CHAPMAN LAW REVIEW

Citation: Mason R. Clark, *It Takes a Village (To Raise Children's Privacy)*, 29 CHAP. L. REV. 495 (2026).

It Takes a Village (To Raise Children's Privacy)

Mason R. Clark

CONTENTS

It Takes a Village (To Raise Children's Privacy)

Mason R. Clark∗

Raising children is an expensive and (mostly) rewarding commitment. Many parents, guardians, and caregivers are willing to invest in indestructible car seats, private schools, and organic, farm-fresh, whole-grain, low-sugar, dye-free, naturally flavored foods. Is it reasonable to ask them to invest in children's privacy? Surely companies can't expect parents to stand guard at the edge of a digital playground they never built and never (knowingly) agreed to let their children enter.

The digital age has profoundly reshaped children's privacy. It is hard to imagine listening to a podcast or scrolling on a social media platform without being bombarded by reports, rants, and reels about the unprecedented privacy risks children face online. Most federal and state privacy laws have failed to provide a comprehensive framework for safeguarding children's digital privacy. Scholars in this area have proposed legislative and regulatory reform and critiqued corporate malfeasance. This Article suggests it is time to reimagine the pay-for-privacy (PFP) model—an often-discredited model in which users pay for enhanced privacy protections—as a potential solution to minimize children's privacy risks.

This Article makes three arguments. Part II suggests parents are the primary gatekeepers of children's online privacy, and can responsibly manage their child's digital footprints (with some help). It also acknowledges deceptive corporate privacy practices and explores the pitfalls of PFP models. Part III argues companies are well-positioned to provide detailed reports to parents about their child's data and design child-centric privacy protections using revenue from a PFP model. Part IV then claims that the Federal Trade Commission (FTC) may have the expertise and the momentum to moderate between parents and companies in a PFP model.

Like the adage "it takes a village to raise a child," it takes a village to ensure children's privacy. As caregivers consider essential costs to raising children, this Article argues privacy may be one of those costs. PFP models, with appropriate oversight and equity, can enhance parental engagement and incentivize corporate accountability to foster a more private digital environment for children.

∗ Assistant Professor of Law at St. Mary's University School of Law. Former Bruce R. Jacob Visiting Assistant Professor at Stetson University College of Law (2023–2025).

I. INTRODUCTION

For readers who, like me, started using the internet as children in the early 2000s, they may remember their parents or caregivers watching Dateline NBC's *To Catch a Predator* television series[1] and constantly lecturing them about the internet's inherent danger. But no matter how many controls, filters, and blockers parents deployed to stop children from using chatrooms and websites, children were nonetheless able to create social media accounts (the most popular at the time being Myspace) and enter online chatrooms like AOL Instant Messenger to have months-long conversations with complete strangers. The rise of social media use among children and the ensuing moral panic about children's online activities resulted in controversial pieces of legislation like the Deleting Online Predators Act,[2] aimed at preventing children from using social networking sites and chatrooms. This and other pieces of legislation ultimately failed and, as discussed later in this Article, so too have many recent attempts to legislate children's online privacy.

Congress's repeated failure to pass comprehensive protections for children online is perhaps more distressing in today's modern digital age. Although concerns about children's digital privacy still include the "stranger danger" and/or cyberbullying fears from almost thirty years ago, parents are now also concerned about the massive amounts of data—personal, usage, or otherwise—collected from children by online platforms. From nightly news segments to viral TikToks, Americans are reckoning with a growing sense that today's children are also being surveilled and manipulated by the countless devices and platforms they use at home and even in the classroom. Pediatricians, psychologists, and even social media influencers have warned that children are living through a massive, uncontrolled experiment with childhood itself. Jonathan Haidt, one of the most visible critics of children's relationships with technology, calls this period of children's increased use of technology "The Great Rewiring," and he argues that technology has altered not just how children so-

1 For an interesting post hoc review of the controversial television series, see Adrian Horton, *To Catch a Predator: Exploring the Uneasy Legacy of the Controversial TV Series*, THE GUARDIAN (Jan. 27, 2025, at 07:56 ET), https://www.theguardian.com/film/2025/jan/27/to-catch-a-predator-sundance [https://perma.cc/H2JL-VMSS].

2 H.R. 5319, 109th Cong. (2006); *see* Wade Roush, *The Moral Panic over Social-Networking Sites*, MIT TECH. REV. (Aug. 7, 2006), https://www.technologyreview.com/2006/08/07/228481/the-moral-panic-over-social-networking-sites/ [https://perma.cc/8UN5-Q4F9].

cialize and learn, but how they are profiled, categorized, and monetized by the devices and platforms they use.[3]

And yet, the legal tools available to respond to these harms remain limited and outdated. At the federal level, the Children's Online Privacy Protection Act (COPPA), enacted in 1998, remains the central statute regulating the collection of data from children under thirteen.[4] COPPA was groundbreaking at the time of its passage, but it is now widely seen as insufficient. Legal scholars have criticized its reliance on parental consent,[5] its exclusion of certain apps which have teen users and exclusion of teens aged thirteen to seventeen altogether,[6] and its inability to adapt to mobile platforms, biometric data, and algorithmic profiling.[7] COPPA "can be better understood in light of the privacy protection climate in 1998," and may have been "enacted at a time when the major concern was protecting kids from revealing personal information rather than companies collecting kids' user data."[8] And although the Federal Trade Commission (FTC), the agency responsible for enforcing COPPA, has taken notable enforcement actions under the statute—such as two settlements totaling $520 million with Epic Games, Inc. in 2022 and a $170

---

3 JONATHAN HAIDT, THE ANXIOUS GENERATION: HOW THE GREAT REWIRING OF CHILDHOOD IS CAUSING AN EPIDEMIC OF MENTAL ILLNESS 3–7 (2024); *see also* FED. TRADE COMM'N, A LOOK BEHIND THE SCREENS: EXAMINING THE DATA PRACTICES OF SOCIAL MEDIA AND VIDEO STREAMING SERVICES, at i (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf [https://perma.cc/4AX8-7MPV] (reporting on social media companies' use of personal data that "pose unique risks to children and teens").

4 15 U.S.C. §§ 6501–6506. COPPA applies to "operators" of commercial websites, including mobile apps, that are directed at children under thirteen or have actual knowledge that they are collecting personal information from children under thirteen. *See* Abdullah Ahmed, Hashim Hayat & Daheem Hayat, *A Comprehensive Guide to COPPA*, WALTURN (May 23, 2024), https://www.walturn.com/insights/a-comprehensive-guide-to-coppa [https://perma.cc/3F8W-E7S7]. Some of the requirements include notice to parents of data collection, use, and disclosure practices (through privacy policies); obtaining verifiable parental consent before collecting, using, or disclosing children's personal data; and restrictions on behavioral advertising toward children. *Id.*

5 *E.g.*, Zahra Takhshid, *Children's Digital Privacy and the Case Against Parental Consent*, 101 TEX. L. REV. 1417, 1417–22 (2023) (arguing that reliance on parental consent to protect children's privacy is a "fundamental problem" of COPPA).

6 *Id.* at 1454 ("Nevertheless, although not required by COPPA, companies may ask for parental waivers to insulate themselves from potential liability for kids between the ages of thirteen to eighteen."); *see also* Stacey Steinberg, *The Myth of Children's Online Privacy Protection*, 77 SMU L. REV. 441, 449 (2024) (describing how TikTok and Instagram, two social media apps which are not governed by COPPA, are legally accessed by children over thirteen).

7 Steinberg, *supra* note 6, at 457–58 ("When COPPA was initially enacted in 1998, few could imagine a world connected in the ways in which we are now. . . . While policymakers seem aware that such risks exist, federal lawmakers have been unable to agree on legislation to address these growing concerns.").

8 Takhshid, *supra* note 5, at 1426.

million settlement with Google and its subsidiary, YouTube, in 2019[9]—these large settlements are relatively rare. Steinberg described the Google and YouTube settlement as "a drop in the bucket" compared to the revenue made while the companies were being accused of COPPA violations.[10]

Repeated attempts to modernize COPPA have failed. In 2023, bipartisan coalitions in Congress introduced both the Kids Online Safety Act (KOSA) and the Children and Teens' Online Privacy Protection Act (COPPA 2.0), which sought to expand the statute's reach to older minors, limit behavioral advertising, and enhance transparency requirements.[11] Despite support from children's advocacy groups and FTC commissioners, the bills failed to pass, and Senator Ed Markey (D-Mass.)—one of COPPA's original sponsors—said "House Republican leaders abandoned their responsibility and prevented this Congress from enacting life-saving measures for our families."[12]

Recently, Senator Markey and Senator Bill Cassidy (R-La.) reintroduced COPPA 2.0 and were able to obtain unanimous passage of the legislation through the U.S. Senate Commerce Committee in June 2025.[13] The FTC also finalized changes to the

---

9 Press Release, Fed. Trade Comm'n, FTC Finalizes Order Requiring Fortnite Maker Epic Games to Pay $245 Million for Tricking Users into Making Unwanted Charges (Mar. 14, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-finalizes-order-requiring-fortnite-maker-epic-games-pay-245-million-tricking-users-making [https://perma.cc/5XLD-Q3TS]; Press Release, Fed. Trade Comm'n, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law (Sep. 4, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law [https://perma.cc/CLR6-XNXW].

10 Steinberg, *supra* note 6, at 455.

11 Kids Online Safety Act, S. 1409, 118th Cong. (2023); Children and Teens' Online Privacy Protection Act, S. 1628, 117th Cong. (2021); *see* Kevin Collier, *Why a Landmark Kids Online Safety Bill That Just Passed the Senate Is Still Deeply Divisive*, NBC NEWS: TECH (July 31, 2024, at 11:03 PT), https://www.nbcnews.com/tech/tech-news/will-kosa-coppa-20-controversial-bills-explained-rcna163243 [https://perma.cc/92CR-BWS9].

12 See Press Release, Sen. Ed Markey, Sen. Markey Statement on Failure to Pass COPPA 2.0 Children and Teen Privacy Legislation by End of Congress (Dec. 18, 2024), https://www.markey.senate.gov/news/press-releases/sen-markey-statement-on-failure-to-pass-coppa-20-children-and-teen-privacy-legislation-by-end-of-congress [https://perma.cc/LD6X-WKEF].

