in COPPA, new sector-specific proposals, and state comprehensive data privacy laws, operates through the vehicle of parental control. The goal may be to encourage parent-child engagement and to limit data collection without parental consent, as COPPA's sponsors suggested, but that is not the same as protecting youth privacy directly. The next Section finds a similar pattern governing student data and explores how the law secures parental control over student information.

2. Laws and Practices Governing Information About Students

The commitment to parental authority in the student privacy context began in 1974 with the adoption of the Family Educational Rights and Privacy Act ("FERPA").[50] As a condition for federal funding, FERPA

sensitive "data concerning a known child"); Delaware Personal Data Privacy Act, Del. Code Ann. tit. 6, §§ 12D-103(d), 12D-104(b) (2023) (effective Jan. 1, 2025) ("In the case of processing personal data of a known child, the parent or legal guardian may exercise such consumer rights on the child's behalf.").

[49] See, e.g., Connecticut Data Privacy Act, Pub. Act No. 22-15, §§ 4(b), 6(a)(4), 12(a)(3), 2022 Conn. Acts 34, 39, 41, 48 (Reg. Sess.) (requiring parental consent concerning the processing of "sensitive data" about a known child "without processing such data in accordance with COPPA"); Indiana Consumer Data Protection Act, Pub. L. No. 94-2023, art. 15, ch. 4, § 1(5), 2023 Ind. Acts 1050, 1062 (stating that controllers shall not process sensitive data about a known child without processing such data in accordance with COPPA); Iowa Act Relating to Consumer Data Protection, ch. 17, § 4(2), 2023 Iowa Acts 31, 36 (same); Kentucky Consumer Data Protection Act, ch. 72, §§ 2(4), 4(1)(e), 2024 Ky. Acts 389, 393, 395 (same); Maryland Online Data Privacy Act of 2024, ch. 454, §§ 14-4603(C), 14-4605(D)(2), 2024 Md. Laws 16, 18–19 (same); Minnesota Consumer Data Privacy Act, ch. 121, art. 5, § 325O.03, subd. 2(b), 325O.05, subd. 2(b), 2024 Minn. Laws 2160, 2166, 2169 (same); Montana Consumer Data Privacy Act, ch. 681, §§ 4(3), 5(3)(b), 2023 Mont. Laws 2161, 2166 (same); Nebraska Data Privacy Act, §§ 6, 7(1), 2024 Neb. Laws 624, 627–28 (same); New Hampshire Act Relating to the Expectation of Privacy, ch. 5, § 507-H:4(II), -H:6(I)(d), 2024 N.H. Laws 18, 23, 25 (same); New Jersey Data Protection Act, ch. 266, § C.56:8-166.12(9)(a)(4), 2024 N.J. Laws 6–7 (same); Oregon Consumer Data Privacy Act, ch. 369, §§ 2(3)(g), 4(3), 5(2)(b), 2023 Or. Laws 983, 986–88 (same); Tennessee Information Protection Act, ch. 408, §§ 47-18-3203(a)(1), 47-18-3204(a)(6), 2023 Tenn. Pub. Acts 1, 5, 7 (same); Texas Data Privacy and Security Act, ch. 995, §§ 541.005, 541.051(a), 2023 Tex. Gen. Laws 3157, 3162 (same); Utah Consumer Privacy Act, ch. 462, §§ 13-61-202(2), 13-61-302(3)(b), 2022 Utah Laws 3799, 3804–05 (same); Virginia Consumer Data Protection Act, Va. Code Ann. §§ 59.1-576(D), 59.1-577(A), 59.1-578(A)(5) (2025) (same).

[50] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g. In the late 1960s and early 1970s, Congress held extensive hearings on the perils of "databanks" of personal data. Danielle Keats Citron, A More Perfect Privacy, 104 B.U. L. Rev. 1073, 1077 (2024); Barry

requires that schools let parents access children's school records and request corrections.[51] Students, however, do not have the right to access their records until their eighteenth birthday or when they enroll in postsecondary education.[52] Congress paired FERPA with the Protection of Pupil Rights Amendment ("PPRA"), which required schools to obtain parental consent before students complete surveys seeking personal information about students' political views, religion, sexual practices, and more.[53] With the passage of the No Child Left Behind Act,[54] schools must let parents inspect all in-school surveys, not just those created by the Department of Education.[55] Under the maximalist approach of FERPA and PPRA, parents have authority over students' records until children turn eighteen or enroll in postsecondary education.[56]

FERPA and the PPRA grew out of concerns about inaccurate and biased student records.[57] Education journalist Diane Divoky exposed numerous instances where school records pegged children as troublemakers, exhibitionists, and "bed-wetter[s]" and mothers as "alcoholic[s] with many boyfriends."[58] A substitute teacher in Colorado saw her own sixth-grade son's school record, which claimed he had "Marxist tendencies."[59] She had to enlist the ACLU to get the record expunged.[60]

Friedman & Danielle Keats Citron, Indiscriminate Data Surveillance, 110 Va. L. Rev. 1351, 1374–76 (2024).

[51] 20 U.S.C. § 1232g(a)(1)(A), (a)(2).

[52] Id. § 1232g(d); 120 Cong. Rec. 39864–65 (1974).

[53] 20 U.S.C. § 1232h(b).

[54] No Child Left Behind Act of 2001, Pub. L. No. 107-110, 115 Stat. 1425 (2002).

[55] Id. § 1061 (codified as amended at 20 U.S.C. § 1232h(c)(1)(A)(i)).

[56] Aryeh Neier, Dossier: The Secret Files They Keep on You 24 (1975); Lynn M. Daggett, Student Privacy and the Protection of Pupil Rights Act as Amended by No Child Left Behind, 12 U.C. Davis J. Juv. L. & Pol'y 51, 58 (2008).

[57] Fanna Gamal, The Private Life of Education, 75 Stan. L. Rev. 1315, 1326–27 (2023).

[58] Neier, supra note 56, at 17–18. Arthur Miller's foundational work drew attention to computerized school records, whose detailed dossiers of sensitive student information risked becoming "record prison[s]." See Arthur R. Miller, The Assault on Privacy: Computers, Data Banks, and Dossiers 7, 50, 112–14 (1971). He warned educators that "sensitive data derived from an easily accessible and often naive student population may be used to the prejudice of the file subjects." Id. at 113. School dossiers create the "risk of stereotyping or classifying [children] in a way that detrimentally affects their educational development or societal mobility." Id. at 114. School dossiers would be "dangerous if preserved for too long" especially if "material is inaccurate or projects a derogatory image of the child." Id. at 112. Those records could follow children into adulthood, damaging their life chances. Id. at 4–7.

[59] Neier, supra note 56, at 17.

[60] Id.

Lawmakers wanted parents to have the ability to check and ask to correct the personal information that schools were collecting and storing about their children. Senator James Buckley of New York introduced FERPA as an amendment to federal education law,[61] pointing to instances where parents were barred from reviewing children's school records. He noted the growing trend of students answering surveys about their personal views, family, and home life without parental consent.[62] Senator Buckley viewed parents as "the first and most important teachers of their children"; he was chagrined by the notion that educators—"entrust[ed]" only for "basic educational purposes"—could simply disregard the "values and beliefs and opinions of the parents . . . [who] have the primary natural, legal and moral responsibility for the upbringing of their children."[63] He said the goal of FERPA was "to restore parental rights and to protect privacy."[64] Senator Buckley's floor remarks emphasized parental control as the obvious (and only) policy choice.

FERPA passed the Senate by a voice vote,[65] cleared the House on July 31, 1974, with little opposition,[66] and became federal law later that year.[67] Just four years later, FERPA was expanded under the auspices of another "parental control" amendment.[68] This amendment focused on psychological surveys, which were increasingly being administered by schools as part of new data-driven educational practices. Senator Orrin Hatch, the amendment sponsor, echoed Senator Buckley when he argued that it was a "travesty" for schools to administer psychological surveys without written parental consent.[69] The "travesty" was the lack of parental control, not the surveys themselves.

Since the 1970s, parental control over students' information has been the accepted regulatory approach. A key difference today is the breadth of youth data included in school records. Pursuant to FERPA, schools

[61] 120 Cong. Rec. 14579–81 (1974).
[62] Id. at 14581, 14585–88, 14597.
[63] 121 Cong. Rec. 13991 (1975).
[64] 120 Cong. Rec. 14581 (1974).
[65] Notably, Senator Buckley conceded to dividing his proposed FERPA amendment, such that the more contentious subsection (b)—requiring parental consent for psychological assessments and experimental studies—could be voted on separately. That subsection was defeated by a 40-43 vote. 120 Cong. Rec. 14594–95 (1974); 121 Cong. Rec. 13991 (1975).
[66] 120 Cong. Rec. 26128 (1974).
[67] Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, § 513, 88 Stat. 571, 571.
[68] Education Amendments of 1978, Pub. L. No. 95-561, § 1250, 92 Stat. 2143, 2355–56.
[69] 124 Cong. Rec. 26681–82 (1978).

may designate third-party vendors as "school official[s]" to help them provide institutional services.[70] On that basis, thousands of K-12 public schools have contracted with surveillance companies to scan students' laptop activities (emails, chats, browsing, searches, and files) for "problematic" activities like bullying, self-harm, and safety threats.[71] During the 2021–2022 school year, eighty-nine percent of surveyed teachers reported that monitoring software was installed on students' school-issued and/or personal devices.[72] Schools may consent to vendors' collection of student data on parents' behalf, satisfying COPPA, so long as the collection is exclusively for the school's benefit.[73] Many of those same surveillance companies also offer parental control apps that track children's locations and provide alerts about potential problems.[74]

Some states have reinforced the commitment to parental control by requiring schools to include those commitments in their contracts with vendors. For instance, New York's education law required the development of a statewide "Parents' Bill of Rights for Data Privacy and Security," which promises parents that "[e]ducational agency contracts with vendors . . . receiv[ing Personally Identifiable Information] will address statutory and regulatory data privacy and security requirements."[75]

[70] 34 C.F.R. § 99.31(a)(1)(i)(B) (2025). Schools have wide latitude to decide if outside parties count as school officials; they are not required to document disclosure to third parties. Elana Zeide, Student Privacy Principles for the Age of Big Data: Moving Beyond FERPA and FIPPs, 8 Drexel L. Rev. 339, 360–61 (2016).

[71] Citron, Surveilled Student, supra note 15, at 1450–53.

[72] Elizabeth Laird, Hugh Grant-Chapman, Cody Venzke & Hannah Quay-de la Vallee, Ctr. for Democracy & Tech., Hidden Harms: The Misleading Promise of Monitoring Students Online 7–8 (2022). The most surveilled students are students from vulnerable backgrounds. A national survey showed that six in ten Hispanic students, six in ten Black students, seven in ten rural students, and seven in ten students from low-income families rely on school-issued devices. Id. at 23.

[73] Sara Kloek, Student Data Privacy in the United States, *in* Children's Privacy and Safety, supra note 29, at 123, 135. Schools have notified parents about surveillance software in a haphazard manner. Elizabeth Warren & Ed Markey, Constant Surveillance: Implications of Around-the-Clock Online Student Activity Monitoring 3 (2022), https://www.warren.senate.gov/imo/media/doc/356670%20Student%20Surveillance.pdf [https://perma.cc/92N6-55K9]. According to researchers, one in five parents does not know if their school uses student monitoring software. Laird et al., supra note 72, at 17.

[74] Bark is a dominant provider of student monitoring services; it offers parental monitoring apps. See Bark, https://www.bark.us/bark-app/ [https://perma.cc/9KW7-66SU] (last visited Aug. 29, 2025).

[75] Education Law § 2-D Parents' Bill of Rights for Data Privacy and Security (2024), https://www.nysed.gov/sites/default/files/programs/data-privacy-security/parents-bill-of-rights-8.28

States are also extending parental control to school-provided mental health services. For example, Florida's new parental rights law "reinforce[s] the fundamental right of parents to make decisions regarding the upbringing and control of their children" by requiring parental consent before schools can provide services concerning the "student's mental, emotional, or physical health or well-being."[76] Idaho and Kentucky require similar notification and consent from parents before children can use any school health and wellness service.[77]

These laws and proposals lead directly to corporate practices that put parents in charge of youth access to online spaces. These laws and practices require that parents assume the burden of providing verified consent to prior approval. That burden-shifting, however, is not the same as protecting youth privacy and safety.

The next Section explores how scholars have not meaningfully wrestled with the parental control model undergirding youth privacy law. Whether by overlooking young people's absence from privacy laws or recognizing and accepting the parental control model with subtle improvements, there has been too little interrogation of the prevailing approach.

B. Scholarly Blind Spots on Youth Privacy

Given the near universality of parental control over youth privacy, most privacy scholars either collapse the two concepts by equating parental control with youth privacy protection or recognize parental control and accept it. These approaches have precluded a deep interrogation of youth privacy law and whether parental control actually contributes to youth privacy.

Some privacy policy and scholarship conflate the means (parental control) with the ends (youth privacy). The FTC falls into this trap.[78] So

.24_0.pdf [https://perma.cc/8FJB-HAPA]; accord N.Y. Educ. Law § 2-d(3) (McKinney 2024) (detailing the parents bill of rights and vendor obligations when retaining personally identifiable information).

[76] Fla. Stat. Ann. § 1001.42(8)(c)(1) (West 2025).

[77] Idaho Code § 33-6001(3), (5) (2023); Ky. Rev. Stat. Ann. § 158.191(2) (West 2023).

[78] Speaking in support of changes to the FTC's COPPA Rule, then-FTC Chair Lina Khan stated that the rule "strengthens key protections for kids' privacy online . . . [b]y requiring parents to opt in to targeted advertising practices." Press Release, Fed. Trade Comm'n, FTC Finalizes Changes to Children's Privacy Rule Limiting Companies' Ability to Monetize Kids' Data (Jan. 16, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finali

do scholars who describe COPPA as protecting children's privacy by regulating the handling of their data.[79] COPPA, however, does not do that, at least not directly. COPPA secures parental involvement in children's online activities and conditions data collection on parental consent.[80] Whether parental involvement protects children's privacy is a second-order question. When scholars collapse youth privacy into parental control, they cannot interrogate the daylight between them.[81]

Another strand of privacy scholarship separates youth privacy from parental control and endorses the parental control approach. Anita Allen notes that COPPA "confers legal power over children to parents or other adult guardians, enabling paternalistic and authoritarian intervention . . . designed to" make "the knowledge and consent of their parents" a prerequisite for children's use of digital services.[82] Allen argues that COPPA's "powerful right [of parents] to veto" a website's handling of children's data is "clearly needed" because children are irresponsible and thus may jeopardize their families' privacy.[83] Allen was early to warn that teenagers over COPPA's thirteen-year-old threshold would still "recklessly disclose personal information"[84] and endorsed

zes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data [https://perma.cc/SJU2-8WNF].

[79] E.g., Dan Feldman & Eldar Haber, Measuring and Protecting Privacy in the Always-On Era, 35 Berkeley Tech. L.J. 197, 215 (2020).

[80] See supra Subsection I.A.1.

[81] Elana Zeide argues that FERPA "regulates the disclosure of student information . . . on a model that, theoretically, provides parents *and students* with control." Zeide, supra note 70, at 342 (emphasis added). FERPA's cosponsor Senator Buckley, she asserts, sought to provide "parents *and students* with more notice of and control over disclosure." Id. at 355 (emphasis added). But FERPA imposes parental control over student records until children have effectively become adults. Id. at 356. Fanna Gamal argues that to achieve the important anti-racist goal of protecting against inaccurate, biased, and troubling "dirty data" in student records, FERPA should be amended to allow "parents [to] appeal documenting decisions to a neutral, third-party actor outside of schools, or be permitted to appeal a documentation decision to a panel of educators and parents with no connection to the student's home school district." Gamal, supra note 57, at 1336, 1359–60 (citation omitted). Given the failure to disaggregate parental control from youth privacy, Gamal sees parents as part of the solution.

[82] Anita L. Allen, Unpopular Privacy: What Must We Hide? 186 (2011) [hereinafter Allen, Unpopular Privacy]; see also Elana Zeide, Student Privacy's Student Neglect: Toward a Student-Centric Paradigm, 93 Geo. Wash. L. Rev. 535, 540 (2025) (acknowledging that "'student privacy' statutes rarely grant rights to students").

[83] Allen, Unpopular Privacy, supra note 82, at 178–79. As Allen explained, invading children's privacy to find out if they are making poor choices or engaging in unsafe behavior "can be a matter of responsible parenting." Anita L. Allen, The Virtuous Spy: Privacy as an Ethical Limit, 91 Monist 3, 6–7 (2008).

[84] Allen, Unpopular Privacy, supra note 82, at 182.

efforts to extend parental consent requirements to cover older youth, as we now see in recent legislative proposals.