13 Press Release, Sen. Ed Markey, Senators Markey and Cassidy Celebrate Committee Passage of Children and Teens' Online Privacy Protection Legislation (June 25, 2025), https://www.markey.senate.gov/news/press-releases/senators-markey-and-cassidy-celebrate-committee-passage-of-children-and-teens-online-privacy-protection-legislation [https://perma.cc/H5PQ-ZFS6]. COPPA 2.0 would improve upon COPPA's protections in five key areas by: (1) banning targeted advertising to children and teens, including those up to age sixteen; (2) requiring companies to permit users to delete personal information collected from a child or teen; (3) establishing data minimization rules to prohibit the excessive collection of children and teens' data; (4) revising COPPA's "actual knowledge" standard (discussed above) to close the loophole that allows platforms to ignore kids and teens on their sites; and (5) prohibiting internet companies from collecting

COPPA Final Rule,[14] requiring "parents to opt in to third-party advertising" and "address[ing] the emerging ways that consumers' data is collected and used by companies, and particularly how children's data is being shared and monetized."[15] Yet even with this recent momentum by both Congress and the FTC—and COPPA 2.0's support from groups like the Center for Digital Democracy and Google[16]—it remains to be seen if COPPA 2.0 will survive another round of bargaining in the House and ultimately be enacted as a federal law. With regard to the changes to the Final Rule, specifically, privacy experts note "the timing of the [F]inal [R]ule is uncertain following the Trump administration's stay of new regulations," and believe "the [F]inal [R]ule's future may hinge on the new administration's priorities — namely, whether [FTC] Chair [Andrew] Ferguson will revisit amendments he took issue with now that the administration paused the rule's publication."[17]

Moreover, in the absence of any legislative revisions to COPPA or a comprehensive federal privacy law[18]—or an omnibus privacy law which is industry agnostic and protects both children

---

personal information from users who are thirteen to sixteen years old without their consent. *Id.*

14 The Children's Online Privacy Protection Rule, referred to as the "COPPA Final Rule" or simply the "Rule," is the FTC's implementing regulation for enforcing COPPA, and it was last amended in January 2013. *See* 16 C.F.R. pt. 312 (2025).

15 Press Release, Fed. Trade Comm'n, FTC Finalizes Changes to Children's Privacy Rule Limiting Companies' Ability to Monetize Kids' Data (Jan. 16, 2025) [hereinafter FTC Finalizes Changes], https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data [https://perma.cc/XKE4-J7YW]. The amendments to the Final Rule would include: (1) "[r]equiring opt-in consent for targeted advertising and other disclosures to third parties"; (2) requiring "operators to only retain personal information for as long as reasonably necessary to fulfill a specific purpose for which it was collected"; and (3) improving COPPA's Safe Harbor programs (self-regulatory programs that implement protections of the Rule) transparency. *Id.*

16 Am. Acad. of Pediatrics et al., *CDD Joins Coalition of Child Advocates Urging Senate E&C Committee Members to Advance COPPA 2.0*, CTR. FOR DIGIT. DEMOCRACY: DIGIT. YOUTH (June 23, 2025), https://democraticmedia.org/publishings/letter-cdd-joins-coalition-of-child-advocates-urging-senate-e-c-committee-members-to-advance-coppa-2-0 [https://perma.cc/R8UP-UNPV]; Trinity Velazquez, *Google Supports Louisiana Senator's Bill to Strengthen Online Privacy for Children, Teens*, YAHOO NEWS (June 25, 2025, at 07:08 PT), https://www.yahoo.com/news/google-supports-louisiana-senator-bill-140852940.html [https://perma.cc/E9CV-32GX].

17 Stacy Feuer, Maria Nava & Courtney Cox, *Top 5 Impacts of the New COPPA Rule*, IAPP (Feb. 14, 2025), https://iapp.org/news/a/top-5-impacts-of-the-new-coppa-rule [https://perma.cc/GC7W-JWCG].

18 *See* Lina M. Khan, Samuel A.A. Levine & Stephanie T. Nguyen, *After Notice and Choice: Reinvigorating "Unfairness" to Rein in Data Abuses*, 77 STAN. L. REV. 1375, 1378 (2025) ("The United States is the only advanced economy in the world with no comprehensive law protecting people's online privacy.").

and adults as consumers online—several states have in recent years passed their own children's privacy and/or consumer privacy laws. California, Virginia, Colorado, and Connecticut now provide statutory privacy rights, including access, deletion, and opt-out mechanisms, to residents including teens as young as thirteen.[19] In 2022, California also passed its Age-Appropriate Design Code (AADC), which imposes additional obligations on platforms likely to be accessed by children, including data minimization, high-default privacy settings, and impact assessments for new features.[20] Other states like Arkansas, Delaware, and Utah have also passed laws that target specific purported harms to children online, such as marketing restrictions, social media use, and age verification.[21] These are promising steps, but these state law efforts are "relatively new, infrequently enforced, and challenging for many families, lawyers, and even judges to understand."[22]

More critically, these state laws still rely heavily on "notice and choice" or "notice and consent"—a legal model that has been increasingly disavowed by scholars.[23] Under this model, privacy protection is presumed to occur when a user (or parent) is presented with a disclosure and affirmatively agrees. But as Daniel Solove argues, this approach turns privacy into a procedural formality, not a substantive right.[24] Takhshid further casts doubt on the use of consent-based models for children's privacy, particularly when using services associated with educational technology

19 For a more detailed discussion on the rise of state consumer privacy laws in the absence of a federal privacy law, see Mason R. Clark, *Consumer Privacy and the* Dobbs *Disruption*, 58 U. MICH. J.L. REFORM 1, 12–16 (2024).

20 *See* CAL. CIV. CODE § 1798.99.31 (West 2023).

21 *See* Steinberg, *supra* note 6, at 458–61 (describing the state legislative efforts—some successful and some failed—at protecting children's online privacy through a variety of mechanisms).

22 *Id.* at 461.

23 Several recent publications discuss the failures of notice and choice in U.S. privacy law. *See* Khan, Levine & Nguyen, *supra* note 18, at 1375 (arguing that "for much of its history, the [FTC] relied on self-regulation through a 'notice and choice' framework that left the public vulnerable in an era of rampant data collection and digital surveillance"); *see also* Takhshid, *supra* note 5, at 1455 (suggesting that privacy law should "move away from frameworks that seek to protect children's digital privacy by relying on notice and parental consent forms and instead advocate[] for the adoption of positive law to protect children's digital privacy"); Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. 593, 593 (2024) (claiming that "[t]he evidence of actual consent is nonexistent under the notice-and-choice approach").

24 Solove, *supra* note 23, at 599–601 (describing how the "choice" in notice-and-choice is "take-it-or-leave-it—either do business . . . or do not," privacy policies are often unreadable, and plaintiffs have few remedies for breach of privacy notices without FTC intervention).

(EdTech), artificial-intelligence-enabled tools, and voice- and facial-recognition tools.[25]

Parents are cast as the primary protectors of their children's digital privacy under existing state and federal privacy laws. Parents are the ones who download the apps, configure the devices, enter the birthdates, and, at least on paper, consent to data collection. Under COPPA, they are required to provide "verifiable parental consent" before websites or online services may lawfully collect data from children under thirteen.[26] Under state laws like the California Consumer Privacy Act (CCPA) and Virginia Consumer Data Privacy Act, they can exercise data subject rights (such as the right to opt-out of sale or sharing of personal information) on their child's behalf.[27] In theory, this structure places control in the hands of families. In practice, it places the burden there instead—one that most parents are ill-equipped to shoulder.[28]

This burden creates what this Article refers to as a "parent's privacy paradox."[29] Like the broader privacy paradox that describes users who say they value privacy but do not act to protect it, parents often express deep concern about their children's digital safety but are either unprepared to take meaningful action(s) to prevent privacy harms—such as consenting even though they don't understand the technology—or willing to accept privacy harms and provide their child's personal information in spite of

---

25 Takhshid, *supra* note 5, at 1420 ("In the era of EdTech and artificial-intelligence-enabled tools such as ChatGPT, and voice-and facial-recognition tools, parental consent can no longer meaningfully serve its traditional purpose of protecting the best interests of the child, particularly given the complexity of innovation and potential for breaches of privacy . . . ." (footnote omitted)).

26 15 U.S.C. §§ 6501–6506; 16 C.F.R. § 312.5 (2025).

27 CAL. CIV. CODE § 1798.120(c) (West 2023); VA. CODE ANN. § 59.1-577(A)(5) (2023).

28 *See* Steinberg, *supra* note 6, at 464–65. Here, Steinberg critiques the notion that parents are the gatekeepers of children's privacy, highlighting the possibility of conflicting interests between parent and child:

> It is important to note that there may be times where a child's interest and a parent's interest do not align regarding children's privacy and protection. While parents may want to protect children, young people have interests in autonomy and independence. Our legal system is ill equipped to give young people a meaningful voice when their interests do not match those of their parents.

Id. (citation omitted).

29 For an introduction to "the privacy paradox," see Patricia A. Norberg, Daniel R. Horne & David A. Horne, *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*, 41 J. CONSUMER AFFS. 100, 100–01 (2007); *cf.* Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1, 1 (2021) (arguing that the privacy paradox is a "myth created by faulty logic" and is a reductive concept that does not account for the "vast, complex, and never-ending project" that is managing one's privacy).

understanding the technology.[30] A "parent's privacy paradox" is an extension of the privacy paradox which describes the disconnect between parental concern and parental capacity.

The reasons parents intentionally or unintentionally act against their children's privacy interests are manifold. Parents are busy. They are not privacy professionals. Many of them lack the time, training, or technical fluency to parse privacy policies.[31] And even if they want to opt out, they might not know how. Platforms bury privacy settings across multiple menus, use dark patterns to obscure opt-out options, and frame default tracking as necessary to the user experience.[32] Empirical studies confirm this disconnect.[33]

The discrepancy is not necessarily a reflection of parental apathy. It reflects a system that outsources legal compliance to the least empowered stakeholder in the data ecosystem. And when platforms default to parental opt-outs (rather than opt-ins), most families may end up accepting the status quo.[34] Behavioral economists have long shown that default settings carry outsized influence, particularly when users are fatigued or uncertain.[35] As children's data is silently collected through location tracking, browsing habits, and voice recordings, very little of these practices are disclosed, and almost none of them are explained to parents in plain language.[36]

---

30 *See* Takhshid, *supra* note 5, at 1421 (writing that even though parents may grant consent, they "are not sufficiently aware of the potential harms of online activities and their technological complexities to be able to meaningfully consent to them on behalf of their children"); *see also* Stacey B. Steinberg, *Sharenting: Children's Privacy in the Age of Social Media*, 66 EMORY L.J. 839, 843–44 (2017) (describing how parents may intentionally or unintentionally violate their own children's privacy by choosing to share their children's personal information online).

31 Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1436–37 (2017) (noting that in the context of COPPA notice and parental consent requirements, "[c]onsumers frequently do not read or understand privacy policies").

32 WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 23–25 (2018) (discussing how design shapes user decision-making).

33 Elvy, *supra* note 31, at 1441 (noting that "[c]onsumers may want more privacy and control over their data . . . , but they may not know how to achieve this result," and citing empirical studies conducted by the Pew Research Center and the FTC that explore how consumers understand privacy policies and how companies overpromise privacy protections).

34 *See* Solove, *supra* note 23, at 601–02 (describing how "a remarkably low percentage of people opt out," even though opt-out mechanisms remain fundamental to emerging privacy laws in the U.S.).

35 Cass R. Sunstein, *The Ethics of Nudging*, 32 YALE J. ON REG. 413, 416–17 (2015).

36 *See* FED. TRADE COMM'N, *supra* note 3, at i, 42; Michael Atleson et al., *AI and the Risk of Consumer Harm*, FED. TRADE COMM'N (Jan. 3, 2025),

Even well-meaning attempts to help parents can backfire. App store labels may disclose whether a product collects personal data, but rarely clarify what kind, how it is used, or who it is shared with. "Parental control" tools often block or restrict access without providing transparency about underlying data flows. As a result, parents conflate control with protection, assuming that if they've toggled the right content filters, then they've addressed privacy. But privacy isn't just about what children see. It's about who sees them and what can be done with the digital record of their behavior.

This is the heart of the parent's privacy paradox: The law expects parents to make meaningful, informed privacy decisions but gives them neither the visibility nor the infrastructure to do so. What looks like empowerment is often abdication disguised as agency.

This is not a call to exclude parents from the conversation. Some scholars have suggested that parents should be *less* involved in gatekeeping their children's privacy in order to give children a voice in their own decision-making.[37] But neither children nor their parents can bear the burden alone. This Article argues that a restructured pay-for-privacy (PFP) model—one that requires companies to provide parents with accessible and actionable privacy insights in the palm of their hands—could be a better solution than continued failed attempts under consent models.

This restructured model must be tailored specifically for children's digital privacy. The model is simple in concept: parents would pay a modest monthly fee—say, three to five dollars—for a regularly issued, mobile-accessible report that tells them what data has been collected from their child, by whom, and for what purposes. This report would also include interactive tools (like a toggle button) to opt out of behavioral targeting, restrict the sale of data, and delete specific categories of personal information. Think of it as a privacy control center for parents delivered on a smartphone and not buried in an app's website or privacy policy. Importantly, the PFP model does not replace legal obligations. It supplements them. Platforms would still be required to comply with COPPA, the AADC, and other applicable state consumer privacy laws like the CCPA, all of which require companies to

https://data.aclum.org/storage/2025/01/FTC_www_ftc_gov_policy_advocacy-research_tech-at-ftc_2025_01_ai-risk-consumer-harm.pdf [https://perma.cc/8KBN-TQ3J].

37 Steinberg, *supra* note 6, at 473 (writing that, among other reforms, the law should honor a child's right to privacy for various reasons, not least among them to protect children from parents' "[s]harenting," meaning the parents' posting of their child's personal information online).

have this kind of data on hand anyway.[38] The PFP layer simply packages existing compliance obligations (like data subject rights centers, opt-out toggle buttons, and transparency requirements) into a format that parents can read and use.

The PFP model draws inspiration from tools or requirements that already exist but are underutilized or inaccessible. Many companies now must respond to data subject requests under privacy laws like the European Union's General Data Protection Regulation (GDPR), the CCPA, and other emerging state privacy laws, that let their users view, correct, limit, or delete their data.[39] The PFP proposal envisions a streamlined, mobile-friendly tool that tells parents: *Here's what we've collected. Here's what we're doing with it. Here's what you can do next.*

To prevent abuse or inequity, the PFP model must be paired with regulatory guardrails. Companies would be prohibited from inflating prices, coercing families into paid plans, or punishing users who don't subscribe. Pricing caps and sliding-scale subsidies could ensure that the tool is accessible to low-income families.[40] The FTC would serve as the supervisory and enforcement agency, empowered to enforce penalties under its section 5 authority to prevent unfair or deceptive practices,[41] a power it may be more willing to wield given its recent interest in revising the COPPA Final Rule.[42]

---

38 COPPA requires operators of websites to provide, upon request by a child's parent, "a description of the specific types of personal information collected from the child by that operator" and to provide notice on the website of "what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information." 15 U.S.C. § 6502(b)(1)(A)(i), (b)(1)(B)(i). The AADC requires businesses that provide online products or services to conduct a Data Protection Impact Assessment which, among other things, includes documentation of the business's collection of children's personal information and the impacts and risks of such collection and subsequent data management practices. CAL. CIV. CODE § 1798.99.31(a)(1)(B)(i)–(viii) (West 2025). Finally, the CCPA requires businesses to provide both a right to know and a right to access the personal information being collected, used, sold, or disclosed by the business, as well as the purposes for which it is collected, sold, or shared. CAL. CIV. CODE § 1798.110.

39 Richard English, *Data Subject Access Requests (DSARs) for GDPR and CCPA Compliance*, DISCO: BLOG (Mar. 19, 2025), https://csdisco.com/blog/dsars-gdpr-ccpa-guide [https://perma.cc/BH58-67FU]; *see supra* note 19 and accompanying text.

40 *See* Elvy, *supra* note 31, at 1400. The price caps and sliding-scale subsidies could serve to prevent a PFP model that creates what Elvy describes as a "divide between those that can afford privacy and those that cannot." *Id.*

41 15 U.S.C. § 45; *see A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N (July 2025) [hereinafter *A Brief Overview*], https://www.ftc.gov/about-ftc/mission/enforcement-authority [https://perma.cc/EX2N-KPY5].

42 *See* FTC Finalizes Changes, *supra* note 15.

This is not a radical departure. Americans already pay for subscription-based digital services that offer enhanced control, fewer ads, or higher privacy, such as YouTube Premium, Apple's Private Relay, or Meta Verified.[43] The difference here is that the model would be child-centered and equity-aware. It would recognize that while the ideal solution is a substantial revision to federal privacy laws like COPPA that limits or outright bans the collection, use, and disclosure of children's data, the reality is that (1) this type of legislation is unlikely; (2) most parents are navigating a fragmented, underregulated digital landscape; and (3) companies are well-positioned—due to the data subject rights they must grant under emerging state privacy laws—to provide a report that helps parents understand their children's online activities.

Monetizing privacy raises innumerable ethical concerns, some of which this Article addresses in detail in the next section. Many scholars have warned that monetizing privacy risks creating a two-tiered system, one in which wealthier families can afford enhanced protections while low-income families cannot.[44] This concern is particularly urgent when applied to children. If privacy becomes a subscription-based service, the protections children receive will depend not on their needs or vulnerabilities, but on their parents' income and digital literacy.

This Article does not dismiss these critiques. A functional PFP model must be accompanied by strong regulatory guardrails to prevent coercion, ensure equity, and limit abuse. These guardrails include: (1) design restrictions; (2) proactive FTC enforcement; and (3) baseline protections for all. PFP services should be priced low enough (three to five dollars per month) that most families can reasonably afford them. Higher fees would disincentivize adoption and exacerbate inequality. Low-income families should receive access to PFP tools at reduced or no cost. This could be facilitated through school partnerships, Medicaid eligibility, or federal grants to nonprofit intermediaries. Companies offering PFP must be prohibited from manipulating users into

---

43 *See, e.g.*, *iCloud Private Relay & Privacy*, APPLE: LEGAL (Dec. 12, 2025), https://www.apple.com/legal/privacy/data/en/icloud-relay/ [https://perma.cc/3QQK-B7ZF]; *Stand Out with Meta Verified*, META, https://about.meta.com/technologies/meta-verified/ [https://perma.cc/W7JF-EFWH] (last visited Nov. 15, 2025).

44 Elvy, *supra* note 31, at 1402 ("Even when [low-income and minority] consumers obtain access to the Internet, they may be subjected to increased data collection and a lack of privacy and control with respect to their data unless they are able to pay for the products and services offered by PFP companies to minimize these concerns.").

upgrading via dark patterns,[45] misleading interfaces, or degraded default experiences. Companies may not withhold core privacy rights from users who decline to pay, a form of non-discrimination protection already seen in emerging state privacy laws like the CCPA.[46] PFP services must offer additive transparency and control and not just replace the rights that should be universal. By embedding these protections into the framework, the PFP model becomes a transitional tool that helps families navigate a complex digital world without waiting for additional legislation or resorting to a total privatization of data.

Moreover, the existence of a voluntary, regulated PFP system may exert pressure on companies to improve their free-tier offerings. Proactive FTC investigation and enforcement could expose disparities in treatment between paid and unpaid users, motivating platforms to converge toward higher standards of care. It can also further restrict behavioral advertising and mandate clearer data disclosures.

Under this proposal, companies offering PFP services would be required to register their tools with the FTC and submit periodic compliance reviews. These reviews would assess whether the PFP tool (1) satisfies design restrictions and requirements; (2) follows FTC guidance and enforcement; and (3) establishes baseline protections for all. The FTC would also establish complaint portals—both for parents and public-interest watchdogs—to report abuse.

This regulatory structure is not without precedent. The FTC has already demonstrated its capacity to supervise complex digital ecosystems. In 2019, the Agency imposed a $5 billion fine on Facebook (now Meta), and required detailed privacy program audits after a series of misleading practices were uncovered and a complete overhaul of Facebook's own internal privacy department structure.[47] The 2019 YouTube settlement likewise forced Google to change how it collects data from children, restrict per-

---

45 S. 1409, 118th Cong. (2023) (describing a dark pattern as a design practice that has "the purpose or substantial effect of subverting or impairing user autonomy, decision-making, or choice in order to weaken or disable safeguards or parental controls").

46 Alysa Z. Hutnik, Aaron J. Burstein & Alexander I. Schneider, *The CCPA Non-Discrimination Right, Explained*, KELLEY DRYE (Apr. 29, 2020), https://www.kelleydrye.com/viewpoints/blogs/ad-law-access/the-ccpa-non-discrimination-right-explained [https://perma.cc/P5ZQ-29Q9].

47 Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook [https://perma.cc/JZQ3-6ES9].

sonalized ads on kids' content, and create a pathway for channel-level COPPA compliance.[48]

More importantly, the FTC has shown its willingness to evolve as the technology children use (and the privacy threats it creates) changes. In 2024, the FTC released a 6(b)[49] study of social media platforms, highlighting aggressive data harvesting from youth.[50] That same year, it updated the COPPA Rule to clarify that companies may not use age-gating to avoid liability and must provide clearer data disclosures and default settings for child-directed services.[51] The goal is not to offload privacy responsibilities onto the market, but to create infrastructure that works now while larger reforms remain politically stalled.