A third strand of privacy scholarship fails to tackle parental authority at all. Acknowledging the potential for divergence between parents' and children's interests regarding student records, Elana Zeide would not upset the prevailing balance of power between parents, children, and tech companies.[85] Instead, she proposes that schools bear fiduciary duties to students. On the one hand, this would allow them to challenge practices that undermine student privacy. On the other hand, schools already leverage the fiduciary-like rhetoric and responsibilities of *in loco parentis* to justify indiscriminate student surveillance in the name of protecting children from safety risks.[86] Given that background, the parental control model would in effect remain undisturbed.

None of these scholars sufficiently interrogate the rationales for subsuming young people's rights under some other authority, whether it be parents or schools. The next Part fills that gap by excavating the underlying rationales for the parental control model.

II. UNDERSTANDING PARENTAL CONTROL

This Part explains *why* youth privacy law treats parents as the sole privacy authorities for their children and surfaces the underlying logics of the parental control model. We begin with the reliance on childhood development insights about youth immaturity and vulnerability. We

[85] Zeide, supra note 82, at 540, 542. Zeide's policy recommendation—the recognition of "information fiduciar[ies]"—would make schools stewards rather than simple controllers of student data. Id. at 600–01. This approach sits in a scholarly tradition. One of us (Citron) has recommended fiduciary-like regulation for companies amassing intimate information. See Citron, Fight for Privacy, supra note 13, at 156–65 (proposing to treat companies amassing personal data as data guardians with robust duties). The other (Waldman) has suggested that the law of privacy should learn from fiduciary law and protect as private information that is shared in contexts of trust. Waldman, Privacy as Trust, supra note 20, at 62–75; see also Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age 103 (2004) (arguing that the law should conceive of companies that collect and use our personal information as being in a fiduciary relationship with us); Neil Richards & Woodrow Hartzog, A Duty of Loyalty for Privacy Law, 99 Wash. U. L. Rev. 961, 964–65 (2021) (same); Jack M. Balkin, Information Fiduciaries and the First Amendment, 49 U.C. Davis L. Rev. 1183, 1186 (2016) (same); Jack M. Balkin & Jonathan L. Zittrain, A Grand Bargain to Make Tech Companies Trustworthy, The Atlantic (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/ (same).

[86] Citron, Surveilled Student, supra note 15, at 1454, 1463, 1465–66.

connect those rationales to legal doctrines in consumer privacy law. We then turn to social norms that valorize parental control as best for families.

A. Developmental Perspective

A key justification for the parental control model is that young people cannot protect their own privacy interests. The reasoning goes like this: young people are too immature to understand the consequences of online activities, too vulnerable to withstand corporate manipulation, and too irresponsible to care about either.[87] As a result, the argument continues, parents must care about it for them.

The backdrop for this perspective is critical to foreground: U.S. lawmakers and advocates have embraced the view that privacy law should be driven by individual notice, control, and participation.[88] This raises a threshold question: Do young people have the capacity to exercise those rights? Traditionally, the answer has been no. Testimony and statements from lawmakers and advocates highlight the concern that youth lack the maturity necessary to make sound judgments about their personal data.

In the debates about COPPA, industry lobbyists and consumer advocates had few points of agreement beyond the conclusion that a notice-and-choice approach would not work for children as they cannot make "complex judgments."[89] The Clinton White House supported measures enabling "parental choice" because children "lack the cognitive ability to recognize and appreciate privacy concerns."[90] As Anita Allen explains, COPPA's parental control model grew out of the view that families needed protection from "the immature preferences of children" with "poor judgment[]" whom website operators could trick and for whom "music and sweets [were] more important . . . than electronic information privacy and data protection."[91] The FTC's early approach to

[87] See Allen, Unpopular Privacy, supra note 82, at 177.

[88] We discuss that legal framing—notice (transparency), choice (consent), and other rights—in more detail later on in this Part.

[89] Kathryn C. Montgomery, Generation Digital: Politics, Commerce, and Childhood in the Age of the Internet 81–82 (2007).

[90] William J. Clinton & Albert Gore, Jr., The White House, A Framework for Global Electronic Commerce 18 (1997); see also 144 Cong. Rec. S8483 (daily ed. July 17, 1998) (statement of Sen. Richard Bryan) ("The Internet offers unlimited potential for assisting our child's growth and development. However, we must not send our children off on this adventure without proper guidance and supervision.").

[91] Allen, Unpopular Privacy, supra note 82, at 177, 188; see also 144 Cong. Rec. S8482 (daily ed. July 17, 1998) (statement of Sen. Richard Bryan) ("Web sites were using games,

children's privacy was also based on the view that maturity must precede the recognition of privacy rights.[92]

Lawmakers and advocates have continued to emphasize youth immaturity and vulnerability as a key rationale for laws empowering parents. When discussing the Protecting Kids on Social Media Act, which would require parental consent for youth under seventeen to create social media accounts, Senator Brian Schatz underscored that powerful corporate algorithms would overwhelm a child's developing brain.[93] Representative Debbie Wasserman Schultz argued in favor of parental control over children's use of social media because the "most vulnerable stages of a child's life" are at stake.[94] The Utah social media law's legislative findings state that individuals who are under eighteen "have less awareness of the risks, consequences, and safeguards related to a social media company's processing of minors' personal data."[95]

Advocates underscore children's immaturity in supporting parental control measures.[96] Common Sense Media's founder James P. Steyer explained, "Children and teens are uniquely vulnerable on social media and other internet platforms . . . [because t]heir brains are still developing. They are impulsive and prone to oversharing . . . . Young children do not understand the consequences of such sharing . . . ."[97] Samir Jain, Vice

contests, and offers of free merchandise to entice children to give them exceedingly personal and private information about themselves and their families. Some even used cartoon characters who asked children for personal information, such as a child's name and address and e-mail address, date of birth, telephone number, and Social Security number.").

[92] Montgomery, supra note 89, at 84, 90–91, 96–97 (describing the FTC's focus on parental consent due to perceived youth vulnerability).

[93] Deirdre Walsh, Bipartisan Senators Predict Parents Will Overcome Tech Lobby to Protect Kids Online, NPR (May 5, 2023, 5:00 AM), https://www.npr.org/2023/05/05/1173683051/bipartisan-senators-predict-parents-will-overcome-tech-lobby-to-protect-kids-onl [https://perma.cc/ZHA6-M5AN].

[94] Press Release, Off. of Rep. Buddy Carter, Wasserman Schultz, Carter, Schrier, Miller-Meeks Introduce Social Media Child Safety Bill (Dec. 5, 2023), https://buddycarter.house.gov/news/documentsingle.aspx?DocumentID=11533 [https://perma.cc/NA5Q-UM8S].

[95] Utah Code Ann. § 13-71-102(8) (West 2024).

[96] Much like lawmakers, advocates accept this legal framing of individual choice and control, as explored more fully below.

[97] Holding Big Tech Accountable: Targeted Reforms to Tech's Legal Immunity: Hearing Before the Subcomm. on Commc'ns & Tech. of the H. Comm. on Energy & Com., 117th Cong. 4 (2021), https://democrats-energycommerce.house.gov/sites/evo-subsites/democrats-energycommerce.house.gov/files/documents/Witness%20Testimony_Steyer_2021.12.01.pdf [https://perma.cc/3LLZ-9BJV] (statement of James P. Steyer, CEO & Founder, Common Sense Media); see also Maryland Senate Finance Committee, FIN Committee Session, 2/14/2024 #1, at 06:27:12 (YouTube, Feb. 14, 2024) [hereinafter Maryland Senate Finance

President of the Center for Democracy and Technology, noted that "[kids] don't understand or appreciate . . . the ways they may be victimized."[98] When endorsing the parental control model in state social media laws, family law scholars point to childhood as a unique time of "vulnerability" and "inevitable dependency," which make adolescents prone to being "impulsive, reckless, vulnerable to peer pressure, and in possession of more transitory personality traits."[99] Parents step in during that time of dependency.

Developmental rationales for parental control rest on the assumptions that decision-making maturity is a necessary precondition of privacy authority and that young people lack that maturity. Under that view, young people are only capable of making sound privacy-related choices once they fully develop a sense of self and demonstrate the ability to make informed choices.[100] These developmental rationales translate into binary age designations under COPPA and FERPA—youth either fall above or below the age of supposed maturity at which they develop the capacity to make informed privacy choices.

The next Section dives deeper into the law's rationales and explanations for parental control, focusing on privacy law and its persistent adherence to the fiction of rational choice at scale.

Committee Video], https://www.youtube.com/watch?v=Nq6ApUJKGcc [https://perma.cc/4FUJ-2YL5] (statement of Beth Jarrett) (arguing that parental control is essential because children "do not yet understand the impact of their online presence").

[98] Legislative Solutions to Protect Kids Online and Ensure Americans' Data Privacy Rights: Hearing Before the Subcomm. on Innovation, Data & Com. of the H. Comm. on Energy & Com., 118th Cong., at 01:10:37 (YouTube, Apr. 17, 2024) [hereinafter Legislative Solutions Hearing], https://www.youtube.com/watch?v=li_-czubkbw&t=4s [https://perma.cc/U9M8-DYPV] (statement of Samir Jain, Vice President of Pol'y, Ctr. for Democracy & Tech.).

[99] Katharine Silbaugh & Adi Caplan-Bricker, Regulating Social Media Through Family Law, 15 U.C. Irvine L. Rev. 1, 21–22 (2024). Those character traits "last[] through the mid-twenties" because children's brains, personalities, and cognitive abilities are still developing well beyond the teenage years. Id. at 24; see also id. at 22 n.121 (citing Nat'l Acads. of Scis., Eng'g & Med., The Promise of Adolescence: Realizing Opportunity for All Youth 1 (2019) (describing adolescence as a "critical period of development")).

[100] See, e.g., Harold M. Proshansky & Abbe K. Fabian, The Development of Place Identity in the Child, *in* Spaces for Children: The Built Environment and Child Development 21, 29–30, 36 (Carol Simon Weinstein & Thomas G. David eds., 1987) (linking psychological development to children's ability to make privacy-related decisions); see also Alan P. Bates, Privacy—A Useful Concept?, 42 Soc. Forces 429, 429–31 (1964) (arguing that self-consciousness is necessary for understanding the concept of privacy).

B. Privacy Law

Patterns in privacy law support giving parents authority over children's privacy interests. Privacy law's "notice-and-consent" framework is premised on decision-making rationality, something that children presumably do not possess and that adults presumably do. Privacy law also has a history of privileging parental rights when they conflict with children's privacy interests.

1. The Effect of Notice-and-Consent

Parental control is reinforced by the notice-and-consent regime at the heart of much U.S. privacy law. Under that regime, digital platforms must post privacy policies notifying consumers about their data-handling practices;[101] consumers then consent to or are presumed to have consented to those practices.[102] The notice-and-consent regime operates via click-to-agree buttons (that people obligingly click), opt-out mechanisms (that are hardly used), and long privacy policies (that no one reads).[103]

The notice-and-consent approach presumes decision-making rationality, wherein people read a company's privacy policy, understand the trade-offs involved in sharing personal data, weigh the pros and cons, and act accordingly.[104] Rationality is a foundational principle in the

[101] As required by the California Online Privacy Protection Act of 2003. Cal. Bus. & Prof. Code § 22575 (West 2004).

[102] See, e.g., Daniel J. Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 Colum. L. Rev. 583, 600–06, 628–30 (2014) (detailing how the FTC constructed its Section 5 enforcement framework as consistent with the existing self-regulatory notice-and-consent approach to consumer privacy). But see Joel R. Reidenberg, N. Cameron Russell, Alexander J. Callen, Sophia Qasir & Thomas B. Norton, Privacy Harms and the Effectiveness of the Notice and Choice Framework, 11 I/S: J.L. & Pol'y for Info. Soc'y 485, 490–96 (2015) (critiquing the notice-and-comment regime). When companies' practices deviate from statements in their privacy notices or mislead consumers via omission, they put themselves at risk of FTC or state attorney general investigation for deceptive practices. Solove & Hartzog, supra, at 628–36 (describing the FTC's theories of enforcement for deceptive trade practices); Danielle Keats Citron, The Privacy Policymaking of State Attorneys General, 92 Notre Dame L. Rev. 747, 763–71 (2016) [hereinafter Citron, Privacy Policymaking] (describing the efforts of state attorneys general to enforce broken consumer privacy promises).

[103] See Ari Ezra Waldman, The New Privacy Law, 55 U.C. Davis L. Rev. Online 19, 22 (2021) [hereinafter Waldman, The New Privacy Law]; George R. Milne & Mary J. Culnan, Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices, 18 J. Interactive Mktg. 15, 15 (2004).

[104] Ari Ezra Waldman, Cognitive Biases, Dark Patterns, and the "Privacy Paradox," 31 Current Op. Psych. 105, 105 (2020).

privacy literature,[105] and it remains a bedrock assumption among regulators and policymakers.[106]

This approach puts children on the outside of privacy law looking in. As supporters of the parental control model emphasize, young people cannot make rational decisions because they lack emotional maturity and intellectual capacity.[107] Since privacy law puts the onus on individuals to make informed decisions—by reading privacy policies and making choices—anyone who lacks the capacity for rational decision-making must have those decisions made for them.

Without a doubt, privacy law did not have to develop this way; the foundations of notice-and-consent were erected during a time of anti-regulatory fervor that valorized individual autonomy and free markets.[108] But since current privacy law on the books demands rationality, the parental control model logically followed suit.

2. The Effects of Privacy Tort Law

Privacy tort law also has a history of prioritizing parental decisions over children's privacy interests. In *Sidis v. F-R Publishing Corp.*,[109] former "child prodigy" William James Sidis sought in adulthood to "live as unobtrusively as possible."[110] The U.S. Court of Appeals for the Second Circuit ruled that despite a decades-long effort to remain out of

[105] Opinion Surveys: What Consumers Have to Say About Information Privacy: Hearing Before the Subcomm. on Com., Trade & Consumer Prot. of the H. Comm. on Energy & Com., 107th Cong. 14 (2001) (statement of Alan F. Westin, President, Priv. & Am. Bus.). Alan Westin argued that consumers could be categorized as privacy "[f]undamentalists," "[u]nconcerned," or "[p]ragmatists" who made different yet rational choices based on how much they cared about privacy and the invasiveness of online activities. Id. at 14–16; see also Richard A. Posner, The Right of Privacy, 12 Ga. L. Rev. 393, 397 (1978) (articulating economic analysis of privacy as a weighing of pros and cons prior to disclosure).

[106] See, e.g., Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 62 (2012) ("[P]rivacy statements should contain some standardized elements . . . to allow consumers to compare the privacy practices of different companies . . . ."); Facebook, Social Media Privacy, and the Use and Abuse of Data: Joint Hearing Before the S. Comm. on Com., Sci. & Transp. & the S. Comm. on the Judiciary, 115th Cong. 3 (2018) (statement of Sen. John Thune, Chairman, S. Comm. on Com., Sci. & Transp.) ("[B]oth sides of the bargain need to know the stakes that are involved. Right now, I am not convinced that Facebook users have the information that they need to make meaningful choices.").

[107] See supra Section II.A.

[108] Waldman, The New Privacy Law, supra note 103, at 19, 22 (highlighting the deregulatory, classically liberal origin of early consumer privacy laws).

[109] 113 F.2d 806 (2d Cir. 1940).

[110] Id. at 807.

the public eye as an adult, Sidis could not obtain redress from *The New Yorker* after it published a "Where Are They Now?"-style biography.[111] While *Sidis* is often read as a case about the conflict between the public's right to know and an individual's right to privacy, it is also a case about parents and children.[112]

Sidis sued *The New Yorker* for invading his privacy, arguing that the magazine's exposé about his thoughts and activities, drawn from conversations in his home, amounted to a breach of the private life that he had carefully cultivated in adulthood.[113] As a child, Sidis was thrust into the limelight by his parents Boris and Sarah, who talked to the media about his intellectual feats (including his ability to read at eighteen months and to speak eight languages at six years old).[114] His parents pointed to their child's unusual abilities as proof of their exceptional child-rearing skills.[115] Newspapers and magazines covered his graduation from college at sixteen, his university teaching at seventeen, and his attendance at law school before dropping out at nineteen.[116] From his twenties onward, Sidis tried to escape his over-exposed past, doing whatever he could to live a private life because he "hated" that he had become a "household name."[117] He begged the press to leave him alone.[118] He largely succeeded

[111] Id at 807–08, 810; see also Jared L. Manley, Where Are They Now?, New Yorker, Aug. 14, 1937, at 22, https://archives.newyorker.com/newyorker/1937-08-14/flipbook/022/.

[112] Indeed, this is how the writer of the article, James Thurber—who wrote under the pseudonym Jared Manley—saw the situation, and he aimed to warn parents about the downsides of exposing children's intimate lives to the public. Amy Wallace, The Prodigy: A Biography of William James Sidis, America's Greatest Child Prodigy 228, 236 (1986) (explaining Thurber's view that what he thought stood out from his story was his "sincere feeling that the piece would help to curb the great American thrusting of talented children into the glare of fame or notoriety, a procedure in so many cases disastrous to the later career and happiness of the exploited youngsters" (citation omitted)). And yet Thurber effectively erased the child at issue in the story—the young William James Sidis.