This vision of enforcement does not rely solely on federal intervention. State Attorneys General would retain their powers under state consumer protection laws and consumer privacy laws, and they could bring actions for deceptive or discriminatory PFP offerings. Nonprofit watchdogs, legal clinics, and privacy researchers would be encouraged to test and challenge offerings. Together, this would allow PFP to function not as a Band-Aid, but as a bridge with a regulated, transparent tool for families that connects a broken present to a more secure future.

The stakes could not be higher. The digital economy is not waiting for Congress to act. While lawmakers debate, companies are refining machine-learning models on behavioral data collected from children.[52] They are building advertising profiles, mapping social graphs, and recording location histories, all before a child has learned how to write in cursive (if that is even still required!).[53] Privacy harms are live and ongoing erosions of children's autonomy and psychological safety. Parents know this, but knowing is not the same as acting, especially in an ecosystem designed to resist action.

---

48 Press Release, Fed. Trade Comm'n, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law (Sep. 4, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law [https://perma.cc/TGB5-FEGD].

49 *A Brief Overview*, *supra* note 41 ("Section 6 of the FTC Act provides another investigative tool. Section 6(b) empowers the Commission to require an entity to file 'annual or special . . . reports or answers in writing to specific questions' to provide information about the entity's 'organization, business, conduct, practices, management, and relation to other corporations, partnerships, and individuals.'" (citing 15 U.S.C. § 46(b))).

50 FED. TRADE COMM'N, *supra* note 3, at i.

51 FTC Finalizes Changes, *supra* note 15.

52 *See* FED. TRADE COMM'N, *supra* note 3, at 72–73.

53 *Id.*

The PFP model proposed in this Article is, at best, a pragmatic solution in a broken system. It offers parents a chance to reclaim some control, not by decoding terms of service or clicking through endless menus, but by receiving a regular, visual report that tells them: *This is what we collected, this is how it was used, and this is what you can do about it.* Crucially, PFP only works if it is regulated and equitable. It must include a firm legal floor (no one should be penalized for not paying); sliding-scale subsidies for low-income families; a mobile-friendly design to meet users where they are; and active FTC and state-level enforcement to deter deception and abuse. If designed this way, PFP can function as a tool of empowerment. It can pressure companies to compete on transparency and usability. It can nudge families toward more active engagement. And it can fill the gap between what the law should require and what it currently allows.

This Article proceeds in three Parts. Part II explores the "parent's privacy paradox" and, while it critiques the failure of consent-based regimes in children's privacy law, it suggests that parents can still make choices about their children's digital privacy if they are better informed with easily accessible information. Part III analyzes how some companies, particularly those which exist outside of COPPA's purview, are technically and financially well-positioned to implement a regulated PFP model and how the model aligns with existing legal obligations and emerging consumer trends. And Part IV proposes a regulatory framework for PFP, focusing on equity, usability, and enforceability under FTC supervision and existing state privacy law. Together, these sections advance a single proposition: Children's privacy is a collective responsibility.

II. CAN (OR SHOULD) PARENTS MAKE PRIVACY CHOICES?

Parents are often the gatekeepers and the first line of defense for their children's digital privacy. They buy the devices, download the apps, set the passwords, and, under laws like COPPA, are expected to give "verifiable parental consent" before personal data is collected.[54] In theory, parents decide what data is collected, when, and by whom. In practice, however, parents only have the illusion of control. Parents are routinely overburdened (or intentionally misled) by consent forms and privacy policies. They are told they are in control, but the control is often

[54] 16 C.F.R. § 312.5(a)(1) (2025) ("An operator is required to obtain verifiable parental consent before any collection, use, or disclosure of personal information from children . . . .").

symbolic. As such, scholars have critiqued parental consent as the basis for protecting children's privacy.[55] This section agrees that parental consent cannot be the bedrock of children's privacy online for the very same reasons articulated by Takhshid, Steinberg, Solove, and many others. However, even if parental consent no longer serves as the foundation of children's privacy, it does not mean that parents cannot—or should not—still retain some decision-making authority. If parents are given frequent, easily accessible information about their children's online activity in the palm of their hands, and they can make decisions about that activity (such as by requesting the collector to delete the data) with one click on their mobile device, they can help mitigate against downstream privacy harms.

A. The Illusion of Consent

Most privacy interfaces are not designed for usability. They are designed for legal compliance and user attrition.[56] Platform interfaces routinely hide key privacy settings across multiple menus and use algorithms, data analytics, and/or artificial intelligence in their data processing to further obfuscate data collection practices.[57] Even though many platforms and devices offer parental controls, these tools often overwhelm parents and present a host of other problems for both parent and child.[58]

Scholars have recognized this problem for years. Hartzog and Solove have each critiqued the legal system's reliance on consent mechanisms and "notice-and-choice" regimes that are structurally designed to fail.[59] Not to mention, most companies are strongly incentivized to obtain consent, so they may make

---

55 *See* Takhshid, *supra* note 5, at 1417 (arguing that "under the common law tradition of protecting the best interests of the child, when it comes to protecting children's digital privacy, relying solely on parental consent is insufficient and ill-suited" and suggesting that common law privacy torts may "motivate companies to be more vigilant towards handling minors' data to avoid potential lawsuits"); *see also* Steinberg, *supra* note 6, at 464–65 (writing that parental consent sometimes intentionally or unintentionally harms children and robs them of their autonomy and independence).

56 HARTZOG, *supra* note 32, at 27–32.

57 FED. TRADE COMM'N, *supra* note 3, at 61–62.

58 Sara M. Grimes & Riley McNair, *Parental Controls on Children's Tech Devices Are Out of Touch with Child's Play*, THE CONVERSATION (July 6, 2025, at 08:51 ET), https://theconversation.com/parental-controls-on-childrens-tech-devices-are-out-of-touch-with-childs-play-257874 [https://perma.cc/LLF6-MKTF] (explaining that a study by the Family Online Safety Institute revealed parents don't use parental controls because they feel overwhelmed, and suggesting that parental controls present other problems such as a lack of risk awareness by children and poor communication between parent and child).

59 HARTZOG, *supra* note 32, at 60–61; Solove, *supra* note 23, at 601 (stating that "[t]he notice-and-choice approach has been savaged in academic literature").

special effort to manipulate or coerce their customers—children and adults—into providing it.[60]

Parental consent in the modern privacy landscape operates more like a waiver than an informed choice. And because many privacy policies are vague or incomplete, parents are often only minimally aware that data is even being collected, sold to brokers, or shared with unknown third parties.[61] The parent's privacy paradox, then, becomes more profound when one considers the scope and opacity of modern data collection. Children's devices track browsing history, app usage, geolocation, search queries, biometric signals, and even facial expressions—often without any ongoing disclosure and with the assistance of emerging artificial intelligence capabilities.[62] Many of these activities are justified by platforms under broad headings like "functional data" or "performance analytics," which are rarely explained in concrete terms.[63] This makes meaningful oversight nearly impossible. The average parent, even one with a college education, cannot reasonably be expected to navigate a privacy regime that assumes such a high level of privacy literacy. Yet that is exactly what the current system demands.

But altering the parental consent model is no small task. The concept of consent has long served as the backbone of American privacy law.[64] If a company tells you what it is doing with your data and you agree, that agreement legitimizes the practice. This logic extends to COPPA, which prohibits the collection of personal data from children under thirteen without "verifiable parental consent."[65] It also underlies the broader consumer privacy laws passed in California, Virginia, and other states, which permit data collection and sharing so long as users are given notice and an opportunity to opt out.[66]

But as countless privacy scholars have shown, consent in this context is largely legal fiction.[67] In the children's privacy

60 Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1489 (2019).

61 Solove, *supra* note 23, at 622 (asserting that "[w]hat people are told in privacy notices are vague meaningless statements" which do not describe internal governance programs or "how well privacy is integrated into the design of products and services, among many other things").

62 FED. TRADE COMM'N, *supra* note 3, at v–vi.

63 *Id.* at 27.

64 Solove, *supra* note 23, at 596.

65 16 C.F.R. § 312.5 (2025).

66 *See* CAL. CIV. CODE § 1798.120 (West 2023); VA. CODE ANN. § 59.1-577(A) (2023).

67 Solove, *supra* note 23, at 598–600.

context, this fiction becomes even more absurd. Children cannot consent, and parents are asked to consent on their behalf, often without understanding the full scope of what they are authorizing.[68] Although there have been recently enacted state consumer privacy laws and changes to the COPPA Final Rule, as discussed above, these laws have so far failed to require companies to provide intelligible summaries of exactly what a parent is consenting to on behalf of their child. And once consent is given, it is rarely revisited. Unlike data processing under the GDPR, which often requires renewed or contextual consent,[69] COPPA consent is typically a one-time event. Data collection continues indefinitely unless the parent actively intervenes, which, as noted earlier, most do not. This creates a regulatory sleight of hand in which companies claim legal compliance by offering notice and obtaining consent, but in practice, the parent neither notices nor consents in any meaningful way. Daniel Solove refers to this as "murky consent"—a model in which the existence of a checkbox or policy is treated as proof of agreement, regardless of actual comprehension or voluntariness.[70] He argues that the law must shift away from consent as a universal solution and toward substantive privacy protections that apply regardless of whether a user clicks "I agree."[71]

Children's data deserves nothing less. If it is acknowledged that parents are overwhelmed, interfaces are deceptive, and privacy policies are unreadable, then it must also be acknowledged that consent alone cannot carry the regulatory burden. Any privacy regime that depends on informed parental decision-making must first give parents the tools, time, and support to make decisions that matter. Because even some who criticize consent-based regimes acknowledge that individual choices will (and should) nevertheless be made:

> Respect for people's autonomy gives them space to make informed choices based on their determination of what is in their own self-interest. The problem is that for privacy, people's decisions are often highly manipulated and ill-informed. . . . Even accepting that these problems can never be surmounted, respect for autonomy involves

---

68 Takhshid, *supra* note 5, at 1421 ("Today, across the internet from online gaming to other entertainment apps, companies rely on parental consent . . . . [P]arents themselves are not sufficiently aware of the potential harms of online activities and their technological complexities to be able to meaningfully consent to them on behalf of their children.").

69 Commission Regulation 2016/679, art. 7, 2016 O.J. (L 119) 37 (EU). Under article 7 of the GDPR, consent must be freely given, specific, informed, and unambiguous. *Id.* It also must be given each time a company creates a new use or purpose for the data. *Id.*

70 *See* Solove, *supra* note 23, at 593–94.

71 *See id.* at 632–33.