[113] Morris L. Ernst & Alan U. Schwartz, Privacy: The Right to Be Let Alone 181–83 (1962).

[114] Meet William James Sidis: The Smartest Guy Ever?, NPR (Jan. 23, 2011, 2:44 PM) [hereinafter Meet William James Sidis], https://www.npr.org/2011/01/23/132737060/meet-william-james-sidis-the-smartest-guy-ever [https://perma.cc/H5LU-AC7E].

[115] Wallace, supra note 112, at 52 (detailing the opinion of Dr. Boris Sidis, William's father, that his education of his son, rather than heredity, helped William develop his "hidden energy").

[116] Id. at 106, 112–14, 125, 135.

[117] Meet William James Sidis, supra note 114 (quoting Amy Wallace); accord Ernst & Schwartz, supra note 113, at 182.

[118] Amy Gajda, Seek and Hide: The Tangled History of the Right to Privacy 158 (2022).

until *The New Yorker* sent a female reporter to pose as a friend of a friend to learn intimate details about his (now-adult) life.[119]

Acknowledging that Sidis was thrust into the public light against his will as a child and that he "loathed [the] public attention," the court nevertheless refused to recognize his privacy tort claim.[120] The court underscored that whatever privacy Sidis wanted and claimed as an adult, the public's lingering interest in "whether or not he had fulfilled his earl[ier] promise" doomed his privacy claim.[121]

The decision is a testament to the lasting power parents have over their children's privacy. That Sidis was "once a public figure . . . [who] excited both admiration and curiosity" was his parents' choice.[122] The decisions that his parents made to publicize his life when he was a young child determined the privacy that Sidis could later claim when he was an adult. Although Sidis was "neither politician, public administrator, nor statesman"[123]—namely, the kind of public figure that traditionally might merit narrower privacy rights in the public interest[124]—his parents' choices prevailed into adulthood.

This approach retains its force today. For example, a school administrator's interest in telling a student's parents that their child had been disciplined for kissing a student of the same sex was found to outweigh the student's privacy right to keep their sexual orientation from their parents.[125] According to David Meyer, this kind of decision is typical; judges may recognize that children have constitutional rights, but they rarely and "haltingly" accept that those rights prevail over their parents' interests.[126] This privileging of parental authority puts Sidis's modern-day equivalents at risk. In an era of extensive "sharenting" on social media, where parents disclose intimate details about their

[119] Meet William James Sidis, supra note 114.
[120] Sidis v. F-R Publ'g Corp., 113 F.2d 806, 807–09 (2d Cir. 1940).
[121] Id. at 809.
[122] Id.
[123] Id.
[124] See Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193, 214–16 (1890) (discussing the relationship between the right to privacy and "publication of matter which is of public or general interest" for both private and public figures).
[125] Nguon v. Wolf, 517 F. Supp. 2d 1177, 1195 (C.D. Cal. 2007).
[126] David D. Meyer, The Modest Promise of Children's Relationship Rights, 11 Wm. & Mary Bill Rts. J. 1117, 1117–18 (2003).

children's lives, those children may have little to no recourse for their parents' invasions of their privacy.[127]

Therefore, legal doctrines central to privacy law seem to support the parental control model. As the next Section shows, lawmakers and advocates for parental authority also rely on societal interests in the family unit to justify their position.

C. Societal Interests in Parental Control

Family welfare concerns animate support for the parental control model. Arguments grow out of traditional understandings of family values and contemporary notions of good parenting.

1. Family Values

Some lawmakers and advocates view parental control as essential to protecting the integrity of the family. Under this view, because the family needs privacy, parents must be equipped to protect it.[128] Arguments about family privacy are premised on concerns about the "sanctity" of the family unit.[129]

Consider remarks made in support of a Utah social media law that required anyone under eighteen to obtain parental consent before creating

[127] See, e.g., Naomi Cahn, Maxine Eichner & Mary Ziegler, Children at Work, Parental Rights—and Rhetoric, 77 Ark. L. Rev. 257, 258 (2024); Stacey B. Steinberg, Sharenting: Children's Privacy in the Age of Social Media, 66 Emory L.J. 839, 839, 868–75 (2017). For a heartbreaking case in point, see Shari Franke, The House of My Mother: A Daughter's Quest for Freedom 53 (2025) (explaining that she had no choice but to appear on her mother's family vlog in her early teen years and asking, "What are the lasting repercussions of growing up on camera, without any say in the matter? How does that constant exposure shape a child's sense of self, their future relationships, their very understanding of privacy?").

[128] See Clare Morell, Adam Candeub, Jean Twenge & Brad Wilcox, Inst. for Fam. Stud. & Ethics & Pub. Pol'y Ctr., Protecting Teens from Big Tech: Five Policy Ideas for States 7 (2022), https://ifstudies.org/ifs-admin/resources/final-ifs-eppc-protectingteensfrombigtech-aug2022.pdf [https://perma.cc/6WUJ-Q6HG] (arguing that states should "[m]andate [f]ull [p]arental [a]ccess to [m]inors' [s]ocial [m]edia [a]ccounts" so parents "know exactly what their child is doing online, who they are interacting with, [what] direct messages they are exchanging, and what they are posting and seeing," thus enabling parents to protect the family).

[129] Moore v. City of East Cleveland, 431 U.S. 494, 503 (1977) (plurality opinion). It is true that not all arguments for family privacy are the same. See, e.g., Dorothy E. Roberts, Punishing Drug Addicts Who Have Babies: Women of Color, Equality, and the Right of Privacy, 104 Harv. L. Rev. 1419, 1425 (1991) (arguing that state intervention into poor Black women's reproductive rights can violate the family's right of privacy by "impos[ing] a standard of motherhood that is offensive to principles of both equality and privacy").

a social media account.[130] The law's cosponsor, Representative Jordan Teuscher, emphasized that solutions to social media harms must "happen within the home."[131] In other words, the locus of the privacy interest is the family at home. The Institute of Family Studies, whose work inspired the law, explained that the law secured "famil[y] . . . authority over their technologies."[132]

Similar sentiments have been expressed by federal lawmakers. Senator Edward Markey likened his support for parental oversight over children's online activities to his mother's refusal to answer the doorbell when salesmen rang: "[T]hat same sense of privacy is still present in American families, in America's mothers and fathers. They don't want strangers in their living rooms, in their kitchens, in their bedrooms, with their children."[133] The remarks of state and federal lawmakers converge on the views that the family unit needs privacy and that parents must be given the means to protect it.

Along these lines, parental control is viewed as necessary to protect against youthful indiscretion that might undermine the family's reputation and safety. When testifying on behalf of Utah's social media law, Katie Hawes, Director of the State Attorney General's Consumer Protection Division, warned that kids are prone to sharing information that would "create risks" by revealing "who you are as a family."[134] Under this view, parental control is essential to stop children from exposing "sensitive information about the entire family."[135]

---

[130] Recent amendments to that law removed the parental consent provision. H.B. 464, 2024 Gen. Sess., Reg. Sess. (Utah 2024). An accompanying amendment now includes verified parental consent to change any privacy-protective defaults for anyone under eighteen years old, which is a significant change. Utah Code Ann. § 13-71-204(1) (West 2024).

[131] Utah House of Reps., House Floor Audio on H.B. 464, Day 37, 2024 Gen. Sess., at 02:10:22 (Feb. 22, 2024), https://le.utah.gov/av/floorArchive.jsp?markerID=126885 [https://perma.cc/ZL4U-JU3S] (statement of Rep. Jordan D. Teuscher).

[132] 5 Questions with Family Studies, supra note 45.

[133] 170 Cong. Rec. S5565 (daily ed. July 30, 2024) (statement of Sen. Edward Markey).

[134] Utah Senate, Social Media Regulation Amendments: Hearing on S.B. 194 Before the H. Judiciary Comm., 2024 Gen. Sess., at 18:13 (Feb. 26, 2024), https://le.utah.gov/av/committeeArchive.jsp?mtgID=19186 [https://perma.cc/J8G7-GRPC] (statement of Katie Hawes, Dir., State Att'y Gen. Consumer Prot. Div.).

[135] Utah Senate, Social Media Regulation Amendments: Hearing on S.B. 194 Before the S. Bus. & Lab. Comm., 2024 Gen. Sess., at 23:55 (Feb. 14, 2024), https://le.utah.gov/av/committeeArchive.jsp?mtgID=19200 [https://perma.cc/S7BR-UYF3] (statement of Serge Jorgensen, Partner, Sylint Grp.); see also Utah Senate, Senate Floor Audio on S.B. 194, Day 35, 2024 Gen. Sess., at 16:29 (Feb. 20, 2024), https://le.utah.gov/av/floorArchive.jsp?markerID=126525 [https://perma.cc/YCH4-SW8G] (statement of Sen. Michael McKell) (describing the

2. The Surveillance Imperative of "Good" Parenting

The parental control model is viewed as integral to responsible parenting. Senator Bill Cassidy argued that requiring companies to give parents the ability to control children's online behavior "will give the parents the peace of mind to know their child is safer . . . . Anyone with children knows that they would do anything to protect those children."[136] Representative John James underscored that enabling parental tracking of children's digital activities would democratize effective parenting because "not every parent, not every socioeconomic status, has the time in the day to look over their kid's shoulders twenty-four hours a day."[137]

Lawmakers have a receptive audience for these arguments: parents with sufficient income are subscribing to surveillance services.[138] Surveillance companies market parental control tools as crucial to limiting youth access to dangerous sites that would harm "unsuspecting families"[139] and detecting hints of danger and self-harm.[140] Cellphone services offer physical location tracking so parents "will always know where [their children] are."[141] PC Tattletale warns parents that "even if they are not supposed to, we all know that your child WILL go online unsupervised if they think that no one will find out!"[142] This market is energized by what one of us (Citron) has called "Spying Inc.," an

importance of obtaining parental consent before social media companies collect children's personal data); 170 Cong. Rec. S5565 (daily ed. July 30, 2024) (statement of Sen. Edward Markey) (comparing family privacy from online marketers today to family privacy from door-to-door salesmen of the past); 144 Cong. Rec. S8482–83 (daily ed. July 17, 1998) (statement of Sen. Richard Bryan) (Other websites "were collecting personal financial information like what the family income was, does the family own stocks or certificates of deposit, did their grandparents give them any financial gifts? . . . [C]ompanies are attempting to build a wealth of information about you and your family without an adult's approval . . . .").

[136] 170 Cong. Rec. S5503 (daily ed. July 25, 2024) (statement of Sen. Bill Cassidy).

[137] Legislative Solutions Hearing, supra note 98, at 02:21:40 (statement of Rep. John James).

[138] Cf. Gary T. Marx & Valerie Steeves, From the Beginning: Children as Subjects and Agents of Surveillance, 7 Surveillance & Soc'y 192, 204 (2010) (collecting examples of data-tracking services); Stuart C. Aitken, Geographies of Young People: The Morally Contested Spaces of Identity 178–80 (2001) (explaining that parental control can motivate children to seek privacy and autonomy in new forms).

[139] Circle, https://meetcircle.com/ [https://perma.cc/4L4D-Z2XX] (last visited Aug. 30, 2025).

[140] See, e.g., Marx & Steeves, supra note 138, at 204 (collecting several examples).

[141] Id. at 200 (citation omitted).

[142] Id. at 205 (quoting PC Tattletale, https://web.archive.org/web/20090902034322/http://www.pctattletale.com:80/ [https://perma.cc/69XT-53C2] (last visited Aug. 30, 2025)).

ecosystem of businesses whose profits depend on maximal surveillance.[143]

Preying on parents' fears and insecurities, technology company rhetoric suggests that a failure to monitor children's online activities amounts to parental negligence.[144] The overriding theme can be summed up this way: "Leave [n]othing [t]o [c]hance!! Know everything, and I mean [e]verything, about your [teen] . . . ."[145] If digital surveillance of young people's every move is a necessary part of parents' duty of care, parents must be in charge of their children's privacy. Surveillance tools are as necessary for parenting as clothing, food, and shelter.

Therefore, norms about parenting justify the parental control model. Those norms both influence and reflect legal imperatives, which in turn reinforce the seeming obviousness of parental authority.[146] But the model is anything but obvious.

Having now constructed the edifice of the parental privacy control model, the next Part challenges its foundations, assumptions, and justifications.

III. CHALLENGING THE RATIONALES FOR PARENTAL CONTROL

Despite its popularity, the parental control model collapses in on itself. This Part explains how and responds to the reasoning described above. The parental control model treats young people, including late adolescents, with a heavy hand of disempowerment. It ignores the importance of intimate privacy for those under eighteen. It is based on

[143] Citron, Fight for Privacy, supra note 13, at 21; Danielle Keats Citron, Spying Inc., 72 Wash. & Lee L. Rev. 1243, 1243–45 (2015).

[144] Marx & Steeves, supra note 138, at 193–206; see id. at 207–12 (collecting marketing examples for children and parents).

[145] Id. at 204 (fifth alteration in original) (quoting Alltrack USA, https://web.archive.org/web/20090916030337/http://www.alltrackusa.com:80/ [https://perma.cc/KW2M-GVXZ] (last visited Aug. 30, 2025)).

[146] On the relationship between law and norms, see generally Cass R. Sunstein, On the Expressive Function of Law, 144 U. Pa. L. Rev. 2021 (1996) (articulating one function of law as making expressive statements that impact social norms); Elizabeth S. Scott, Social Norms and the Legal Regulation of Marriage, 86 Va. L. Rev. 1901 (2000) (exploring the relationship between law and norms in the marital context); Danielle Keats Citron, Law's Expressive Value in Combating Cyber Gender Harassment, 108 Mich. L. Rev. 373 (2009) (arguing that cyber harassment law can reverse the norms around and trivialization of cyber gender harassment); Matthew Tokson & Ari Ezra Waldman, Social Norms in Fourth Amendment Law, 120 Mich. L. Rev. 265 (2021) (identifying and challenging the deep reliance of courts on social norms in Fourth Amendment law).

legal fictions that do not withstand scrutiny. And it places unique and unequal burdens on women and the most marginalized young people.

A. Misleading and Misdirected Claims About Child Development

Expansive parental control is premised on the rationale that young people lack the maturity to understand and protect their own privacy interests.[147] But that argument rests on a misleading narrative of how child development works. Young people do not suddenly reach cognitive maturity at seventeen or eighteen.[148] Developmental psychologists and childhood experts agree that maturation is an evolving process.[149] Over time, youth gain cognitive skills that enable them to make autonomous decisions.[150] They mature in different ways at different stages; practices supporting growth at one stage may be unnecessary or even harmful at another stage.[151] By middle adolescence, young people develop cognitive abilities similar to those of adults "in reasoning about moral dilemmas, understanding social rules and laws, [and] reasoning about interpersonal relationships and interpersonal problems."[152] If youth privacy law

[147] See supra Section II.A. There is great irony in this argument. The law assumes that young people are sufficiently immature to need parents to navigate their privacy for them, yet they are simultaneously sufficiently mature to become parents themselves, see, e.g., Megan Messerly & Adam Wren, National Right to Life Official: 10-Year-Old Should Have Had Baby, Politico (July 14, 2022, 12:51 PM), https://www.politico.com/news/2022/07/14/anti-abotion-10-year-old-ohio-00045843, and to be incarcerated as adults, see, e.g., Vincent M. Southerland, Youth Matters: The Need to Treat Children Like Children, 27 J.C.R. & Econ. Dev. 765, 778–81 (2015) (chronicling the response to the super-predator myth and its increase in incarceration of youth as adults); Kristin Henning, The Challenge of Race and Crime in a Free Society: The Racial Divide in Fifty Years of Juvenile Justice Reform, 86 Geo. Wash. L. Rev. 1604, 1622 (2018) (noting the high rates of young people tried and imprisoned as adults).

[148] Kay Mathiesen, The Internet, Children, and Privacy: The Case Against Parental Monitoring, 15 Ethics & Info. Tech. 263, 269 (2013).

[149] Joseph Goldstein, Albert J. Solnit, Sonja Goldstein & Anna Freud, The Best Interests of the Child: The Least Detrimental Alternative 8 (1996); see also Jeffrey Jensen Arnett, Emerging Adulthood: The Winding Road from the Late Teens Through the Twenties, at v–vii (2004) (showing how a young person's adolescence through their twenties is a period of continual development); Robert Epstein, The Case Against Adolescence: Rediscovering the Adult in Every Teen 19–20 (2007) (criticizing the "artificial extension of childhood"); Franklin E. Zimring, The Changing Legal World of Adolescence, at x–xii (1982) (discussing legal notions of adolescence and adulthood).