> preserving space for individual choice, as unsound and compromised as it often is.[72]

B. Solutions Without Consent

What are scholars, lawmakers, and regulators proposing now to address the insufficiency of consent-based privacy? There is a plethora of proposals, some of which are industry specific (e.g., EdTech v. social media) but almost all of which are in favor of abandoning parental consent as the bedrock for children's privacy. For example, Takhshid argues that, in the EdTech sphere, COPPA's "verifiable parental consent" mechanism invites oversimplified (and overabused) parental consent forms that do not address other uses of children's data; creates a heavy burden for parents to access and understand school records; and violates public policy by allowing companies to use the "parental-consent apparatus" to put the "child's privacy rights at the mercy of a tech company."[73] Takhshid expressly rejects the argument that parental consent for EdTech data collection is equivalent to their right to make decisions concerning the care and control of children under the Fourteenth Amendments' Due Process Clause, instead claiming that parents are not exercising their right to shape their child's education when they make uninformed choices about such data collection.[74] Her solutions included both "tough regulation," which could have companies "competing . . . by promoting . . . top-notch privacy-protection tools rather distracting apps and colorful games,"[75] and exploration of common law privacy tort lawsuits.[76]

Steinberg, on the other hand, supports comprehensive federal legislation,[77] arguing that "[c]hildren's online privacy law is in disarray."[78] She suggests that lawmakers should use the California AADC[79] as a model for children's privacy legislation in the U. S. for a variety of reasons, noting that it incorporates many in-

---

72 *Id.* at 628.

73 Takhshid, *supra* note 5, at 1442–46.

74 *See id.* at 1446–47.

75 *Id.* at 1448–49.

76 *See id.* at 1449.

77 *See* Steinberg, *supra* note 6, at 467.

78 *Id.* at 443.

79 CAL. CIV. CODE § 1798.99.31 (West 2025); *see also* Rory Sweeney, *The California Age-Appropriate Design Code Act*, CAL. LAWS. ASS'N (Oct. 16, 2023), https://calawyers.org/privacy-law/the-california-age-appropriate-design-code-act/ [https://perma.cc/RJ72-AWMC] (detailing that this law is designed to "promote a 'high-level' of privacy by default," prohibit profiling, precise geolocation collection, and harmful design tricks like dark patterns, and "reinforc[e] data minimization and purpose limitation principles").

ternational principles[80] and sufficiently narrows the scope to larger corporations to preempt corporate interest pushback.[81] Perhaps more novel, however, is Steinberg's argument against recent state children's privacy laws in Arkansas, California, Delaware, Texas, and Utah[82] that rely on the parental consent mechanism, citing concerns about children's autonomy and their civil rights.[83]

Legal scholars and commentators have long observed that privacy harms are disproportionately concentrated among low-income and marginalized communities.[84] The consent-based privacy regimes (particularly consent mechanisms present in old models of PFP, such as the privacy-discount plans)[85] fall hardest on families with the fewest resources because privacy-discount plans "may force consumers to make difficult choices between privacy and other necessities."[86] Even if we assume that all parents want to protect their children's digital privacy—and the data suggests they do—the ability to do so varies dramatically. Not all families have equal access to information, time, tools, or financial flexibility. As a result, a parent may intentionally or unintentionally sacrifice their children's data privacy in ways that could prove harmful down the road. Elvy writes,

---

80 *See* Comm. on the Rights of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, at 3–6, 8–11, 14–16, 19, U.N. Doc. CRC/C/G/25 (Mar. 2, 2021); *see also* Steinberg, *supra* note 6, at 469–74 (highlighting key provisions of this convention).

81 Steinberg, *supra* note 6, at 468–69.

82 *See id.* at 443, 458–61.

83 *See id.* at 464–65 ("While parents may want to protect children, young people have interests in autonomy and independence."); *see also* Natasha Singer, *Silicon Valley Battles States over New Online Safety Laws for Children*, N.Y. TIMES (Feb. 1, 2024), https://www.nytimes.com/2024/01/31/technology/social-media-free-speech-netchoice.html [https://perma.cc/64AU-5LVW] (suggesting parental consent could keep young people from reproductive health and/or gender identity resources).

84 *See* Danielle Keats Citron, *A Poor Mother's Right to Privacy: A Review*, 98 B.U. L. REV. 1139, 1142 (2018) ("Nowhere is that power disparity [between government and corporate power over those they surveil] more evident than the State's surveillance of society's most vulnerable members."); *see also* Michele Estrin Gilman, *The Class Differential in Privacy Law*, 77 BROOK. L. REV. 1389, 1393–94 (2012) (describing how low-income Americans experience privacy differently than middle- and upper- class Americans); Nathan Newman, *How Big Data Enables Economic Harm to Low-Income Consumers*, HUFFPOST (Nov. 15, 2014), https://www.huffpost.com/entry/how-big-data-enables-econ_b_5820202 [https://perma.cc/9QL2-YSCB] (explaining how big data platforms use low-income consumer data to target vulnerable consumers with "economically exploitative services").

85 Elvy, *supra* note 31, at 1391–92 (describing privacy-discount programs as those in which "consumers also pay for privacy controls by incurring higher fees. However, unlike in the privacy-as-a-luxury model, consumers are encouraged to relinquish their privacy and data through the use of discounts.").

86 *See id.* at 1405.

> Eventually information about a child's behavioral status, preferences, experiences and other sorts of child-related data could be used to determine the types of opportunities that children receive during childhood as well as negatively impact their adulthood lives and prospects. Thus, rising data quality and quantity and increases in the digital footprints of children combined with new platforms for collecting and sharing household (and child) data may exacerbate privacy concerns for children.[87]

These disparities may be replicated when children's data is at stake. Families with fewer resources may be more likely to allow companies to monetize children's data so the families can afford necessities.[88] By contrast, wealthier families are more likely to pay for subscriptions that promise privacy, offer enhanced settings, or restrict third-party tracking.[89] This creates a stratified digital environment where privacy is a premium feature and surveillance is the default for everyone else.

It is clear from scholarship and recent legislative and regulatory activity that consent and/or notice-and-choice regimes are falling out of favor among privacy advocates because user consent is rarely well-informed and is often manipulative (at best) or coercive (at worst), particularly for those in underrepresented communities. The risk, of course, is that any privacy model—especially a PFP model, as this Article considers—could also entrench inequities. If enhanced transparency and data control are only available to those who can afford them, the children most vulnerable to exploitation will be the least protected. The PFP market "not only confirms privacy's value to users of a company's products and services but also implies the existence of lower-tier options for those unable to afford these premium privacy protections."[90]

Any serious effort to address children's privacy must confront these structural inequities. And even under the PFP model this Article proposes, parents—even parents who are able and willing to pay for privacy reports on their children's data—cannot be solely responsible for protecting children's privacy. A reimagined PFP model must be paired with a regulatory regime specifically designed for the realities of all families, not just those who can afford privacy. For this reason, any PFP model must be paired with the following regulatory guardrails: (1) design restrictions; (2) proactive FTC enforcement; and (3) baseline protections for all,

---

87 *Id.* at 1408.

88 *See id.* at 1407.

89 *See id.* at 1402.

90 Jeffrey L. Vagle, *Privacy's Commodification and the Limits of Antitrust*, 77 ARK. L. REV. 51, 72 (2024).

regardless of payment. Without these safeguards, PFP becomes a vehicle for exclusion instead of a tool for empowerment.

C. PFP as a Practical Solution

The PFP model proposed in this Article is not a cure-all. It is not a substitute for comprehensive federal privacy legislation, any sort of structural reform of coercive data collection practices, or the total abandonment of consent or notice-and-choice privacy frameworks. This Article agrees with scholars who see "privacy self-management" and rights to notice, access, and consent as "laudable goals" that nonetheless "hid[e] bad practices behind a veil of user consent based on little or no understanding of what is being consented to."[91] However, given that federal legislation seems unlikely, structural reform is, by its nature, a long process, and the most recent privacy laws at the state and federal level continue to uphold consent-based regimes, a *reimagined* PFP model—one in which (1) consent is irrelevant, and (2) parents are paying for one-click accessibility and control made possible by their contributions—could ignite a market-based solution.

In the best-case scenario, the PFP model this Article proposes would serve as a bridge away from the ruins of consent-based regimes and toward the control over information envisioned by privacy advocates. It could address two scoping problems with COPPA—that it only applies to children under thirteen and to online apps and services "directed to children"—by encouraging companies who have both under- and over-thirteen users to generate revenue from parents of both demographics.[92] The PFP model would also build on some of the more recent rights afforded to consumers, generally, under state privacy laws—such as the right to access and delete data and the right to opt-out of data sharing—and present meaningful options to parents in the palm of their hands.

Under the proposed PFP framework, parents would pay a fee to receive a monthly privacy report delivered via mobile app or email that outlines: what data was collected from their child;

---

91 *Id*. at 78.

92 15 U.S.C. §§ 6501–6502; *see* Zoë MacDonald, Note, *Defending Children's Data Privacy: Strategies for the 21st Century*, 76 U.C. L.J. 589, 594 n.22 (2025) (citing Eva Rothenberg, *Meta Collected Children's Data from Instagram Accounts, Unsealed Court Document Alleges*, CNN (Nov. 26, 2023, at 15:12 ET), https://edition.cnn.com/2023/11/26/business/meta-collecting-data-children-facebook/index.html [https://perma.cc/WGZ8-YKGD]) ("Instagram explicitly prohibits children under thirteen from creating accounts, meaning COPPA would not apply; but in reality, there are many users under age thirteen on the social media app and one lawsuit alleges that Instagram is aware of that fact and still collects user data without complying with COPPA.").

which companies collected it; whether it was shared or sold; what privacy choices are available (e.g., deletion, opt-out, restriction); and a one-click option to exercise those controls. All of this would be regulated by the FTC, which would establish minimum usability standards, audit compliance, and enforce penalties under its section 5 unfairness and deception authority.[93] Companies would be required to offer a no-cost baseline tier of privacy protection, and pricing for enhanced PFP services would be capped at a low, family-friendly level (e.g., three to five dollars per month), with subsidies for low-income households.

The goal of the PFP model and the monthly privacy report is not to turn privacy into a product. The goal is to make some of the rights mentioned above and afforded to consumers in various states[94] clearly presented to and easily exercised by any parent who pays for it. This begs the question: If those rights already exist in some states, why should parents have to pay for it? There are several reasons.

First, even though all the state privacy laws have opt-in consent requirements for collecting personal information from minors, the majority of them only require this consent for "sensitive data" collected from users thirteen or younger.[95] Second, none of those state privacy laws provide a private right of action for violating these rights—parent, child, or otherwise.[96] And third, recent enforcement reports across the states show that many states have not filed any complaints enforcing their laws, and "many consumers don't yet understand the finer points of submitting a violation complaint."[97]

The state consumer privacy laws thus create similar scoping problems and have yet to have any meaningful enforcement. Regarding the consumers' ability to understand how to submit a rights request, this problem echoes the problem with notice-and-

---

93 *See* 15 U.S.C. § 45(a)(1).

94 *See* INT'L ASS'N OF PRIV. PRO., US STATE PRIVACY LEGISLATION TRACKER 2025: COMPREHENSIVE CONSUMER PRIVACY BILLS (2025), https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf [https://perma.cc/3CXY-PBD9]. There are currently nineteen state consumer privacy laws in the U.S. *Id.* All nineteen states provide their residents the right to access what information has been collected about them and delete that information. *Id.* All but two states also provide the right to correct the information collected and opt out of the processing of personal data for profiling and/or targeted advertising purposes. *Id.*

95 *Id.*

96 *See id.*

97 Caroline Kibby, *Emerging Trends, Insights from Public Enforcement of US State Privacy Laws*, IAPP (June 30, 2025), https://iapp.org/news/a/emerging-trends-insights-from-public-enforcement-of-us-state-privacy-laws [https://perma.cc/3QTL-D2DJ].

choice as articulated above. Most parents interact with digital services through their smartphones while managing competing obligations. They need privacy tools that are designed for real-world parenting rather than web-based dashboards that assume hours of free time and technical fluency.[98]

By offering a recurring, digestible report and a centralized control interface, PFP can reduce the friction that discourages privacy-protective behavior. This matters in a parental context because rather than expecting a parent to scour each app's privacy policy or locate obscure settings, the PFP tool can surface key risks and offer one-click solutions regardless of any (uninformed) consent granted. The PFP model also introduces competitive pressure. If companies are required to disclose their data collection practices in plain terms each month, and parents begin comparing reports across platforms, the most privacy-invasive services may face market pushback. Parents may choose apps or devices with stronger protections, incentivizing companies to improve their default designs. In this way, PFP could promote privacy as a product differentiator. Of course, the PFP model will require buy-in from large tech companies, something that has proven to be difficult to obtain in many other attempts to regulate children's privacy.[99]

Still, no one should confuse a market tool with a rights-based framework. PFP is valuable precisely because the rights-based framework is currently weak. Until Congress enacts a federal children's privacy law with substantial improvements to COPPA or regulators clamp down hard on Big Tech and social media companies (or both), parents will remain the gatekeepers of their children's privacy. And as this Part has shown, they are currently defending the gates without much armor.

The failure of current privacy law is as much conceptual as it is technical or procedural. By currently placing the burden of privacy protection on parental consent mechanisms, parents are expected to serve as digital gatekeepers in an environment designed to overwhelm them, while companies and lawmakers escape accountability by insisting that the tools to exercise any

---

98 *See id.* In the article, Kibby describes how Texas consumers were confused about how to exercise their rights because "the method varies from [company to company]." *Id.* Kibby further notes that "consumers and businesses alike aren't quite sure yet how to adapt to the rights and responsibilities created by privacy laws." *Id.*

99 *See Big Tech's Scramble to Stop Child Safety Laws*, TECH TRANSPARENCY PROJECT (May 3, 2023), https://www.techtransparencyproject.org/articles/big-techs-scramble-to-stop-child-safety-laws [https://perma.cc/KC82-Y49K].

sort of control or choice exist, even if they are impossible to use. A better approach begins by recognizing that children's privacy is a collective public interest, not a private task.[100] Just as society regulates toy safety, food labeling, and school curricula to protect child development, it must also regulate data collection practices that shape how children are profiled and marketed to. A child's digital life should not be determined by their parents' tech savvy or disposable income. It should be supported by infrastructure that makes active participation possible.

The broader ambition of the PFP model is not just to give parents rights they should (or do) already have, but to redesign the structure of responsibility. It suggests that children's privacy should be shared between parents, companies, and regulators and sustained by systems that are accessible and responsive. By reframing privacy as a collective responsibility, PFP challenges the notion that protecting children's privacy is dualistic, where you can either strip parents and children of autonomy and place all responsibility on the companies to engage in ethical data collection practices, or you can place the burden solely on parents to exercise what little rights they do have based on information that is inaccessible and through mechanisms they do not have time or understanding to navigate. It acknowledges that structural problems require structural solutions, and that meaningful child privacy requires participation from all stakeholders. The next Part of this Article turns to the other stakeholders—the companies and the FTC—and outlines how to implement PFP with fairness, transparency, and enforceability.

III. A PFP MAKEOVER: CORPORATE ACCOUNTABILITY

A. Platforms are Positioned to Act

If parental consent is no longer a reliable foundation for children's data protection—and Part II argued it is not—then responsibility must shift upstream. The natural candidates are the platforms and service providers that design, deploy, and profit from the data collection infrastructure. These companies are best positioned to implement real-time privacy protections because they control the data pipelines, the user interfaces, and the economic incentives that shape behavior.

---

100 *See* Takhshid, *supra* note 5, at 1445 (proposing reforms to parental consent in the EdTech space by arguing that children's privacy is a collective public interest, not a private task).

Platforms already collect and process vast volumes of data on children, often with remarkable precision. In the average household, a single tablet or smartphone app may track usage metrics, device identifiers, browsing history, purchase patterns, location data, behavioral engagement, and biometric inputs like voice or facial recognition.[101] These data flows are rarely disclosed in meaningful detail to parents, yet platforms manage them in real time for internal purposes, and they even use certain data to produce targeted advertising and algorithmic optimization designed to keep them engaged.[102] If they can deploy infrastructure to monetize children's attention, they can certainly deploy infrastructure to help parents monitor it.

From a technical standpoint, most large platforms already possess the architecture needed to implement a PFP system where revenue from parents helps fund the generation of a monthly privacy report. They have user authentication systems, mobile push notifications, granular tracking dashboards, customer segmentation tools, and API endpoints that allow for data reporting and user-specific customizations. Companies like Google and Apple already offer parents partial visibility through tools such as Google Family Link and Apple Screen Time, which include device-level summaries of usage and controls over app permissions.[103] These tools, however, are siloed, underadvertised, and focused more on screen time than data collection. A PFP tool could draw on these existing capabilities but shift the emphasis toward ongoing data transparency and control.

Financially, platforms are also incentivized to offer differentiated privacy services. Scholars have shown that privacy has already become a product differentiator in some consumer products, such as the difference in pricing for an Apple iPhone versus an Android smartphone.[104] Apple promotes its devices as privacy-forward by default and has adopted App Tracking Transparency (ATT) policies that signal a growing market awareness of privacy

---

101 *See* FED. TRADE COMM'N, *supra* note 3, at 25–26.

102 *See* Michal Lavi, *Targeting Children: Liability for Algorithmic Recommendations*, 73 AM. U. L. REV. 1367, 1376–77 (2024) (describing how Facebook used inferences about minors' moods and insecurities to target advertisements to them "when [Facebook's] algorithm believed they were most vulnerable").

103 *See Use Screen Time on Your iPhone and iPad*, APPLE (Sep. 15, 2025), https://support.apple.com/en-us/HT208982 [https://perma.cc/NEA4-CTZG]; *Help Keep Your Family Safer Online*, GOOGLE: FAMILY LINK, https://families.google.com/familylink/ [https://perma.cc/Q7FS-CE8F] (last visited Dec. 23, 2025).

104 *See* Elvy, *supra* note 31, at 1400–01.

preferences.[105] This commercial reality suggests that platforms are not only capable of monetizing privacy, but that they are already doing so.

Many platforms are also well-positioned to provide monthly privacy reports because they must have the necessary data anyway under the emerging state privacy laws mentioned above. While these laws currently require these disclosures only upon request and not on a regular schedule (again, as a reflection of notice-and-choice), they nonetheless require companies to maintain detailed logs of how user data, including children's data, is processed. These laws could form the basis for a reporting infrastructure that could be repurposed or extended automatically to parents of children who choose to pay for the report in any jurisdiction, not just one in which the state legislature has passed a privacy law. Put simply, many companies—or perhaps, the most problematic companies, like social media conglomerates and streaming service providers—have the infrastructure to generate the monthly privacy report quickly and accurately, and they will have additional revenue to provide it automatically to any parent who pays for the report.

But just because these companies are well-positioned to provide these monthly privacy reports through the PFP model, the model cannot be left to self-regulation without effective regulatory oversight. In fact, privacy "self-regulation," generally, has been noted by the FTC to be a failure.[106] The PFP model would still require a regulatory framework that ensures these services are oriented toward children's privacy and equitable for all parents and children. The FTC's role in regulating the PFP model is discussed more in Part IV.

Critics may argue that giving companies more control over privacy delivery will only exacerbate the power discrepancy between consumer and company and entrench what Vagle and others have described as "information asymmetries."[107] Vagle suggests:

---

105 *See Privacy. That's Apple.*, APPLE: PRIVACY, https://www.apple.com/privacy/ [https://perma.cc/96PF-Q2D8] (last visited Dec. 23, 2025).

106 *See* Khan, Levine & Nguyen, *supra* note 18, at 1406.

107 Vagle, *supra* note 90, at 78 (describing the "click to agree" on terms of service as an example of "[p]rivacy-related information asymmetr[y]," wherein the user has little to no understanding of what they just consented to while the company ostensibly knows exactly what it allows them to do with the data collected); *see also* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1683 (1999) (describing an early iteration of information asymmetry as the "knowledge gap" between data processors and individuals trying to exercise a privacy choice, and how "[t]he result of this asymmetrical knowledge will be one-sided bargains that benefit data processors").

> The growing spectrum of individual privacy harms continues to be documented as new circumstances arise, new technologies are developed and deployed, and as our understanding of all of the above evolves, a thread that runs throughout the sources of these injuries is the relationship between privacy and power. The power dynamic between the collectors of information and those from which it is collected is quite one-sided, where individuals are disempowered by information asymmetries, technology black boxes, and the lack of any real choices when it comes to privacy protections.[108]

But PFP does not necessarily grant platforms more control. This Article's model demands more accountability: The platforms must provide accessible data automatically, and they can't evade that obligation like they often do under state consumer privacy laws. It asks them to use their existing infrastructure to serve a public goal and help protect children from downstream privacy harms. If companies can use engagement dashboards to optimize ad revenue, they can also use them to generate monthly privacy reports for parents. The platforms are already collecting the data. They already have the infrastructure. They already differentiate based on privacy. What they lack is a legal, ethical, and enforceable obligation to put these tools to work for families. The PFP model—designed with the parent in mind but implemented by the platforms—offers a viable path forward.