[150] Tamar Schapiro, Childhood and Personhood, 45 Ariz. L. Rev. 575, 587–89 (2003). This is true despite age-based cultural rites of passage that frame popular consciousness about maturity. See Jonathan Todres, Maturity, 48 Hous. L. Rev. 1107, 1148–56 (2012).

[151] Goldstein et al., supra note 149, at 8–9.

[152] Emily Buss, Developmental Jurisprudence, 88 Temp. L. Rev. 741, 761 (2016) (alteration in original) (quoting Brief for Amici Curiae American Psychological Ass'n et al. in Support

reflected what the scientific community knows about the processes of maturation, lawmakers would and should endeavor to capture that nuance in a meaningful way.

Instead, law and reform proposals proceed with little rhyme or reason. Age is the tool that lawmakers have used to differentiate young people who are subject to parental control from young people who have cognizable privacy interests.[153] While age could be used in a thoughtful and reasoned way, this has not been the case in youth privacy law. Age designations appear somewhat random. Age benchmarks are often "crude judgment[s]"[154] that approximate goals like incentivization of parental involvement,[155] antidiscrimination,[156] administrability,[157] and clarity.[158] Age can serve as a proxy for these ends, yet sound policy requires a reasonable explanation.[159] Youth privacy law provides little to no such explanation.

The earliest youth privacy law, FERPA, marked a young person's eighteenth birthday as the age at which they gained access to student records; until then, parents were in control.[160] More than twenty years

of Petitioners/Cross-Respondents in Nos. 88-1125, 88-1309 and in Support of Appellees in No. 88-805 at *19–20, Hodgson v. Minnesota, 497 U.S. 417 (1990) (Nos. 88-1125, 88-1309) & Ohio v. Akron Ctr. for Reprod. Health, 497 U.S. 502 (1990) (No. 88-805)).

[153] Goldstein et al., supra note 149, at 5.

[154] Elizabeth S. Scott, The Legal Construction of Adolescence, 29 Hofstra L. Rev. 547, 559 (2000) [hereinafter Scott, Legal Construction].

[155] Id. at 560.

[156] See Elizabeth S. Scott & Laurence Steinberg, Blaming Youth, 81 Tex. L. Rev. 799, 836–37 (2003) (noting that case-by-case maturity decisions would likely be based on implicit biases).

[157] See C. Antoinette Clarke, The Baby and the Bathwater: Adolescent Offending and Punitive Juvenile Justice Reform, 53 U. Kan. L. Rev. 659, 686–87 (2005) (highlighting the administrative ease of age demarcations of adulthood).

[158] Scott, Legal Construction, supra note 154, at 561.

[159] Justice Oliver Wendell Holmes, Jr., noted:

> When a legal distinction is determined, as no one doubts that it may be, between night and day, childhood and maturity, or any other extremes, a point has to be fixed or a line has to be drawn, or gradually picked out by successive decisions, to mark where the change takes place. Looked at by itself without regard to the necessity behind it the line or point seems arbitrary. It might as well or nearly as well be a little more to one side or the other. But when it is seen that a line or point there must be, and that there is no mathematical or logical way of fixing it precisely, the decision of the legislature must be accepted unless we can say that it is very wide of any reasonable mark.

Louisville Gas & Elec. Co. v. Coleman, 277 U.S. 32, 41 (1928) (Holmes, J., dissenting).

[160] 20 U.S.C. § 1232g(a)(1)(A), (b), (d); see also Todres, supra note 150, at 1118–45 (describing how different statutes, common law rules, and court decisions make age determinations of adulthood).

later, in 1998, Congress designated thirteen as the relevant age for children's online privacy.[161] Under COPPA, parents control children's privacy for the twelve-and-under set. On their thirteenth birthday, youth transform into adults with the same negligible privacy rights as adults. Learning from FERPA, twenty-first-century lawmakers are trying to extend the time that parents are in charge. Both the American Data Privacy and Protection Act ("ADPPA") of 2022, a bipartisan federal privacy bill, and KOSPA, which passed in the Senate in 2024, used seventeen as an age benchmark.[162]

As these laws and bills show, the parental control model has toggled from eighteen to thirteen and back to seventeen, but with little explanation. These choices are not just random; they are baffling given the stakes. FERPA has kept youth from accessing and seeking to correct inaccuracies in student records when it matters the most—before they apply to college or university. With COPPA, Congress gave parents privacy control over children under thirteen and treated adolescents as adults, which, given the paucity of data privacy protections, meant children thirteen and older had no privacy at all. In the United States, companies can collect and exploit the personal data of anyone thirteen and older so long as they do not lie about their data-handling practices.

We understand why family law scholarship does not reject age benchmarks: on crucial issues, courts can consider a young person's circumstances to ensure that age rules do not miss the mark.[163] For instance, the mature minor doctrine allows courts to identify youth "capable of appreciating the nature, extent, and potential consequences" of medical treatment so they can consent to such treatment over parental objections.[164] Similarly, family court judges deciding custody disputes have discretion to weigh the preferences of teenagers exhibiting indicia of maturity.[165] These doctrines act as safety valves, letting courts assess a

[161] 15 U.S.C. § 6501(1).

[162] American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 2(11) (2022); Kids Online Safety and Privacy Act, S. 2073, 118th Cong. § 101(9) (2024).

[163] See Scott, Legal Construction, supra note 154, at 560 ("[Age classification] generally functions quite well. For most purposes, no great harm results from postponing adult legal status until the designated age, or from giving parents legal authority and thereby involving them in their adolescent children's lives.").

[164] Restatement (Third) of Torts: Intentional Torts to Persons § 15 cmt. b (Am. L. Inst., Tentative Draft No. 4, 2019); see also, e.g., In re E.G., 549 N.E.2d 322, 327–28 (Ill. 1989) (stating the mature minor rule and allowing minors to refuse lifesaving treatment).

[165] Barbara A. Atwood, The Child's Voice in Custody Litigation: An Empirical Survey and Suggestions for Reform, 45 Ariz. L. Rev. 629, 641 n.59 (2003) (listing state laws); see also

child's actual circumstances to ensure that age designations make sense in context.

By contrast, youth privacy law has no such safety valves; age operates as an on-off switch. Federal laws like FERPA and COPPA, as well as state social media and privacy laws, admit no complexity or nuance. They have no backstops or off-ramps. They offer no opportunity to ensure that information rules make sense for a given youth.[166]

Youth privacy law's blunt use of age without clear reasons and insensitivity to variation are one set of concerns. As the next Section illustrates, social science evidence makes clear that the maturity argument is woefully incomplete and that young people want, need, and endeavor to achieve intimate privacy for the good of their development, maturation, and growth.

B. Intimate Privacy's Centrality to Youth Development

Contrary to the conventional wisdom animating much of U.S. youth privacy law, young people have a rich understanding of privacy and claim it for themselves as they develop. Social science literature shows that navigating privacy helps children develop skills of self-regulation, autonomy, and independence.[167] Once young people carve out privacy, it enables self-discovery and the formation of intimate relationships. Current privacy law ignores these aspects of privacy's importance for youth.

1. Claiming Privacy

Even early childhood is marked by a desire for privacy. Children as young as two years old create "physical privacy mark[ings]" at home by retreating to confined spaces that function as "exclusive preserve[s]."[168]

Saxon v. Saxon, 428 S.E.2d 376, 377–78 (Ga. Ct. App. 1993) (giving special weight to preference of fifteen-year-old son); Burney v. Burney, 152 S.E.2d 871, 873 (Ga. 1966) (reversing the trial court's custody decree where a fifteen-year-old's wishes were not granted).

[166] See Allen, Unpopular Privacy, supra note 82, at 179 (noting that the lack of a mature minor exception in COPPA means that "parents rule officially and absolutely").

[167] Tom Frijns, Catrin Finkenauer, Ad A. Vermulst & Rutger C.M.E. Engels, Keeping Secrets from Parents: Longitudinal Associations of Secrecy in Adolescence, 34 J. Youth & Adolescence 137, 138 (2005); Skyler T. Hawk, Loes Keijsers, William W. Hale III & Wim Meeus, Mind Your Own Business! Longitudinal Relations Between Perceived Privacy Invasion and Adolescent-Parent Conflict, 23 J. Fam. Psych. 511, 512 (2009).

[168] Ross D. Parke & Douglas B. Sawin, Children's Privacy in the Home: Developmental, Ecological, and Child-Rearing Determinants, 11 Env't & Behav. 87, 91, 100 (1979); Parke,

Social scientists Maxine Wolfe and Robert Laufer, who studied children's privacy practices, found that children as young as seven have complex understandings of privacy: they think about and try to control what others know about them.[169] For instance, kindergartners in open-plan classrooms demonstrate their desire for privacy by complaining about having no place to go when they want to concentrate on a task.[170] They try to keep certain activities from others and carve out time by themselves.[171] Children ranging from nine to sixteen years old close the doors to their bedrooms and bathrooms to keep out parents and siblings.[172] Household members can access those spaces only with children's consent.[173] These practices let children "determine the amount and type of social and physical contact among individual family members and . . . limit access of outsiders."[174]

Family circumstances and physical surroundings shape children's privacy efforts.[175] In suburban, middle-class homes with multiple rooms, youth assert their desire for privacy by retreating to their bedrooms.[176] Where children share rooms, privacy manifests less in exerting autonomy over physical spaces and more in claiming psychological space from others.[177]

Children also attempt to achieve privacy by retreating into their thoughts or concealing their reading, watching, and communications. That is how the young William James Sidis tried to find privacy amidst

supra note 16, at 65–66 (citation omitted). Infants show a need for privacy by wriggling away from caregivers, establishing distance, and going to sleep to escape overstimulation. Barry Schwartz, The Social Psychology of Privacy, 73 Am. J. Socio. 741, 749 (1968).

[169] Maxine Wolfe & Robert Laufer, The Concept of Privacy in Childhood and Adolescence, *in* Man-Environment Interactions: Evaluations and Applications, pt. II, unit 6, at 29, 51 (Daniel H. Carson ed., 1974).

[170] Id. at 29–30.

[171] Id. at 33.

[172] Parke & Sawin, supra note 168, at 91; Parke, supra note 16, at 66–67.

[173] Parke, supra note 16, at 65; Max van Manen & Bas Levering, Childhood's Secrets: Intimacy, Privacy, and the Self Reconsidered 159 (1996).

[174] Parke, supra note 16, at 65; see also Jeanne R. Steele & Jane D. Brown, Adolescent Room Culture: Studying Media in the Context of Everyday Life, 24 J. Youth & Adolescence 551, 551 (1995) ("[B]edroom[s] . . . [are] important haven[s] for most teenagers, a private, personal space . . . .").

[175] Arnold Simmel, Privacy Is Not an Isolated Freedom, *in* Privacy 71, 76–78 (J. Roland Pennock & John W. Chapman eds., 1971).

[176] Wolfe & Laufer, supra note 169, at 37.

[177] Simmel, supra note 175, at 74–78 (describing early stages of development and connecting the "life cycle" of development with different but ongoing manifestations of privacy).

the onslaught of publicity thrust upon him by his parents and the press. For Sidis, "[t]hinking—analyzing, pondering abstractions—was his refuge, his place of privacy and play. . . . [His] only refuge was in learning."[178] More than a century later, Juniper Galvani, a youth advocate from Vermont, explained that when she was young, she realized that she could watch YouTube without her parents finding out by hiding her iPad "in a big picture book."[179]

Youth engage in privacy-protective tactics online. They take steps to protect self-expression and group activity from parents, teachers, acquaintances, and strangers.[180] Teenagers post coded statements that would be understood by close friends and elude parental comprehension.[181] They create multiple profiles on social media to manage who has access to their photographs, thoughts, and feelings.[182] They have social media accounts for family members, friends, and acquaintances and alternative accounts that only select individuals can access (and from which parents are often excluded).[183] They delete and un-tag content, remove friends, and deactivate profiles to ensure that their personal expression is not seen by certain audiences.[184] Young queer people erase visits to LGBTQ+-oriented chat rooms from their browser

[178] Wallace, supra note 112, at 55.

[179] Vermont Senate Committee on Economic Development, Housing, and General Affairs, Senate Economic Development - 2024-02-15 - 9:00 AM, at 17:00 (YouTube, Feb. 15, 2024) [hereinafter Vermont Senate Video], https://www.youtube.com/watch?v=DMxhzRvCjrY [https://perma.cc/Y6QY-5AMN] (statement of Juniper Galvani).

[180] Mariya Stoilova, Sonia Livingstone & Rishita Nandagiri, Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy, 8 Media & Commc'n 197, 199 (2020) [hereinafter Stoilova et al., Digital by Default].

[181] danah boyd, It's Complicated: The Social Lives of Networked Teens 66–67 (2014) (explaining how teenagers post encoded messages like song lyrics to convey meanings to friends without alarming their mothers by making them think they are suicidal).

[182] Lia Emanuel & Danaë Stanton Fraser, Exploring Physical and Digital Identity with a Teenage Cohort, *in* ICD '14: Proceedings of the 2014 Conference on Interaction Design and Children 67, 73 (Ole Sejer Iversen et al. eds., 2014); danah boyd & Alice Marwick, Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies 20 (May 9, 2011) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128 [https://perma.cc/2DJQ-MF8Z].

[183] See boyd, supra note 181, at 19–23.

[184] Mary Madden et al., Pew Rsch. Ctr. & Berkman Ctr. for Internet & Soc'y, Teens, Social Media, and Privacy 17–18 (2013), https://www.pewresearch.org/wp-content/uploads/sites/9/2013/05/PIP_TeensSocialMediaandPrivacy_PDF.pdf [https://perma.cc/937L-D7ZG]; boyd, supra note 181, at 70–71 (noting an interview with a Black eighteen-year-old girl who explained that she would deactivate her Facebook account whenever she was not using the site to prevent state agencies and guardians from foster care from seeing her posts).

histories to ensure that their parents cannot discover their identities before they are ready to come out on their own terms.[185]

Young people have resisted corporate surveillance by using incognito tabs to shield their browsing or deleting their search history to minimize the exposure of data about their thinking.[186] Yet resistance is impossible when youth (or adults, for that matter) do not know about the vast ecosystem of commercial data exploitation by social media platforms, advertisers, marketers, data brokers, and commercial websites in the information economy.[187] When young people are informed about commercial data exploitation, they express a desire for privacy.[188] In one study, youth aged sixteen to eighteen who were informed about commercial privacy risks showed less interest in buying things online.[189]

To sum up, young people claim intimate privacy by closing doors; burying themselves in their thoughts; keeping their feelings to themselves; concealing their browsing, reading, and video watching; and engaging in varied tactics online to segment who can access and understand their communications. Young people route around obstacles and use whatever powers they can to manage the boundaries around their intimate lives and data. Much of this privacy management is for the good of self-development and maturation, to which we now turn.

2. Leveraging Privacy to Grow and Mature

Adults often fail to recognize the privacy that youth want, expect, and assert.[190] Adults tend to view children's sharing of information online as relinquishing privacy; parents' central worries are that strangers will contact their kids online and that young people will erode the family's

[185] boyd, supra note 181, at 52 (noting that an interviewee, a queer teenage girl, also reported using an Internet Explorer browser when visiting LGBTQ+-related sites and Google Chrome while maintaining her straight persona in an effort to keep digital traces of her queer and straight identities separate).

[186] Stoilova et al., Digital by Default, supra note 180, at 201.

[187] Id.

[188] Sonia Livingstone, Mariya Stoilova & Rishita Nandagiri, Children's Data and Privacy Online: Growing Up in a Digital Age 14–15 (2019); cf. id. at 18 (explaining that teens recognize commercial data tracking).

[189] Id. at 15 (citing Brahim Zarouali, Koen Ponnet, Michel Walrave & Karolien Poels, "Do You Like Cookies?" Adolescents' Skeptical Processing of Retargeted Facebook-Ads and the Moderating Role of Privacy Concern and a Textual Debriefing, 69 Computs. Hum. Behav. 157, 162 (2017)).

[190] boyd & Marwick, supra note 182, at 1 (noting the myth that people assume that young people do not care about privacy).

privacy.[191] The received wisdom is that young people are reckless; consequently, parents hope and expect that their children will not share information about themselves at all.

By contrast, youth expect people in their online networks to be discreet with their information because they have taken steps to ensure their information stays in those networks; their central worry is that their trusted contacts will leak their information to "known others," such as parents and teachers.[192] This disconnect could explain adults' failure to appreciate the extent to which young people want and try to carve out privacy even as they participate in networked activities.

That young people understand and protect their privacy interests differently than adults think they do neither diminishes young people's desire for privacy nor undermines their expectation of privacy. Those differences do not render youth intimate privacy unworthy of recognition and protection. What is more, this disconnect is fabricated. A longstanding line of social literature shows that adults expect trusted networks to be discreet with their personal information, just as youth do.[193]

Youth intimate privacy is essential for growth and maturation. Behavioral scientists suggest that children's concealment of their thoughts, feelings, and desires from parents or guardians is critical to development because it helps them realize that they have the ability to

[191] Id. at 5; Suzanne Choney, Parents Worry About Strangers—and Advertisers—Tracking Kids Online, Says Report, Today (Nov. 21, 2012, 2:07 PM), https://www.today.com/money/parents-worry-about-strangers-advertisers-tracking-kids-online-says-report-1c7204133 [https://perma.cc/P382-DB8K].