The monthly privacy report would have to be accessible. In privacy terms, accessibility may translate to "transparency." But transparency in privacy law is tricky. Too much information (like a long privacy policy or the terms of use as described by Vagle above) can overwhelm a user, but a "very simple notice can't accurately describe many of the intricate ways that personal data is processed."[109] Various privacy laws in the U.S. and abroad typically require privacy policies or other notices be written in "clear and plain language" or be "reasonably accessible."[110]

Unlike privacy policies, terms of use, or even concisely written consents, the monthly privacy report would deliver a recurring snapshot of how a child's data was processed over the past month. It would summarize, in natural language and visual form, what types of data were collected (such as location, biometric, browsing history, or interactions), which entities collected it (specific app names or third-party services), and for what purposes (like advertising, analytics, content recommendation, or

108 *Id.* at 85.
109 Solove, *supra* note 23, at 617.
110 *Id.* at 616.

feature customization). It would also flag any high-risk behaviors—such as passive listening, behavioral profiling, or sale of data to brokers—and provide the parent with one-click options to delete, restrict, or opt out.

Crucially, this report must be delivered through channels parents already use, such as push notifications on mobile apps, monthly text or email alerts, or integration with other platforms like Google Family Link or Apple Screen Time. Expecting parents to log into a web portal and navigate nested menus is a recipe for disengagement. Design must meet the parent where they are (and, in my experience, parents are usually tired, busy, and multitasking until they have hit peak sensory overload).

In privacy terms, the monthly privacy report should not be "frictionless"[111] but rather should be a recurring report that says: *This is what we have done with your child's data. Click here to change that.* The monthly privacy report adapts to a child's evolving digital life. It captures new app installations, changes in data-sharing practices or data sharing partners, and/or shifts in behavioral patterns over time. For example, if a child begins spending more time on a platform that intensifies ad targeting, the report can flag that change and alert the parent. This proactive alerting creates a feedback loop that enhances both awareness and control, something virtually absent from the current consent-based regime, particularly on social media platforms and streaming services, which rely on frictionless consent to continuously collect and share a child's data.

Technically, such reports are not hard to generate. Platforms already track every relevant metric for internal use.[112] They know which apps are opened, how long they're used, what information is shared, and which third parties are involved.[113] These data pipelines already feed advertising analytics, product development, and machine learning models.[114] A report tool would

---

111 William McGeveran, *The Law of Friction*, 2013 U. CHI. LEGAL F. 15, 15 (2013). William McGeveran defined "friction" as "the forces that impede individuals from disclosing personal information when they use online services." *Id.* For example, friction could be the number of boxes one must check or webpages one must navigate through before providing consent to share certain information. *Id.* at 15–17. Frictionless sharing, on the other hand, could be Netflix sharing all videos someone has watched with third parties after they consented just one time for one particular video. *See id.*

112 *See* BUREAU OF CONSUMER PROT., FED. TRADE COMM'N, BRINGING DARK PATTERNS TO LIGHT 12–14 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800+Dark+Patterns+Report+9.14.2022+-+FINAL.pdf [https://perma.cc/M35A-KCCX].

113 *See id.* at 16–17.

114 *See id.* at 35.

simply repurpose that infrastructure to surface those insights for parents, not just advertisers.

A key challenge is standardization. As discussed above, the current state consumer privacy laws are struggling with standards for identity verification, processes for submitting rights requests, and other requirements under those laws.[115] If each platform creates its own version of the monthly privacy report, inconsistency will undermine usability. Policymakers or regulators like the FTC could develop reporting standards akin to the FDA's Nutrition Facts label or financial credit disclosures so that data categories and rights icons or toggle buttons are uniform across platforms and avoid the historical problems with various consent requirements and language.[116] For example, a red-yellow-green visual scale might signal privacy risk levels, while boldface toggle buttons[117] could highlight the rights associated with that data. Standardization would ensure comparability and reduce cognitive load.

Parents should be able to contextualize what matters in the monthly report, even if they don't fully grasp what exact data was collected or how that may impact their child. For instance, instead of reporting that "third parties may receive anonymous identifiers," the report might state: *Your child's location data was shared with four companies for advertising purposes. You can restrict this here*. Or: *This app collected facial recognition data to personalize filters. This is uncommon and may carry additional privacy risks*. Parents should be told not only what happened, but why it matters and what they can do. This model would benefit platforms as well. Companies that adopt a clear, usable privacy report could build trust, reduce customer service burdens, and position themselves as family-friendly brands. They would also reduce legal exposure. The FTC and state Attorneys General increasingly view vague or deceptive privacy disclosures as unfair or deceptive under section 5 of the FTC Act.[118] A month-

115 *See* Kibby, *supra* note 97.

116 *See* Solove, *supra* note 23, at 638.

117 *See id.* at 615 (noting that the California Consumer Privacy Act requires a conspicuous toggle button that users may click to opt out of a company's selling or sharing of personal information, but arguing this "fail[s] to guarantee that the privacy notices are read").

118 *See* 15 U.S.C. § 45(a)(1). See Mobilewalla, Inc., File No. 202-3196 (F.T.C. Jan. 14, 2025), and Gravy Analytics, Inc., File No. 212-3035 (F.T.C. Jan. 14, 2025), for how the FTC approved consent orders prohibiting Defendants from collecting, using, or selling location data without clear and conspicuous notice to, and affirmative express consent from, consumers after determining Defendants had misleading privacy disclosures.

ly privacy report that is uniform and consistent could serve as affirmative evidence of compliance.

Moreover, this approach complements legal notice requirements. Just as nutrition labels do not replace ingredient lists but distill the key ingredients in a standard American's diet, a monthly privacy report would distill privacy disclosures into an intelligible, consistent format. It can also serve as a tool for enforcement and parental redress when paired with backend access logs and audit trails. Misrepresented data practices in a report could become a potential basis for regulatory action.

Ultimately, the monthly privacy report transforms privacy from a one-time interaction into an ongoing conversation. It brings visibility to invisible processes. It equips parents with actionable intelligence. And it reshapes the role of the platform from passive collector to active participant in data stewardship. This ensures privacy is a shared responsibility.

B. Equity in the PFP Ecosystem

A PFP system must be more than a technical feature or market offering. It must be designed from the outset to serve families equitably, or else it risks deepening the digital divide it claims to bridge. As Part II explained, the most vulnerable children are often those whose parents have the least access to privacy-enhancing tools due to cost, language, education, time, or trust. Any viable PFP framework must confront this reality and not reinforce it.

The first and most obvious concern is cost. If PFP services require a monthly payment—no matter how small—some families will be excluded. These families may already be facing economic pressures around rent, food, and health care. Although privacy is important, its cost should not force consumers to choose privacy over essentials.[119] But the concern about privacy as a luxury good, at least as described by Elvy, is related to privacy discount plans or services.[120] The monthly privacy report would not be offered as a sort of privacy discount but as an additional transparency and choice mechanism for parents.

To address this, PFP systems must offer a free baseline level of protection. No family should be required to pay in order to access basic tools for monitoring and controlling their child's data. The paid tier, if adopted, would offer enhanced features like the

119 *See* Elvy, *supra* note 31, at 1405.

120 *See id.*

monthly privacy report. This mirrors the approach taken in other regulated contexts. For instance, federal law mandates that all Americans are entitled to one free annual credit report from each major bureau; premium services like credit monitoring or identity theft protection can be purchased separately.[121] Similarly, broadband providers offering government-subsidized internet under the Affordable Connectivity Program are not permitted to gate essential access behind premium paywalls.[122] The same logic should apply to children's data.

But financial barriers are only part of the problem. Educational and cultural barriers are equally problematic. A 2018 study demonstrated that privacy policies for more than sixty youth-oriented apps in the Apple and Google Play Stores were written at a reading grade level well above the average reading level of U.S. adults.[123] Interfaces are dense and buried within app settings that require digital literacy to navigate.[124] For families with lower digital literacy, privacy policies do little to warn them of privacy- and security-related harms.[125] Those from lower-income communities may also be vulnerable because of cultural privacy practices.[126] The design of the monthly privacy report must therefore prioritize linguistic and cultural inclusivity, plain language communication, and visual aids (such as icons, alerts, and risk indicators) that support understanding across literacy levels.

Usability is another critical factor. Time-strapped parents need tools that work without extensive setup, tech support, or ongoing calibration. The PFP system must be plug-and-play, meaning it integrates with existing devices and requires minimal

---

121 Fair Credit Reporting Act, 15 U.S.C. § 1681j.

122 *Affordable Connectivity Program*, FED. COMMC'NS COMM'N, https://www.fcc.gov/affordable-connectivity-program [https://perma.cc/M297-CD9M] (last visited Dec. 22, 2025).

123 Gitanjali Das et al., *Privacy Policies for Apps Targeted Toward Youth: Descriptive Analysis of Readability*, 6 JMIR MHEALTH & UHEALTH 1, 1 (2018) ("Analysis of privacy policies for these 64 apps revealed an average [reading grade level] of 12.78, which is well above the average reading level (8.0) of adults in the United States.").

124 Taylor Maguire, *The Hidden Risks of Complicated Privacy Settings in Popular Apps*, EMPYRION TECHS. (Aug. 27, 2024), https://www.empyrion.net/resource/the-hidden-risks-of-complicated-privacy-settings-in-popular-apps [https://perma.cc/8WR6-HZE9].

125 *See* Mary Madden et al., *Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 WASH. U. L. REV. 53, 62 (2017).

126 *Id.* at 56 ("In addition to the harms created by targeting or exclusion from opportunity, the poor may face magnified privacy vulnerabilities as a result of community-specific patterns around technology use and knowledge gaps about privacy- and security-protective tools. Legal scholars have identified a broad group of consumers as 'privacy vulnerable' when they 'misunderstand the scope of data collection and falsely believe that relevant privacy rights are enshrined in privacy policies and guaranteed by law.'" (citation omitted)).

configuration for a broad spectrum of mobile devices.[127] It should also offer flexible access options—such as mobile-first design, SMS-based alerts, or even voice-response systems for those who prefer audio interfaces.

Critically, equity in PFP models must be strongly regulated. Regulation is essential to prevent platforms from ignoring the hardest-to-reach users. The FTC and state Attorneys General should incorporate equity audits into their oversight of children's privacy practices and evaluate whether they work for families across income levels, languages, geographies, and device types. Civil rights groups and consumer protection organizations should also be empowered to test PFP systems for disparate impact and file complaints when inequities arise. In short, privacy can't be pay-to-play. It must be pay-to-enhance. And enhancement must never come at the expense of fairness.