[192] Katie Davis & Carrie James, Tweens' Conceptions of Privacy Online: Implications for Educators, 38 Learning, Media & Tech. 4, 6 (2013). This sense of privacy among youth reflects "a [s]ocial [n]etworks [t]heory of [p]rivacy." Lior Jacob Strahilevitz, A Social Networks Theory of Privacy, 72 U. Chi. L. Rev. 919, 919 (2005); see also id. at 974 (arguing that information disclosed to others should be understood as private if it is unlikely to be spread from one network to another).

[193] See, e.g., Erving Goffman, The Presentation of Self in Everyday Life 1–4 (1956); James Rachels, Why Privacy Is Important, 4 Phil. & Pub. Affs. 323, 326–29 (1975); Julie E. Cohen, What Privacy Is For, 126 Harv. L. Rev. 1904, 1905 (2013) ("[Privacy] protects the situated practices of boundary management through which the capacity for self-determination develops."); Liam Bullingham & Ana C. Vasconcelos, 'The Presentation of Self in the Online World': Goffman and the Study of Online Identities, 39 J. Info. Sci. 101, 110 (2013) (arguing that individuals using online technologies engage in image management and persona editing); Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 Stan. L. Rev. 1373, 1427 (2000) (arguing that information privacy allows us to construct Goffman's social facades).

share or withhold their thoughts from others.[194] The "social ritual of privacy" is necessary for understanding boundaries and identity: "It has to do with learning that I can control when, and by whom, the thoughts in my head will be experienced by someone other than myself and learning that I am entitled to such control . . . ."[195] Pamela Wisniewski has shown that experiencing online spaces is part of a "developmental process of adolescent growth" that helps young people develop strategies of resilience "to cope with ever-present risks."[196] And danah boyd put it well when she explained that for teenagers, "being able to achieve privacy is an expression of agency."[197]

Intimate privacy enables young people to develop skills of self-regulation, autonomy, and independence.[198] Children can develop their personalities when parents give them breathing room to do so without monitoring their every move.[199] Time on the internet can undoubtedly be risky, but for young people, it can also be a time to "self-reflect, to study, to figure out [identities], to interact . . . with each other, to grow as people, and to see how the world works."[200] Young people need online communication channels where they can try out ideas and identities free from fear of being misunderstood or embarrassed.[201] Children cannot do that if their online experiences are continuously surveilled by their parents.[202]

[194] See Wolfe & Laufer, supra note 169, at 51 (explaining that such concealment begins as early as five years old); van Manen & Levering, supra note 173, at 107.

[195] Jeffrey H. Reiman, Privacy, Intimacy, and Personhood, 6 Phil. & Pub. Affs. 26, 43 (1976).

[196] Pamela Wisniewski, Heng Xu, Mary Beth Rosson, Daniel F. Perkins & John M. Carroll, Dear Diary: Teens Reflect on Their Weekly Online Risk Experiences, *in* 5 Ass'n for Computing Mach., CHI 2016: Proceedings of the 34th Annual CHI Conference on Human Factors in Computing Systems 3919, 3920 (2016).

[197] boyd, supra note 181, at 76 (emphasis omitted).

[198] Frijns et al., supra note 167, at 138–39 (collecting studies); Karyn D. McKinney, Space, Body, and Mind: Parental Perceptions of Children's Privacy Needs, 19 J. Fam. Issues 75, 77 (1998); Hawk et al., supra note 167, at 512.

[199] van Manen & Levering, supra note 173, at 112.

[200] Vermont House Committee on Commerce and Economic Development, House Commerce - 2024-04-04 - 9:00 AM, at 01:11:01 (YouTube, Apr. 4, 2024) [hereinafter Vermont House Committee on Commerce and Economic Development Video], https://www.youtube.com/watch?v=FzwugdlkKlo [https://perma.cc/B5EZ-YD59] (statement of Juniper Galvani).

[201] Citron, Surveilled Student, supra note 15, at 1457.

[202] Mathiesen, supra note 148, at 269.

Children's experiences with privacy help them understand societal norms and appropriate behaviors. "In this way," Wolfe writes, "children's experiences with privacy feed back into their sense of self-esteem and help define the range, limits, and consequences of individual autonomy."[203] When adults cut back on constantly watching children, children come to understand the privacy that they want and expect, and then they work to claim that privacy.[204]

The privacy afforded by asserting independence from select others is important for identity formation, sexual exploration, and relationship building.[205] As one of us (Citron) has argued, "We are free only insofar as we can manage the boundaries around our bodies and intimate activities."[206] Adolescence is a critical time for intimate and relational exploration.[207] Adolescents use interaction and information-management strategies, such as locked doors, private accounts, and choosing to interact with some but not others, as ways to try out non-normative or sexual maturation activities.[208]

For adolescents who sense that they are different from other boys and girls, whether due to same-sex attraction, the absence of sexual attraction, gender exploration,[209] or any number of other sexual and gender differences, privacy can be lifesaving.[210] Janet Mock, a writer and transgender advocate, recalls being punished as a child when her

[203] Wolfe, supra note 16, at 189.

[204] Id. at 186.

[205] Id. at 184.

[206] Danielle Keats Citron, Sexual Privacy, 128 Yale L.J. 1870, 1874 (2019) [hereinafter Citron, Sexual Privacy].

[207] See Wyndol Furman, The Emerging Field of Adolescent Romantic Relationships, 11 Current Directions Psych. Sci. 177, 178 (2002) (describing the developmental course of adolescent relationships).

[208] Wolfe, supra note 16, at 188.

[209] Marie-Amélie George, Exploring Identity, 55 Fam. L.Q. 1, 1 (2021) (using the term "gender expansive children" to refer to "transgender and nonbinary children, as well as children exploring nontraditional gender identities").

[210] See Sabra L. Katz-Wise, Margaret Rosario & Michael Tsappis, Lesbian, Gay, Bisexual, and Transgender Youth and Family Acceptance, 63 Pediatric Clinics N. Am. 1011, 1016 (2016) (finding that one-third of LGBTQ+ individuals experience parental rejection and report high levels of depression); Caitlin Ryan, David Huebner, Rafael M. Diaz & Jorge Sanchez, Family Rejection as a Predictor of Negative Health Outcomes in White and Latino Lesbian, Gay, and Bisexual Young Adults, 123 Pediatrics 346, 350 (2009) (finding that gay, lesbian, and bisexual young adults who report parental rejection are more than eight times more likely to report attempting suicide and nearly six times more likely to report suffering from high levels of depression).

grandmother found her wearing a dress.[211] As a result, Mock could only experiment with women's clothing and discover her identity when her family members were out of the house.[212] Privacy online gives queer adolescents the chance to discover their identities at their own pace and on their own terms. They can meet and engage with others like themselves from all over the world, which can be a lifeline when family members are hostile.[213] This is not to deny the very real dangers queer youth face online, but our point is more narrow: absolute parental control throughout adolescence can stunt children's growth and endanger queer kids.

The development of close relationships depends upon intimate privacy. Intimate privacy enables all of us, young and old, to develop close friendships and fall in love.[214] It lets us reveal ourselves to others, which is essential for the formation of loving and caring relationships.[215] As Charles Fried eloquently noted, privacy is the "oxygen" for love.[216]

Parent-child relationships are on the line as well. Respecting children's privacy and negotiating privacy boundaries where children are seen and heard *enhances* parent-child relationships.[217] By contrast, when parents track children constantly, their kids come to resent their "spying."[218] A study of online reviews by teenagers and younger children of parental control apps found that seventy-six percent of reviews gave the apps a one-star rating along with comments suggesting that parental monitoring negatively impacted children's relationships with parents.[219] Constant

[211] Janet Mock, Redefining Realness: My Path to Womanhood, Identity, Love & So Much More 27–29 (2014).

[212] Id. at 30–31.

[213] Jennifer Egan, Lonely Gay Teen Seeking Same, N.Y. Times Mag., Dec. 10, 2000, at SM110, https://www.nytimes.com/2000/12/10/magazine/lonely-gay-teen-seeking-same.html.

[214] Rachels, supra note 193, at 328, 331.

[215] Waldman, Privacy as Trust, supra note 20, at 7–8, 69–72; Citron, Sexual Privacy, supra note 206, at 1875 (citing Irwin Altman & Dalmas A. Taylor, Social Penetration: The Development of Interpersonal Relationships (1973)).

[216] Charles Fried, An Anatomy of Values: Problems of Personal and Social Choice 140 (1970).

[217] Pamela J. Wisniewski, Jessica Vitak & Heidi Hartikainen, Privacy in Adolescence, *in* Modern Socio-Technical Perspectives on Privacy 315, 318 (Bart P. Knijnenburg et al. eds., 2022).

[218] Valerie Steeves & Priscilla Regan, Young People Online and the Social Value of Privacy, 12 J. Info. Commc'n & Ethics Soc'y 298, 302 (2014).

[219] Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J. LaViola Jr. & Pamela J. Wisniewski, Safety vs. Surveillance: What Children Have to Say About Mobile Apps for Parental Control, *in* Ass'n for Computing Mach., CHI 2018: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (2018).

parental monitoring makes children anxious, depressed, and less satisfied with their parents.[220] Controlling a child's online experience too closely erodes children's trust in their parents.[221] The same is true for students' relationships with their teachers. A 2023 study found that when teachers tell students that monitoring software has flagged their activities as problematic, students no longer trust teachers to protect their interests.[222]

Adolescents need some independence from their parents to learn how to navigate the world on their own.[223] As Franklin Zimring explains, there are crucial things that "we cannot learn to do well without practice: making decisions, making love, driving, flying, practicing law, parenting, taking risks, saying no, and—most important—choosing the path of our lives in a free society."[224] In other words, "[b]eing mature takes practice."[225] Respecting young people's choices and independence helps them gain experience in decision-making, which is the most effective way to teach them to be free.[226]

The underlying assumption of the parental control model—that maturity must precede the enjoyment of privacy decision-making—has it backwards. The phenomenological experience of navigating privacy, taking control of expression and disclosure where possible, and responding to risks is critical to young people's ability to mature into adulthood.[227] Consider Zimring's reframing of age cutoffs in law: "To ask how old is old enough . . . to drive is . . . to ask the wrong question[]. Instead, we must ask how old is old enough to *learn* to drive . . . ."[228]

[220] Hawk et al., supra note 167, at 511–12, 515.

[221] Wisniewski et al., supra note 217, at 318; Derlega & Chaikin, supra note 18, at 15–16 (describing a letter to an advice columnist in which a parent expressed regret about invading their child's privacy, which resulted in a deteriorated relationship).

[222] Dhanaraj Thakur, Hugh Grant-Chapman & Elizabeth Laird, Ctr. for Democracy & Tech., Beyond the Screen: Parents' Experiences with Student Activity Monitoring in K-12 Schools 9–11 (2023). This is as Arthur Miller suggested in 1971—that students would not confide in teachers if they thought that their discussions would end up in computer files that might hurt them. Miller, supra note 58, at 112.

[223] Zimring, supra note 149, at 90–91.

[224] Id. at 89.

[225] Id.

[226] Id. at 91.

[227] Phenomenology focuses on how individuals understand the world through physical and first-person experiences. Maurice Merleau-Ponty, Phenomenology of Perception 67–74 (Colin Smith trans., Taylor & Francis 2005) (1945); see also Citron, Fight for Privacy, supra note 13, at 113–16; Tom Gerety, Redefining Privacy, 12 Harv. C.R.-C.L. L. Rev. 233, 266 (1977).

[228] Zimring, supra note 149, at 93 (emphasis added).

Independence and privacy are necessary for maturity.[229] If maturity is the goal, as current youth privacy laws suggest, total parental control over youth privacy, from infancy to seventeen, is *not* the answer.

As we have seen, the parental control model of youth intimate privacy law misreads the social science research on childhood development. Parental control can also cause significant harm, particularly to sexual and gender minorities. We identify those harms in the next Section.

C. The Dark Side of Parental Control

The parental control model is based on an overly rosy view of parents and the family.[230] Under that vision, parents work together to care for, supervise, and oversee children in a loving and productive manner.[231] But parents do not always advance their children's well-being; to the contrary, some parents prioritize their own interests to their children's detriment.[232] And parents are not always partners in the work of child-rearing. Parental control has a dark side in reifying traditional power structures.

1. The Harms Parents Can Cause

Some twenty-first-century parents have followed in the privacy-destructive footsteps of Boris and Sarah Sidis. Parent influencers on social media overshare information about their children against their children's wishes.[233] They post sexualized pictures of their children to

[229] See Miller, supra note 58, at 24 ("Privacy is a special kind of independence, which can be understood as an attempt to secure autonomy in at least a few personal and spiritual concerns, if necessary in defiance of all the pressures of modern society. . . . [I]t seeks to erect an unbreachable wall of dignity and reserve . . . [where] some of [one's] thoughts and judgments [can be kept] entirely to [oneself], . . . not even [shared with] those [one] loves and trusts." (first alteration in original) (quoting Clinton Rossiter, The Pattern of Liberty, *in* Aspects of Liberty 15, 17 (Milton R. Konvitz & Clinton Rossiter eds., 1958))).

[230] Anne Dailey and Laura Rosenbury have argued that the law has "romanticized the family as a place of unified interests and shared values." Anne C. Dailey & Laura A. Rosenbury, The New Parental Rights, 71 Duke L.J. 75, 78 (2021).

[231] Id.

[232] See Richard E. Redding, Children's Competence to Provide Informed Consent for Mental Health Treatment, 50 Wash. & Lee L. Rev. 695, 701–09 (1993) (summarizing cases and studies showing that medical professionals sometimes role switch, treating patients' parents as if they were the patients and failing to prioritize a child's interests in the way that medical professionals are bound to do).

[233] See, e.g., Christie Tate, My Daughter Asked Me to Stop Writing About Motherhood. Here's Why I Can't Do That., Wash. Post (Jan. 3, 2019), https://www.washingtonpost.com/lifestyle/2019/01/03/my-daughter-asked-me-stop-writing-about-motherhood-heres-why-i-cant-do-that. For an in-depth discussion of "sharenting," see generally Steinberg, supra note 127

earn money,[234] knowing their young daughters and sons are being fetishized by older men.[235] Parents double down on their exposure of children's private lives by refusing to take down embarrassing posts.[236] Describing their experience, teenagers told *The New York Times* that they felt "naked," "disrespected," "humiliated," and frustrated that their parents did not care about their privacy and security interests.[237] Shari Franke knows this better than most. Her mother, Ruby Franke, psychologically and physically abused her children in service of her family vlogging YouTube channel.[238] Shari's "constant exposure" and "exploitation" were part of a "vicious cycle" that Shari likens to "tak[ing] the most poisonous plant in our garden and, instead of uprooting it, ma[king] it the centerpiece of our lives."[239]

To say the least, parents are not always the idealized protectors of children's privacy. Many parents do not think their children, especially young boys, deserve privacy.[240] Rather, they attribute negative motives to their children seeking privacy.[241] The authority that the law gives parents

(describing how some parents invade their children's privacy when posting information about their children without the child's consent).

[234] See, e.g., Jeff Horwitz & Katherine Blunt, Meta Staff Found Instagram Tool Enabled Child Exploitation. The Company Pressed Ahead Anyway., Wall St. J., https://www.wsj.com/tech/meta-staff-found-instagram-subscription-tool-enabled-child-exploitation-the-company-pressed-ahead-anyway-a18e81e6 (last updated Feb. 22, 2024, 10:08 PM); Jennifer Valentino-DeVries & Michael H. Keller, A Marketplace of Girl Influencers Managed by Moms and Stalked by Men, N.Y. Times (Feb. 25, 2024), https://www.nytimes.com/2024/02/22/us/instagram-child-influencers.html.

[235] Katherine Blunt, The Influencer Is a Young Teenage Girl. The Audience Is 92% Adult Men., Wall St. J. (June 15, 2024, 9:00 PM), https://archive.ph/1IXIH ("The Journal reviewed dozens of conversations in which the men fetishized specific body parts and expressed pleasure in knowing that many parents of young influencers understand that hundreds, if not thousands, of pedophiles have found their children online. . . . 'We're all model scouts, agents and brand owners,' another man replied [on Telegram] in jest. 'We're totally NOT jerking off to the pics.'").

[236] Jen Juneau, Mom Blogger Defends Her Decision Not to Remove Photos of Her Daughter After Child's Request, People (Jan. 7, 2020, 11:50 AM), https://people.com/parents/mom-blogger-wont-take-down-pictures-of-daughter [https://perma.cc/K9UW-Z6R6].

[237] Rachel L. Harris & Lisa Tarchak, Opinion, Mom and Dad, It's My (Digital) Life, N.Y. Times (Sept. 2, 2019), https://www.nytimes.com/2019/09/02/opinion/children-internet-privacy.html.

[238] Rebekah Riess, Prosecutors Say New Video, Documents Show 'Religious Extremism' Motivated Parent Blogger Ruby Franke's Abuse of Children, CNN, https://www.cnn.com/2024/03/23/us/ruby-franke-child-abuse-police-video/index.html [https://perma.cc/PE9K-CBYJ] (last updated Apr. 2, 2024, 2:19 PM).

[239] Franke, supra note 127, at 53.

[240] McKinney, supra note 198, at 80, 83.

[241] Id. at 96.

can be a license to further their own interests.[242] Parental self-interest can eclipse recognition and concern about children's privacy interests. Young people are exploited and denied independence by the very people whom the law entrusts to protect them.

Laws that give parents information about and control over whether their children can seek mental health resources at school disproportionately burden a vulnerable subset of students—those struggling with their mental health.[243] A supportive environment at home can be a boon to young people struggling with anxiety, depression, and suicidal ideation.[244] But for any number of reasons, not all young people have good relationships with their parents (or guardians). This is especially pernicious for youth who already feel unable to turn to their parents for basic needs, particularly LGBTQ+ youth.[245] For queer youth, parental alienation and cruelty, rather than care and concern, are profoundly damaging and regrettably routine. Parents reject their LGBTQ+ children[246] at alarming rates. In this way, state laws that

[242] Anne C. Dailey & Laura A. Rosenbury, The New Law of the Child, 127 Yale L.J. 1448, 1470 (2018).

[243] Citron, Surveilled Student, supra note 15, at 1460–61.

[244] Positive Parenting: Building Healthy Relationships with Your Kids, News in Health (Nat'l Insts. Health, Bethesda, Md.), Sept. 2017, at 1, https://newsinhealth.nih.gov/sites/newsinhealth/files/2017/September/NIHNiHSep2017.pdf [https://perma.cc/PK7M-HGAY] (explaining that parents can foster secure attachment in children such that they are better able to cope with depression); Tianna Hicklin, Supportive Parenting Can Reduce Child's Anxiety, Nat'l Insts. of Health: NIH Rsch. Matters (Mar. 19, 2019), https://www.nih.gov/news-events/nih-research-matters/supportive-parenting-can-reduce-childs-anxiety [https://perma.cc/5GYT-7XKW] (citing a 2019 National Institute of Mental Health study finding parents who were taught supportive ways to respond to their child's anxiety helped reduce their child's levels of anxiety and anxiety-related emotional disorders (citation omitted)).

[245] A survey of 28,000 LGBTQ+ youth found that 46% of respondents aged thirteen to seventeen considered attempting suicide in the past year, whereas 17% had made such attempts; 70% and 57% reported having experienced symptoms of anxiety or depression, respectively; and 56% of LGBTQ+ youth aged thirteen to twenty-four reported wanting mental health care in the past year but being unable to access it, including 41% who reported having forgone help because they did not want to have to obtain parent or caregiver permission. Trevor Project, 2023 U.S. National Survey on the Mental Health of LGBTQ+ Young People 3, 5, 8, 11–12 (2023), https://www.thetrevorproject.org/survey-2023/assets/static/05_TREVOR05_2023survey.pdf [https://perma.cc/Y9TK-NJWB]. For an excellent discussion about how parents and schools are taking control of and harming young people's ability to express their identities, see generally Scott Skinner-Thompson, Identity by Committee, 57 Harv. C.R.-C.L. L. Rev. 657 (2022).

[246] See Emilie D'Amico, Danielle Julien, Nicole Tremblay & Elise Chartrand, Gay, Lesbian, and Bisexual Youths Coming Out to Their Parents: Parental Reactions and Youths' Outcomes, 11 J. GLBT Fam. Stud. 411, 411, 414, 427 (2015); cf. Claire Thornton, 'Rejected Solely Because of Your Identity': Homeless LGBTQ Youths Face Unique Challenges, USA Today

heighten parental control over some students and not others are dangerous.

2. Reinforcing Gender Dynamics in the Family

While some advocates for parental control are forthcoming about their anti-LGBTQ+ motives, there is scarce acknowledgement of the family gender dynamics reified by increasing parental responsibility. Women caregivers are saddled with the greatest burdens of parenting in opposite-sex households.[247] Therefore, when scholars and advocates say that *parents* should monitor their children's digital lives, that recommendation actually means that *mothers* should oversee children's online behavior and read privacy policies.[248] Because mothers end up playing that role, children tend to see their mothers, not their fathers, as coercive when it comes to privacy.[249] No wonder studies show that privacy navigation in the home contributes to *mother*-child conflicts, not father-child conflicts.[250]

(June 2, 2023, 6:01 AM), https://www.usatoday.com/story/news/nation/2023/06/02/lgbtq-homeless-youths-family-rejection/11535821002/ [https://perma.cc/MMJ2-K3EE] (discussing a study finding that more than half of the homeless LGBTQ+ youth population report having "been forced onto the streets" due to parental hostility toward their gender identity or sexual orientation).

[247] See, e.g., Sarah Fenstermaker Berk, The Gender Factory: The Apportionment of Work in American Households 7–10 (1985); Karen Czapanskiy, Volunteers and Draftees: The Struggle for Parental Equality, 38 UCLA L. Rev. 1415, 1469 (1991) (critiquing joint custody on these grounds); Janet K.L. McKeown & Diana C. Parry, First Comes Love, Then Comes Marriage, Then Comes Baby in the Baby Carriage? Exploring How Women Can Use Leisure as Resistance to Gendered Ideologies, 38 Leisure Stud. 191, 192 (2019) (arguing that gendered logics of marriage, family, and parenthood reinforce women's unequal responsibilities in the family); Carolina Aragão, For Many U.S. Moms, Pandemic Brought Increase in Time Spent Caring for Kids While Doing Other Things, Pew Rsch. Ctr. (Oct. 11, 2022), https://www.pewresearch.org/short-reads/2022/10/11/for-many-u-s-moms-pandemic-brought-increase-in-time-spent-caring-for-kids-while-doing-other-things/ [https://perma.cc/9UAC-7WCR] (finding over the 2019–2020 pandemic year that, whereas mothers continued the historical trend of spending more time on primary childcare than did fathers, mothers also spent significantly more time on secondary childcare, caring for children while engaged in other tasks, like work or chores).

[248] Hawk et al., supra note 167, at 512; Robyn N. Waizenhofer, Christy M. Buchanan & Julia Jackson-Newsom, Mothers' and Fathers' Knowledge of Adolescents' Daily Activities: Its Sources and Its Links with Adolescent Adjustment, 18 J. Fam. Psych. 348, 358 (2004).

[249] Parke & Sawin, supra note 168, at 99.

[250] Cf. id. (detailing empirical findings that "in homes where parents, rather than child, control the open/closed status of a child's bedroom door, mothers were rated high on the coerciveness of her suggestions to the child").

The image of the engaged parent is not only gendered, but also class based. The parental control model implicitly reinforces a particular vision of an "ideal" two-parent household where parents have the time and resources to provide the support their children need.[251] Wealthier parents have more time, freedom, and capacity to actively oversee their children's online activities.[252] They are more likely than poorer parents to talk with their children about online harms, go online with them, and point out potential risks.[253] Adding privacy control responsibilities will only widen the existing gaps between primary and secondary caregivers in families and between rich and poor families.

Although it is important to recognize the power imbalances embedded within parental control, more egalitarian family relations do not solve the model's problems. As we discuss below, few parents can actually shoulder the burdens of exclusive parental control.

D. The Lack of Control in Parental Control

The parental control model deflects responsibility away from tech companies and onto private citizens. Instead of leveraging state power to regulate data extraction and manipulation of young people, youth privacy laws outsource that duty to parents. That burden shifting does little to protect children from harm in part because most parents do not have the time or ability to meet those responsibilities.

For most parents, keeping up with requests for consent is impossible. Parents regrettably note that requests for consent (from schools, tech companies, and elsewhere) slip through the cracks.[254] Civil rights advocate David Brody summed up the challenges best when explaining why parents cannot and do not read privacy policies: "[T]here's too many

[251] Dailey & Rosenbury, supra note 230, at 104.

[252] See, e.g., Andrea Duerager & Sonia Livingstone, How Can Parents Support Children's Internet Safety?, EU Kids Online 1–2 (2012), https://eprints.lse.ac.uk/42872/1/How%20can%20parents%20support%20children%E2%80%99s%20internet%20safety%28lsero%29.pdf [https://perma.cc/XGT-L4HC].

[253] Id.

[254] Iowa House of Reps., House Floor Audio on Sen. File 496, Gen. Assemb., at 02:35:05 (Apr. 4, 2023), https://www.legis.iowa.gov/dashboard?view=video&chamber=H&clip=h20230404011950323&dt=2023-04-04&offset=2243&bill=SF%20496&status=r [https://perma.cc/USC4-2GNE] (statement of Rep. Heather Matson) (testifying that the countless number of emails and notices from their kids' schools make it likely that some emails will get missed).

things to be done. And so, look, I just want my kid to be able to watch Bluey."[255]

But even with sufficient time, parents cannot protect their children's privacy with the woefully inadequate tools available to them, including consent toggles, privacy policies, cookie consents, and other detritus of privacy self-management.[256] Because those tools are insufficient, parental control simply demands that parents steward their children through the same inadequate privacy paradigms that adults themselves struggle to navigate. Therefore, the parental privacy control model collapses in practice and in theory.[257]

Consider the notice aspect of the notice-and-consent privacy approach. Widely adopted forms of notice do not work.[258] Adults do not have the time to read them.[259] Even simplified notices appearing as pop-ups do not give adults sufficient information to make privacy choices.[260] Adults cannot comprehend the privacy risks of their own behavior (let alone their children's behavior) because there are too many privacy policies to read, too many uncertain consequences, and too many vague terms.[261] Parents cannot overcome the well-documented cognitive limitations that make informed consent illusory. Parents cannot understand long, legalese privacy policies on behalf of children since they cannot understand those policies for themselves.[262]

[255] Legislative Solutions Hearing, supra note 98, at 01:12:34 (statement of David Brody, Managing Att'y, Digit. Just. Initiative, Laws.' Comm. for C.R. Under L.).

[256] Solove, supra note 26, at 1881, 1888–89; Ari Ezra Waldman, Privacy's Rights Trap, 117 Nw. U. L. Rev. Online 88, 99–100 (2022).

[257] Zahra Takhshid, Children's Digital Privacy and the Case Against Parental Consent, 101 Tex. L. Rev. 1417, 1432 (2023).

[258] Principles of the L.: Data Priv. § 3 cmt. a (Am. L. Inst. 2020).

[259] See Aleecia M. McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 I/S: J.L. & Pol'y for Info. Soc'y 543, 563 (2008) (finding that it would take 244 hours to read all the privacy policies one encountered in the year). Even privacy scholars, including us, who read these policies carefully, have a hard time understanding them! See Joel R. Reidenberg et al., Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding, 30 Berkeley Tech. L.J. 39, 86–88 (2015) (finding that even experts differ in their understandings of privacy policy terms).

[260] Principles of the L.: Data Priv., supra note 258.

[261] Takhshid, supra note 257, at 1420–21; see also Hartzog, supra note 25, at 64 ("[C]ontrol doesn't scale. The sheer number of choices that inundate users under a control regime is overwhelming to the point of futility."); Solove, supra note 26, at 1880–81; Waldman, supra note 256, at 99–100.

[262] Waldman, supra note 104, at 106–07.

Given that adults fall prey to online manipulation, digital addiction, and corporate data-extractive behavior,[263] parental control offers nothing for children. As Rashad Robinson, then-President of Color of Change, told a House subcommittee, "The lie that we simply need to 'put more control in the hands of users' is like stacking our supermarket shelves with poisons and expired foods and then saying we're simply giving consumers more choice."[264] Parents are choking on notice and choice. More parental control cannot and will not change the political economy of informational capitalism, which is rife with data-driven exploitation of adults and youth.[265]

In other words, the ideologies of parental control are radically deregulatory. Parents cannot stem the never-ending corporate exploitation of their children's personal data. To suggest that parents can choose privacy on kids' behalf is magical thinking. Under current law, parents cannot meaningfully restrain corporate use, sharing, and sale of their kids' personal data.

As one of us (Waldman) has argued, this model is a well-worn trick of businesses trying to avoid responsibility for the harms they cause and lawmakers catering to corporate interests.[266] Consider the plastics industry. Bottlers and their allies lobby against environmental laws that would curtail their profits in favor of recycling, which burdens individuals.[267] The industry does this because recycling "stress[es] the individual's act of disposal," shifting responsibility away from producers

[263] Gaia Bernstein, Unwired: Gaining Control over Addictive Technologies 7–9, 18–20, 80, 89 (2023); Press Release, Governor Kathy Hochul, Governor Hochul, Attorney General James, Senator Gounardes, and Assemblymember Rozic Take Action to Protect Children Online (Oct. 11, 2023), https://www.governor.ny.gov/news/governor-hochul-attorney-general-james-senator-gounardes-and-assemblymember-rozic-take-action [https://perma.cc/ES92-RPBG] (statement of Nily Rozic, Assemblymember, N.Y.).

[264] Holding Big Tech Accountable: Targeted Reforms to Tech's Legal Immunity: Hearing Before the Subcomm. on Commc'ns & Tech. of the H. Comm. on Energy & Com., 117th Cong. (2021) (statement of Rashad Robinson, President, Color of Change).

[265] This argument echoes Paul Butler and other critical legal scholars' critique of rights. That critique noted how using individual rights as a means of addressing structural injustice can make the structural problem worse by creating the facade of a solution. See, e.g., Paul D. Butler, Poor People Lose: *Gideon* and the Critique of Rights, 122 Yale L.J. 2176, 2178–79 (2013); Waldman, supra note 256, at 102–03 (applying the critique of rights argument to the privacy context).

[266] Waldman, supra note 256, at 100–01.

[267] Frontline: Plastic Wars (PBS television broadcast, aired Mar. 31, 2020), https://www.pbs.org/wgbh/frontline/documentary/plastic-wars/.

that inundate us with plastic in the first place.[268] Under this model, climate catastrophe is not the result of corporate malfeasance, but rather "human laziness and ignorance."[269] Recycling in lieu of legal obligations enables lawmakers to do nothing about the underlying plastics business and the harm that it causes to the environment. "When responsibility for environmental problems is individualized, there is little room to ponder institutions, the nature and exercise of political power, or ways of collectively changing the distribution of power and influence in society—to, in other words, 'think institutionally.'"[270] The same is true here. When youth intimate privacy is the parents' responsibility, lawmakers avoid having to vote on measures that would upset corporate donors.

Therefore, parents find themselves pulled in opposite directions. On the one hand, they know that they cannot keep up with technology, their children's use of it, and the steps that they are expected to take to monitor that use. On the other hand, they fear for their children's privacy and safety, making calls for further surveillance seem attractive. This push-pull is unsustainable and unfair to parents and guardians.

The parental control model is doing young people a profound disservice. Current law neither prepares young people to protect themselves nor helps nurture them as democratic citizens. In many cases, it is not protecting young people at all. At worst, the parental control model can be dangerous, especially for children from minoritized groups; at its most benign, parental control is ineffective and leaves in place structural injustices hidden behind an avalanche of privacy policies. Youth privacy law is ripe for reform, a task the next Part tackles.

IV. REIMAGINING THE YOUTH INTIMATE PRIVACY PROJECT

This Part lays out four principles that help us begin to reimagine how we might secure intimate privacy for young people. Our overarching goal is to support youth intimate privacy so young people can flourish during formative periods of their lives. The first step toward doing so is to *respect youth voices*. Although they are the targets of youth privacy law, young people have been traditionally left out of the policymaking process, with some noted exceptions. The second principle is *legal reform*. Tech

[268] Michael F. Maniates, Individualization: Plant a Tree, Buy a Bike, Save the World?, 1 Glob. Env't Pol. 31, 43 (2001).
[269] Id.
[270] Id. at 33.

companies must be regulated, and indeed young people have called for precisely that. The third principle is *collaboration* between parents, schools, and young people themselves to secure youth intimate privacy. The fourth is a *support* principle. Parents should not be the only ones responsible for protecting youth intimate privacy. This disserves parents and children. We recognize that parents will be involved in their children's digital lives; we seek to support and decenter them at the same time. These principles aim to replace concentrated power and isolation with legal obligations and multi-stakeholder collaboration.

A. First Principle: The Importance of Youth Voices

Any conversation and policymaking effort about children's privacy should begin with young people themselves. Youth privacy law has largely erased children.[271] Although lawmakers often use the rhetoric of children's protection, far too many of them do not talk to the very youth who will be impacted.[272] Young people should be seen and heard.

Lawmakers should solicit the views of young people to understand the intimate privacy that they want and expect. The perspectives of youth from minoritized groups are especially important; they may have different (and, perhaps, greater) privacy needs than other young people. We need only look to the surveillance of students for proof of concept. The most surveilled public-school students are often the most vulnerable.[273] Surveillance products have disproportionately increased the discipline and suspension faced by Black and Hispanic students; they have had an outsized adverse impact on the self-expression, physical safety, and well-being of LGBTQ+ students.[274] Lawmakers need to hear from youth from marginalized communities.[275]

[271] Dailey & Rosenbury, supra note 242, at 1455–57; id. at 1468–69 ("The authorities framework fails to recognize this rich diversity [of children's experiences] because it ties children's needs and interests to a baseline of adulthood, regarding children as pre-adults, always in the act of becoming full persons but not necessarily full persons in their own right.").

[272] Iowa Senate, Senate Floor Audio on Sen. File 496, Gen. Assemb., at 06:51:13 (Apr. 19, 2023), https://www.legis.iowa.gov/dashboard?view=video&chamber=S&clip=s2023041905 3010270&dt=2023-04-19&offset=647&bill=SF%20496&status=r [https://perma.cc/L2FD-L RJ7] (statement of Sen. Brad Zaun).

[273] Citron, Surveilled Student, supra note 15, at 1461–62.

[274] Id.

[275] Given the disproportionate surveillance of young people from marginalized backgrounds, it may be difficult for lawmakers to convince students of color to talk to them. This challenge is something that lawmakers must consider and work to address. We thank Anita Allen for talking to us about this issue. See, e.g., Anita L. Allen, Dismantling the "Black

Lawmakers should listen to young people when they speak in the public square as well. Students have spoken eloquently about discriminatory dress codes in schools and worked to develop gender-neutral rules that do not unfairly punish young girls.[276] Young people, tired of policymakers who refuse to do anything about the epidemic of school shootings, have developed their own youth-centered campaigns, marched for safer schools, and lobbied local, state, and national policymakers.[277] Youth-centered privacy campaigns are long overdue. And they should be welcomed. Young people are digital natives and most familiar with how they navigate the privacy risks of digital expression. They are, as Emily Buss notes, "in this sense . . . more qualified than anyone else to judge their developmental needs,"[278] perhaps especially so in the technical context. Parental involvement has its place, too. Adults can buoy youth activism by helping organizing efforts, so children can define the privacy issues for which they want to fight; and by creating spaces to bring youth together.[279]

In place of the kind of absolute parental control characterizing youth privacy law today, policymakers should aim for a balance. If choice is going to remain part of any privacy law agenda, integrating young people in its machinery is good policy. Doing so enables them to become even more effective decision-makers when they are adults,[280] when life decisions are, if not necessarily always weightier, certainly more frequent. Parental control may make sense for some young children, many of whom are not allowed on social media anyway. But proposals to subject older teenagers to absolute parental control are stifling and counterproductive, denying young adults their privacy and generating mistrust within

Opticon": Privacy, Race Equity, and Online Data-Protection Reform, 131 Yale L.J.F. 907, 910 (2022); see also Simone Browne, Dark Matters: On the Surveillance of Blackness 17 (2015).

[276] Cheryl Bratt, Top-Down or from the Ground?: A Practical Perspective on Reforming the Field of Children and the Law, 127 Yale L.J.F. 917, 937 (2018).

[277] Id. at 936–38.

[278] Emily Buss, Allocating Developmental Control Among Parent, Child and the State, 2004 U. Chi. Legal F. 27, 35.

[279] Sasha Costanza-Chock, Berkman Ctr. for Internet & Soc'y, Youth and Social Movements: Key Lessons for Allies 2–4 (2012), https://cyber.harvard.edu/sites/cyber.harvard.edu/files/KBWYouthandSocialMovements2012_0.pdf [https://perma.cc/4DU4-SAPY] (discussing youth activism in civil rights movements, including in the citizenship and LGBTQ+ contexts, where recognition and respect for young people's agency is necessary ensure that they are neither invisible nor dismissed as unserious in those movements).

[280] Buss, supra note 278, at 35.

families. Prioritizing youth voices could shift public and lawmaker attitudes. It would accord youth with greater respect and clear recognition of their entitlement to privacy as citizens.[281] Young people would hear the message that their intimate privacy matters and deserves protection.[282] Further progress toward youth intimate privacy becomes more possible with that foundation of respect.

State lawmakers have shown us that hearing from youth about the privacy that they want and expect is possible and desirable. We now turn to those voices and the structural reforms that they support.

B. Second Principle: Structural Reform

Reform should begin with the companies whose practices endanger youth intimate privacy and safety. The reflexive turn to parental control has mostly excused industry from taking responsibility for the harms it causes to youth intimate privacy. For instance, COPPA does not ban (or limit) corporate exploitation of the personal data of youth under thirteen whose parents have consented to the data collection.[283] It enables the handling of youth intimate data until parents take steps to stop it, which, given limits on time, attention, and understanding of privacy policies, they hardly ever do.[284] Privacy law's focus on notice-and-consent has operated as an excuse for indifference to rampant corporate collection and manipulation of young people's data. This creates what Julie Cohen has called a "zone of legal privilege," which insulates corporate business models, recommendation algorithms, and curated search hits from scrutiny.[285]

We need a more active role for law in regulating data-extractive practices aimed at youth.[286] The parental control model absolves government of the responsibility of affirmatively helping parents in the

[281] On expressive effects, see Citron, supra note 146, at 404–14; Sunstein, supra note 146, at 2022–24; Tokson & Waldman, supra note 146, at 279–84; Deborah Hellman, The Expressive Dimension of Equal Protection, 85 Minn. L. Rev. 1, 39–40 (2000).

[282] See Citron, Surveilled Student, supra note 15, at 1472.

[283] 15 U.S.C. §§ 6501–6502; 16 C.F.R. § 312.6 (2025).

[284] See supra notes 260–62 and accompanying text.

[285] See Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism 49 (2019).

[286] This echoes Anita Allen's famous lament that, historically, "[w]omen have had too much of the wrong kinds of privacy" (family privacy and "forced isolation") and too little of the right kinds of privacy (decisional autonomy over their bodies, for example). Anita L. Allen, Uneasy Access: Privacy for Women in a Free Society 37, 52 (1988).

project of securing youth privacy. Although we recognize that the state's entanglements with families can reflect bias,[287] the state can and should provide value by regulating corporate practices and supporting parents' efforts to raise their children while cognizant of and avoiding bias.[288]

We need substantive commitments to youth privacy, rather than procedural protections that overburden and overwhelm parents.[289] That could mean setting privacy defaults to their most private and giving young people opportunities to adjust them to the extent that youth would be inclined to use those adjustments (and to the extent that services would not use those opportunities to manipulate young people).[290] It could mean turning off recommendation algorithms and producing chronological feeds for young users. It could mean disaggregating young people's data from for-profit business models driven by targeted advertisements and recommendation algorithms.[291] It could mean limiting surveillance

[287] See, e.g., Dorothy E. Roberts, Child Welfare and Civil Rights, 2003 U. Ill. L. Rev. 171, 172; Kari E. Hong, Parens Patri[archy]: Adoption, Eugenics, and Same-Sex Couples, 40 Cal. W. L. Rev. 1, 31–32 (2003); Clare Huntington & Elizabeth S. Scott, Conceptualizing Legal Childhood in the Twenty-First Century, 118 Mich. L. Rev. 1371, 1414 (2020); Dorothy E. Roberts, The Value of Black Mothers' Work, 26 Conn. L. Rev. 871, 875 (1994).

[288] See LaToya Baldwin Clark, The Problem with Participation, 9 Mod. Am. 20, 21 (2013) (arguing that exclusive parental responsibilities for raising children systematize racist outcomes for children of color by absolving the state of the responsibility to change biased structures and support children in need). Our legal reform principle would not pit parents against the state but rather enlist legal reform to regulate the extractive behavior of tech companies. In a follow-up article, we explore youth privacy's constitutional underpinnings and its inadequate triadic conception of youth-related problems. We argue that law needs a far more nuanced approach to youth privacy issues today, particularly a wider aperture to see the four crucial players (youth, parents, the state, and tech companies) and to recognize that power resides most heavily in tech companies. Danielle Keats Citron & Ari Ezra Waldman, Youth Privacy's Constitutional Reckoning, 59 Ga. L. Rev. (forthcoming Apr. 2026).

[289] See Cohen, supra note 285, at 160–63, 188–89; Ari Ezra Waldman, Privacy Law's False Promise, 97 Wash. U. L. Rev. 773, 776 (2020).

[290] Ava Smithing, the Director of Advocacy for the Young People's Alliance, explained that changing her preferences and clicking "not interested" and "don't show me ads like this" did not stop social media companies from targeting her when she was younger with advertisements for starvation diets and posts with unattainable beauty goals. Legislative Solutions to Protect Kids Online and Ensure Americans' Data Privacy Rights: Hearing Before the Subcomm. on Innovation, Data & Com. of the H. Comm. on Energy & Com., 118th Cong. (2024), https://www.congress.gov/118/meeting/house/117146/witnesses/HHRG-118-IF17-Wstate-SmithingA-20240417.pdf [https://perma.cc/JZ82-5P75] (statement of Ava Smithing, Dir. of Advoc., Young People's All.).

[291] For instance, in a settlement with New York Attorney General Letitia James, the College Board agreed not to share student data for commercial and marketing purposes. Press Release, Off. of N.Y. State Att'y Gen. Letitia James, Attorney General James and NYSED Commissioner Rosa Secure $750,000 from College Board for Violating Students' Privacy

software used by schools unless they are shown to help students.[292] It could mean radically scaling up regulators' institutional capacity to monitor, investigate, and contest corporate data practices. It could mean an end to corporate profits from youth personal data.[293]

These potential structural reforms resonate with what we hear from youth about the privacy protections that they want and those that they do not want. First, for what young people do not want: in the examples that we have of young people testifying before state lawmakers, young people have *not* called for parental control. Some have called for independence from parents, while others want powerful entities to help their parents.[294]

Now for what youth do want: young people have made clear that they want companies to be required to protect their privacy by default and by design. For instance, Andrew Lear, a high school junior in Maryland, called for the state to pass a law that would guarantee "higher privacy settings by default," so companies would not be able to use his personal data to steer him to negative content.[295] Arielle Geismar told the Maryland Senate that the core problem "was the design" of Instagram, whose algorithm showed her images and videos of "disordered eating . . . content" that encouraged her to starve herself.[296] These young people did not need to be eighteen or twenty-one to understand that parental control could not protect their privacy, health, or safety; they appreciated that the underlying business model and system design

(Feb. 13, 2024) [hereinafter College Board Press Release], https://ag.ny.gov/press-release/2024/attorney-general-james-and-nysed-commissioner-rosa-secure-750000-college-board [https://perma.cc/GGR6-W9HV].

[292] Citron, Surveilled Student, supra note 15, at 1469.

[293] Citron, Fight for Privacy, supra note 13, at 159–62.

[294] When Ms. Galvani testified before the Vermont Senate Committee on Economic Development, she noted that her mother was too overwhelmed to monitor her online activities. Rather than embracing that freedom—she called herself "free-range"—Galvani asked lawmakers to provide support for her mother. Vermont Senate Video, supra note 179, at 16:00 (statement of Juniper Galvani). On the other hand, Hannah Zoulek, who testified before the Utah House Judiciary Committee, pushed back against lawmakers' and parents' rights groups' attempt to mandate parental supervision of children's social media accounts. Utah House of Reps., Hearing on H.B. 311 Before the H. Comm. on the Judiciary, 2023 Gen. Sess., at 01:36:50 (Feb. 3, 2023), https://le.utah.gov/av/committeeArchive.jsp?timelineID=222196 [https://perma.cc/H8CA-HBVH] (statement of Hannah Zoulek).

[295] Maryland House of Delegates Economic Matters Committee, ECM Committee Session, 2/13/2024 #1, at 01:41:22 (YouTube, Feb. 13, 2024) [hereinafter Maryland House ECM Video], https://www.youtube.com/watch?v=rpmStHTvlXs [https://perma.cc/L2G9-B4Q7] (statement of Andrew Lear).

[296] Maryland Senate Finance Committee Video, supra note 97, at 05:37:55 (statement of Arielle Geismar).

exploited their personal data and jeopardized their health and safety in the name of profit.

Consider the experience of the Vermont Kids' Code.[297] Teenagers testified before both houses of the legislature, speaking about their own experiences, the impossibility of parental control in practice, and the need for changes in the design of tech platforms.[298] The Vermont Kids' Code required technology companies to set default settings at "a high level of privacy" and to inform young people when they were being tracked.[299] It prohibited the sale of young people's personal data; it banned dark patterns that manipulated children.[300] Location tracking of children could occur only if children were informed beforehand.[301]

To be sure, several factors contributed to the Vermont legislature's approach, including active involvement from the state's attorney general and a progressive legislature willing to hold exploitative industry to account.[302] But the presence of youth voices and their interest in structural reform is notable and rare among state privacy law debates. We should note that the Vermont legislature passed the Vermont Kids' Code only to face a gubernatorial veto; young people's wishes came so close to being realized.

These structural reforms should not include requiring companies to provide parents with access to their children's social media accounts.[303] The law should not further enhance parental power over children's lives. As a baseline matter, parents have extraordinary power and influence over their children. For instance, parents can and do demand that children show them their personal devices and accounts.[304] They can and do require that

[297] The bill did not survive the governor's veto. See Press Release, Off. of Governor Phil Scott, Action Taken by Governor Phil Scott on Legislation (June 13, 2024), https://governor.vermont.gov/press-release/action-taken-governor-phil-scott-legislation-june-13-2024 [https://perma.cc/M767-QRUG].

[298] Vermont Senate Video, supra note 179, at 07:45 (testimony of Juniper Galvani); Vermont House Committee on Commerce and Economic Development Video, supra note 200, at 01:08:00.

[299] S. 289, 2024 Gen. Assemb., Reg. Sess. § 2449d(a)(1)–(2) (Vt. 2024).

[300] Id. § 2449e(a)(6), (9).

[301] Id. § 2449e(a)(10).

[302] See Press Release, Off. of Vt. Att'y Gen. Charity Clark, Statement from Attorney General Clark on Governor's Veto of H.121, Vermont Data Privacy Act (June 14, 2024), https://ago.vermont.gov/blog/2024/06/14/statement-attorney-general-clark-governors-veto-h121-vermont-data-privacy-act [https://perma.cc/6F3U-NKGY].

[303] See supra Part I.

[304] Parental authority over children's personal lives is sweeping because parents are assumed to possess "what a child lacks in maturity, experience, and capacity for judgment

children download tracking software to their cellphones; the parental control app business is booming. We do not need the law's help here. If the law required parents to check children's online accounts or to download spyware on children's phones, there would be less opportunities for young people to claim and enjoy intimate privacy.

We have seen attempts to depart from the parental control model. During the Biden Administration, federal law enforcers took some steps away from the parental control model. In 2022, the FTC called for comments about alternatives to parental control. Among the ninety-five questions in the FTC's Advance Notice of Proposed Rulemaking ("ANPR") about the surveillance information economy was whether "parental consent [is] an efficacious way of ensuring child online privacy."[305] The FTC asked the public for suggestions about alternative or complementary mechanisms.[306] The FTC appeared to be considering restrictions on corporate behavior, new rules from lawmakers and regulations, and changes to advertising-based business models.[307] The FTC's rulemaking effort focused on structural changes to extractive information business models.

During the Trump Administration, federal regulators are reverting back to parental control. The proposed rulemaking will likely be abandoned now that Andrew Ferguson has become Chair of the FTC, FTC Commissioners Alvaro Bedoya and Rebecca Slaughter have been fired, and Commissioner Melissa Holyoak has taken one of their seats.[308] While

required for making life's difficult decisions." Troxel v. Granville, 530 U.S. 57, 68 (2000) (plurality opinion) (quoting Parham v. J.R., 442 U.S. 584, 602 (1979)). As Clare Huntington and Elizabeth Scott explain, children are "largely invisible as legal persons, presumed to be vulnerable, dependent, and incapable of making self-regarding decisions." Huntington & Scott, supra note 287, at 1373. "[P]arental rights [have] continue[d] to receive substantial deference in American law" on the presumption that parents act in their children's best interests. Id. at 1396. Parents and guardians have "authority to impose constraints on their children's speech, access to information, and engagement in political and religious activities" at home, at school, and in other aspects of children's lives. Restatement of Child. & the L. ch. 18, intro. note (Am. L. Inst., Tentative Draft No. 5, 2023).

[305] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273, 51282 (Aug. 22, 2022).

[306] Id.

[307] Id.

[308] Hearing Before the Subcomm. on Fin. Servs. & Gen. Gov't of the H. Comm. on Appropriations, 119th Cong. 1, 14 (2025), https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-Chairman-Andrew-N-Ferguson-FSGG-Testimony-05-15-2025.pdf [https://perma.cc/MBA3-S5W5] (statement of Andrew N. Ferguson, Chairman, FTC) (testifying that "the Trump-Vance FTC has gone back to the agency's roots. Vigorous enforcement of the law is [the

Chairman Ferguson has expressed at least a rhetorical interest in protecting children's privacy, his FTC has begun investigating practices that "erode parental authority."[309] Chairman Ferguson has declared parental control as the right way to approach children's privacy.[310]

No matter the direction that the FTC takes, the agency is constrained within the limits of its authorizing statute to regulate "unfair or deceptive" business practices.[311] It has limited resources to move beyond its traditional toolkit of procedure-focused consent decrees.[312] What is more, the FTC remains committed to the parental control model, most recently evidenced by its COPPA Rule amendments to give parents control over advertisements targeted to children.[313] Luckily, the FTC is not the only privacy policymaker in view.

State attorneys general ("AGs") have long been privacy norm entrepreneurs and leaders.[314] From social media's earliest days, they have sought fines and structural design changes to data-extractive products.[315] In 2008, after forty-nine state attorneys general formed a task force to investigate child predators' use of social media, the then-dominant platform MySpace agreed to design changes in default settings to prevent strangers over eighteen years old from contacting youth who were sixteen

FTC's] focus. Congress established the FTC to be a cop on the beat for . . . markets, not to make the rules;" and underscoring the agency's interest in reinforcing parental consent and age verification); Lexie White, At GPS 2025: FTC's Holyoak Outlines Next Steps for US Enforcement, Innovation, Int'l Ass'n of Priv. Pros. (Apr. 23, 2025), https://iapp.org/news/a/at-gps-2025-ftc-s-holyoak-outlines-next-steps-for-us-enforcement-innovation [https://perma.cc/GS4Q-UBHY] (describing Holyoak's speech at the 2025 IAPP conference, where she said the FTC would continue to ensure that parents have "meaningful choices to protect their children").

[309] Press Release, Fed. Trade Comm'n, FTC Releases Tentative Agenda for Attention Economy Workshop on June 4 (May 19, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/05/ftc-releases-tentative-agenda-attention-economy-workshop-june-4 [https://perma.cc/VM2F-N5Z7] (explaining that the workshop would examine "how Big Tech companies impose addictive design features, erode parental authority, and fail to protect children from exposure to harmful content").

[310] Suzanne Smalley, FTC Chair Implores Congress to Strengthen Children's Online Privacy Protection Law, The Record (June 4, 2025), https://therecord.media/ftc-chair-implores-congress-to-strengthen-childrens-privacy-law [https://perma.cc/C656-R8KR].

[311] 15 U.S.C. §§ 45(n), 57a(a).

[312] See Solove & Hartzog, supra note 102, at 610–19.

[313] See Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2025).

[314] Citron, Privacy Policymaking, supra note 102, at 749–50.

[315] Adam Thierer, The MySpace-AG Agreement: A Model Code of Conduct for Social Networking? 1–2 (Progress & Freedom Found., Paper No. 15.1, 2008).

and under.[316] In 2023, a bipartisan coalition of state attorneys general, led by Colorado AG Phil Weiser, sued Meta and other social media companies for unfairly exploiting children's personal data to manipulate them to stay online, show them destructive content, and cause serious health problems.[317]

We commend these efforts to protect youth intimate privacy.[318] Laws and law enforcement efforts that secure youth intimate privacy interests would have important expressive effects.[319] They would say to young people that their intimate privacy is of primary importance and that their privacy expectations should be met. This would be a critical step forward for law. Now to nonlegal efforts.

C. Third Principle: Collaboration

Just as lawmakers should seek input and help from young people, so should parents. For parents, collaboration has enormous potential to enhance their relationships with their children, break their isolation, and obtain support. Crucially, when it comes to parents and children, the collaboration principle would largely be driven by personal imperative rather than by law.

Parents who seek to support rather than control their children should collaborate with young people as well as with their schools and teachers. Beginning with parent-child collaboration, we recommend a collaborative posture informed by anti-subordination commitments. An anti-subordination approach would recognize children's unique dependence on parents for support and guidance. Parents would talk to their children about their online activities, conscious of hierarchies, and work to lift up

[316] Citron, Privacy Policymaking, supra note 102, at 776.

[317] Press Release, Off. of Colo. Att'y Gen. Phil Weiser, Bipartisan Coalition of Attorneys General File Lawsuits Against Meta for Harming Youth Mental Health Through Its Social Media Platforms (Oct. 24, 2023), https://coag.gov/press-releases/bipartisan-coalition-of-attorneys-general-file-lawsuits-against-meta-for-harming-youth-mental-health-through-its-social-media-platforms/ [https://perma.cc/C85L-T45N].

[318] Regrettably, some state AGs have fallen into the trap of parental control. After suing a student surveillance company for tricking students into providing personal data that the company shared with marketers, forty-two state AGs settled the lawsuit after the company agreed to allow parents to opt out of the surveys. Citron, Privacy Policymaking, supra note 102, at 776 n.193. In a settlement with New York AG Letitia James, the College Board agreed not to share student data for commercial and marketing purposes. College Board Press Release, supra note 291.

[319] On the law's expressive effects, which refer to the law's role in influencing the public's perception of right and wrong, see supra note 146.

those disadvantaged by the family's traditional power structures.[320] We do not deny that a parent-child hierarchy exists, but parents would be wise to adjust that hierarchy for the good of youth development and youth intimate privacy.

This argument will not appeal to parents who have no interest in working with their children or whose views drive them to reject their children's burgeoning identities. We understand that limitation. Instead, we make this pitch to parents who accept their children's burgeoning identities and want to prioritize their children's interests. This approach would enhance their relationships with their children, rather than undermine them.

How might collaboration work? To the extent feasible, parents would talk to their children about their online activities in ways that support their children's growth, resilience, and independence. Of course, those conversations would be different; they would depend on children's capabilities and vulnerabilities as well as their desire to socialize and engage online. We encourage parents to work with their children to ensure that their needs are met, including their desire and need for intimate privacy.

To be sure, this is not easy. Parents would have to resist the pitch that responsible parenting means continuously tracking and surveilling children. They would have to recognize that children want to engage socially online and treat children as partners in protecting youth intimate privacy and preventing harm.

Collaboration would entail parental recognition of youth intimate privacy interests. This is especially critical for queer youth, who need independence and psychological space to come out to their parents in their own time, if they wish to do so and if they think they could safely share their sexual orientation or gender identity. This is the youth intimate privacy that young people want.

Parents should have ongoing conversations with their kids to strategize ways to protect their intimate privacy and address safety and health concerns.[321] This approach would mean that parents would have to cede

[320] See Scott Skinner-Thompson, Privacy at the Margins 6 (2021) (proposing an anti-subordination agenda for privacy law).

[321] One of us (Citron) and her daughter wrote about this very effort when her daughter was in high school. Danielle Citron & Julia Jean Citron, Parents, Teens, and Technology: Starting the Conversation, Forbes (Aug. 19, 2015, 10:42 AM), https://www.forbes.com/sites/danielleci

some power. It would require parents to trust children as they use online tools. Keeping the lines of communication open for children to talk to parents engenders trust; continuous surveillance and control engender distrust.[322]

Permitting children, especially adolescents, to decide the extent to which they share personal information with their peers (and others) online, enabling them to establish online networks and accounts without parental tracking, and trusting them to set boundaries around their intimate lives are all key to youth self-development. This will allow adolescents to learn the skills of independence and autonomy. It will allow youth to work on self-protection as they wrestle with risk and mistakes.[323]

These suggestions are rooted in parental choice, not law. But there are ways that law could nudge collaboration. The Vermont Kids' Code offered a modest example. It would have required online services to notify children before their parents started tracking their locations.[324] To be sure, parents who have good relationships with their children do not need law to encourage that sort of communication. Parents can just ask their children for permission before tracking their locations. Engaging, working, and negotiating with children about privacy can lead to better outcomes and happier parent-child relationships.[325]

In short, the collaborative principle asks parents to shift their role from authority figure to partner. To be sure, this is not always possible, particularly when parents and children do not have open lines of communication or have frayed or nonexistent relationships. We aim our hopes toward collaboration where it is possible.

A collaborative posture between teachers, students, and parents would be beneficial as well. At present, educators are facing a parental rights movement aiming to prevent young people from being able to reveal their

tron/2015/08/19/parents-teens-and-technology-starting-the-conversation/ [https://perma.cc/8MVV-48K6].

[322] See supra Section IV.A.

[323] Livingstone et al., supra note 188, at 17–22.

[324] S. 289, 2024 Gen. Assemb., Reg. Sess. § 2449e(a)(10) (Vt. 2024).

[325] Pamela Wisniewski, Haiyan Jia, Heng Xu, Mary Beth Rosson & John M. Carroll, "Preventative" vs. "Reactive:" How Parental Mediation Influences Teens' Social Media Privacy Behaviors, *in* Ass'n for Computing Mach., CSCW 2015: Proceedings of the 18th ACM Conference on Computing Supported Cooperative Work & Social Computing (2015), https://faculty.ist.psu.edu/xu/papers/cscw2015pam.pdf [https://perma.cc/8MS4-Y88J] (distinguishing "direct parental intervention" and "active parental mediation").

gender identities to teachers with the expectation of confidentiality.[326] Educators face a difficult choice—their role is to educate, support, and nurture children's citizenship skills, not to betray their confidences and undermine their personal growth. Requiring teachers to out students to their parents is corrosive to parent-child and parent-teacher relationships. It introduces distrust and antagonism. Teachers do not want to betray their students' confidences, and they do not want to create unnecessary tensions with parents; there is already enough opportunity for teachers to clash with parents who might demand higher grades in ways that would disserve the educational mission.

In place of that precarity, educators should be permitted to protect youth intimate privacy in their roles as trusted adults for students and as partners to parents in a child's development. As is true for parents, teachers should not invade students' intimate privacy. To do that, schools and school districts would have to rethink the continuous surveillance of public-school students' laptop activity.[327] Schools should expand their digital citizenship curriculum to include parent-student education about collaborative efforts that can be taken to protect youth intimate privacy and online safety.[328]

Surveillance of students is often a well-intentioned yet reflexive step taken in the name of identifying students' suicidal ideations and protecting schools from potential violence.[329] But no impartial evidence exists that suggests such surveillance actually meets those goals.[330] Dragnet surveillance makes young people unnecessarily liable to control and domination during times of self-discovery, exploration, and anxiety.[331] Schools' contracts with private companies inject profit-seeking corporate practices into nonprofit educational systems.[332] In short, the harms are not worth the costs to intimate privacy. No potential benefits of such surveillance have been shown at all.

[326] See Mary Ziegler, Maxine Eichner & Naomi Cahn, Retrenchment by Division: The New Politics of Parental Rights, 123 Mich. L. Rev. 669, 707–09 (2025) (situating so-called "given name" acts in the context of a powerful parents' rights movement).

[327] Citron, Surveilled Student, supra note 15, at 1450–53. Congress should step in to curtail that surveillance. Id. In the absence of such reform, schools can and should act on their own.

[328] Citron, Fight for Privacy, supra note 13, at 183–84.

[329] Citron, Surveilled Student, supra note 15, at 1463.

[330] Id. at 1464.

[331] Id. at 1457–63.

[332] Id. at 1464–65.

D. Fourth Principle: Support for Parents

As we have shown, youth privacy laws and proposals give parents more control and more responsibility over children's online accounts and activities.[333] This approach leaves parents alone to worry about their children's online activities with little meaningful ability and bandwidth to help them. This burdens parents rather than empowers them.

Children recognize and worry about their parents' exhaustion. Juniper Galvani, the Vermont youth advocate, concedes that "there's just no way" her mother could effectively handle monitoring all of her online activities.[334] Parents testifying before state legislatures say that they do not have the time to monitor their children's online activities in real time or after the fact.[335] Research supports these anecdotes. Snap's CEO and cofounder Evan Spiegel testified before the Senate Judiciary Committee that fewer than one percent of parents use Snap's parental monitoring tools.[336]

A primary consequence of parental control is isolation. Parents are disconnected from individuals, groups, and institutions that could help them as they work collaboratively with their kids on using digital services responsibly and safely. Contrary to politically motivated myths, parental isolation from community is an aberration. Family law scholar Clare Huntington argues that families often rely on the state, community groups, workplaces, and other social institutions to find happiness and fulfillment.[337] Parents should do so too when it comes to privacy.

---

[333] See supra Subsection I.A.1.

[334] Vermont Senate Video, supra note 179, at 16:00 (statement of Juniper Galvani).

[335] Id. at 33:00 (statement of Heidi Schumacher) ("[A]s a pediatrician who's interested in this space, who thought I'd done all the steps and followed the instructions of the app to protect my four-year-old child in a benign video-watching scenario . . . how can you possibly expect other parents and caregivers to be positioned to be continuously responsible for the safety and privacy of their youth online?"); Maryland Senate Finance Committee Video, supra note 97, at 06:26:20 (statement of Beth Jarrett) ("I was quite upset to realize that the so-called control I thought I had set up was not working the way I thought it would and he was, in fact, able to play with and talk to strangers. . . . As adults, we may not have the technological savvy to ensure that safeguards are implemented properly.").

[336] S. Comm. on the Judiciary, 118th Cong., Questions for the Record for Mr. Evan Spiegel, CEO and Cofounder of Snap, Inc. 1–2 (Comm. Print 2024) (questions from Sen. Richard Durbin), https://www.judiciary.senate.gov/imo/media/doc/2024-01-31_-_qfr_responses_-_spiegel.pdf [https://perma.cc/ZU5H-BN65] (noting that only two hundred thousand parents opted to use Snap's Family Center tool, compared to Snap's sixty million daily active users under the age of eighteen).

[337] See Clare Huntington, Failure to Flourish: How Law Undermines Family Relationships 157–58 (2014).

Teachers and counselors, advocacy organizations, and local leaders *could* help parents as they work to secure youth intimate privacy.[338] They could educate parents and young people together about online risks and the available tools for managing those risks.[339] They could offer parents insights into how to talk with their children about online privacy. They could bring together parents and students on back-to-school nights or at other events to discuss the expectations of youth and their parents when it comes to intimate privacy and safety. Parents and students could be encouraged to come up with a plan on how to handle discussions about social media and online activities. Schools could offer clinics for families about online safety and intimate privacy. And they could galvanize and organize parents to advocate for change. Parents need this sort of help.[340] When parents are isolated in their role as privacy deciders, they miss the assistance of interested and supportive community members.

Not only does the parental control model isolate and burden parents, but it also keeps children from individuals, groups, and institutions that could help them tackle safety risks. Sometimes, risks to children are posed by parents, as we have seen for LGBTQ+ youth and young influencers exploited by their parents.[341] Under the parental control model, youth cannot confide in individuals, groups, and institutions that could help them if everything will get back to parents who might abuse them.[342] Exclusive parental control crowds out practical and legal support networks that could help young people. This must change.

CONCLUSION

Youth intimate privacy is at a crossroads. Justifiably concerned about online harms, policymakers have a choice. They can continue an almost unbroken line of youth privacy laws that burden parents (who end up being primarily mothers and women guardians) with the sole responsibility of protecting their children's privacy, or they can change

[338] Laura A. Rosenbury, Between Home and School, 155 U. Pa. L. Rev. 833, 834–36, 843–44 (2007). See generally id. at 885–89 (citing case examples of advocacy groups and legislators supporting parental control over youth privacy).

[339] Citron, Fight for Privacy, supra note 13, at 183–84.

[340] Maryland House ECM Video, supra note 295, at 01:46:10 (statement of Liz Park, Md. Ass'n of Youth Serv. Bureaus).

[341] See supra Section III.C.

[342] This happens through surveillance of social media or school tattling, among other policy-driven possibilities explored in Part I.

course and take a path of support, collaboration, and legal and structural reform. This Article has laid the foundation for such change.

In this Article, we have identified the invisibility of youth in youth privacy law and highlighted the difference between the protection of youth intimate privacy and the law's chosen policy lever—parental control. We have interrogated the rationales for the parental control model and found them lacking at best or dangerous at worst. In place of parental control, this Article has outlined the beginnings of an approach that is youth-centered, collaborative, and dedicated to structural reform. At its core, this model recognizes that everyone has a responsibility to construct youth privacy.

Doing so could not be more important. Online harms are metastasizing; young people are calling for reform; parents are crying out for help. But help is not what more parental control delivers. Instead, it promises more burdens for parents while absolving technology companies of their responsibilities. In other words, parental control seems empowering on the surface. In reality, it is ineffective, contradictory, and potentially harmful to the very people the model is supposed to help. This Article has initiated a youth intimate privacy agenda. That agenda requires the attention of scholars, advocates, and policymakers before it is too late for a generation of young people habituated to and dominated by surveillance.