C. FTC Enforcement and Market Incentivization

1. The FTC's Legacy of Privacy Regulation

No matter how well-designed a PFP model may be in theory, its real-world impact depends on effective regulation and enforcement. Without robust oversight, PFP tools could devolve into glossy dashboards with no legal teeth. The model must be embedded in a regulatory architecture that defines minimum standards, mandates transparency, and deters abuse in order to succeed. That task will fall primarily to the FTC, which remains the de facto national regulator of privacy in the U.S.[128]

The FTC's authority under section 5 of the Federal Trade Commission Act to prohibit "unfair or deceptive acts or practices" provides a strong foundation.[129] Historically, the FTC has used this authority to challenge companies that misrepresent their data practices, enforce privacy statutes, and regulate data transfers between the U.S. and the European Union.[130] It has also enforced COPPA, which requires verifiable parental consent before collecting personal information from children under thirteen.[131] Howev-

127 Elvy, *supra* note 31, at 1400–01 ("Research on the historical digital divide and the demographics of smartphone users indicates that iPhone users tend to have significantly higher incomes than Android users, and low-income individuals frequently rely on smartphones for internet access since 'they do not have broadband.'" (citation omitted)).

128 *See* Khan, Levine & Nguyen, *supra* note 18, at 1380.

129 15 U.S.C. § 45(a)(1).

130 Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585 (2014).

131 15 U.S.C. §§ 6501–6502.

er, the Agency's COPPA enforcement has been somewhat limited by the failure of federal lawmakers to pass updates to the law as the battle over privacy for children alone versus privacy for all Americans continues.[132]

That may be changing. In January 2025, the FTC finalized long-awaited updates to the COPPA Rule, adding restrictions on targeted advertising, limiting data retention, and enhancing parental access rights.[133] These amendments open the door to a more proactive approach that could support the deployment of PFP tools as part of a comprehensive privacy compliance strategy. Under the new rule, parents have "new tools and protections to help them control what data is provided to third parties," including a parental opt-in for third party advertising and other changes that address "how children's data is being shared and monetized."[134] Moreover, the proposed changes would require the FTC-approved COPPA Safe Harbor programs to publicly disclose membership lists and report additional information to the FTC,[135] and—at least for companies who wish to comply with the Safe Harbor programs—these requirements could support additional regulatory mandates like monthly privacy reports with streamlined control panels and minimum usability standards for parental tools.

Beyond COPPA, the FTC has also signaled growing interest in platform accountability. In recent reports and public statements, the Agency has criticized "dark patterns," which are manipulative user interfaces and other practices that exploit users' cognitive biases to suppress privacy choices.[136] Many current children-targeting applications suffer from these defects and impact parental decision-making.[137] A PFP system could prioritize simplicity and accessibility and serve as a model of compliance, while platforms that refuse to adopt such systems may face increasing scrutiny for unfair practices. Perhaps more importantly, the FTC recently used its rulemaking authority under the Magnuson-Moss Act to crack down on dark patterns.[138] Although the Magnuson-Moss rulemaking process is lengthy and politically

132 *See* Steinberg, *supra* note 6, at 454.

133 *See* FTC Finalizes Changes, *supra* note 15.

134 *Id.*

135 *Id.*

136 *See* BUREAU OF CONSUMER PROT., *supra* note 112, at 1–2.

137 *See id.* at 10.

138 Khan, Levine & Nguyen, *supra* note 18, at 1428 (noting that "[d]eploying its [Magnuson-Moss] rulemaking authority [to address dark patterns] . . . represented a significant shift" and a new strategy for the FTC).

fraught,[139] it allows for the creation of binding rules that define acceptable business practices. For example, the FTC could adopt rules specifying what a monthly privacy report must contain, what language it must use, how often it must be delivered, and what technical standards apply.[140] The Agency could also mandate disclosures about whether a platform offers paid privacy enhancements and require that those enhancements meet specific efficacy benchmarks to ensure that parents are not simply paying for the illusion of control. Enforcement, however, remains a sticking point for several reasons.

First, the FTC lacks direct fining authority for first-time violations of section 5, and its enforcement powers are limited to consent decrees and settlement orders.[141] The FTC relies on consent decrees and settlement orders strategically because it has limited resources.[142] These constraints mean that the FTC must be selective and strategic in its cases. To maximize impact, the Agency could partner with state Attorneys General, who could bring actions under parallel state laws. In addition, Congress has repeatedly failed to expand the FTC's enforcement powers through new legislation, including recent unenacted bills KOSA and COPPA 2.0.[143]

Second, any FTC rulemaking will now be impacted by the landmark 2024 U.S. Supreme Court decision in *Loper Bright Enterprises v. Raimondo*.[144] *Loper Bright* overruled the four-decade-old *Chevron* doctrine, holding that under the Administrative Procedure Act, courts must exercise independent judgment in interpreting ambiguous statutes rather than deferring to federal agency interpretations.[145] Although "FTC representatives have stated that this change will have little effect on key issues relat-

---

139 *See* Jon Leibowitz, Chairman, Fed. Trade Comm'n, Remarks at the Association of National Advertisers Advertising Law and Public Policy Conference (Mar. 18, 2010) (transcript available at https://www.ftc.gov/sites/default/files/documents/public_statements/association-national-advertisers-advertising-law-and-public-policy-conference-prepared-delivery/100318nationaladvertisers.pdf [https://perma.cc/HL9W-KLXX]) ("The requirements to promulgate a rule under these procedures are so onerous that the agency has not proposed a new Mag-Moss rule in 32 years."); Solove & Hartzog, *supra* note 130, at 620 (claiming "the FTC has only Magnuson-Moss rulemaking authority, which is so procedurally burdensome that it is largely ineffective").

140 *See* 15 U.S.C. § 57a(b)(1)–(2)(A) (outlining FTC unfair or deceptive acts or practices rulemaking proceedings under Magnuson-Moss).

141 *See* Solove & Hartzog, *supra* note 130, at 605.

142 *Id.* at 624.

143 Kids Online Safety Act, S. 1409, 118th Cong. (2023); Children and Teens' Online Privacy Protection Act, S. 1628, 117th Cong. (2021).

144 *See* 603 U.S. 369, 412–13 (2024).

145 *Id.*

ed to data privacy,"[146] this shift suggests that any legislative action which grants FTC rulemaking authority could be impacted.

Nevertheless, the FTC can support the deployment of PFP models like the monthly privacy report envisioned in this Article. For example, the Agency could issue guidance documents or staff reports that define what a "reasonable" monthly privacy report looks like under section 5. It could launch industry workshops to solicit input from child development experts, designers, educators, and parents. It could also publish compliance checklists or technical templates to help smaller platforms implement PFP tools without prohibitive costs. The FTC has the authority, the expertise, and (increasingly) the political support to make PFP a reality. But it must act deliberately. A good tool in the wrong hands—or one implemented without guardrails—can cause more harm than good. But the success of any PFP model will depend on whether platforms see a business case for adoption. Lasting changes in the tech sector, particularly for privacy changes, often include a balance of stringent regulation and market innovation.[147]

2. The Market and Privacy Innovation

Consumer demand for privacy is rising, especially among parents, and Americans generally agree that the responsibility for protecting children's privacy should be shared between parents, tech companies, and the government.[148] A recent Pew Research Center study of over 5,000 U.S. adults found:

> Americans worry about kids' online privacy – but largely expect parents to take responsibility. Some 89% are very or somewhat concerned about social media platforms knowing personal information about kids. Large shares also worry about advertisers and online games or gaming apps using kids' data. And while most Americans (85%) say parents hold a great deal of responsibility for protecting kids' online privacy, 59% also say this about tech companies and 46% about the government.[149]

---

146 Jeffrey M. Stefan & Marisa K. McConnell, *Impact of Chevron Decision on Compliance Risk Under Data Protection Regimes*, VARNUM (July 22, 2024), https://www.varnumlaw.com/insights/post-chevron-impact-data-privacy/ [https://perma.cc/W686-LP5T].

147 *See* Anu Bradford, *The False Choice Between Digital Regulation and Innovation*, 119 NW. U. L. REV. 377, 410–11 (2024) (describing how data privacy regulation does not have "a one-directional effect on innovation," but instead spurs new innovations, including social and market innovations).

148 *See* COLLEEN MCCLAIN ET AL., PEW RSCH. CTR., HOW AMERICANS VIEW DATA PRIVACY 6 (2023), https://www.pewresearch.org/wp-content/uploads/sites/20/2023/10/PI_2023.10.18_Data-Privacy_FINAL.pdf [https://perma.cc/4UZY-NKSC].

149 *Id.*

Companies are beginning to respond. Apple, for example, has heavily marketed its ATT framework as a selling point for privacy-conscious users.[150] While ATT is not specific to children, it demonstrates how privacy features can serve as brand differentiators. Similarly, Meta's rollout of a paid, ad-free experience in Europe signals a willingness to monetize privacy as a premium offering.[151] These developments suggest that platforms recognize privacy as a value proposition, not just a compliance cost, especially in light of both regulation and market innovations. A PFP model fits well within this trend. It allows platforms to offer differentiated service tiers, including a free version with default privacy protections, and a premium version with enhanced tools such as monthly privacy reports, predictive alerts, and granular parental controls. Just as platforms now sell cloud storage upgrades or priority customer support, they can sell a model that reflects what the above study demonstrated: Parents are still seen as the primary gatekeepers of children's online privacy, but tech companies and regulators are still key stakeholders.[152]

Beyond direct consumer revenue, PFP also opens the door to advertiser relationships that prioritize trust. Brands want to avoid being associated with unethical data practices, especially those involving children. A platform that adopts a certified PFP program could attract advertisers seeking to align with "safe" digital environments. Just as law firms pursue ranking in Chambers and Partners,[153] platforms could pursue privacy certifications that signal their ethical handling of user data. These reputational signals matter in an era of viral backlash.

PFP adoption could also streamline compliance costs. Right now, companies have to comply with some sectoral federal privacy laws, at least nineteen state-specific consumer privacy laws, and even some international privacy regulations like the European Union's GDPR.[154] As regulators in the U.S. and around the

---

150 *See We're Committed to Protecting Your Data*, APPLE: PRIVACY, https://www.apple.com/privacy/features/ [https://perma.cc/3258-7GRC] (last visited Nov. 16, 2025).

151 *See Facebook and Instagram to Offer Subscription for No Ads in Europe*, META (Nov. 12, 2024), https://about.fb.com/news/2024/11/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/ [https://perma.cc/K5E2-M6HN].

152 McClain et al., *supra* note 148.

153 Chambers and Partners is an analytics company that ranks law firms and associated lawyers based on practice areas across the globe. *See* CHAMBERS & PARTNERS, https://chambers.com/ [https://perma.cc/CP77-SBF9] (last visited Nov. 16, 2025).

154 *See U.S. Privacy Laws*, ELEC. PRIV. INFO. CTR., https://epic.org/issues/privacy-laws/united-states/ [https://perma.cc/UC6M-KV9J] (last visited Nov. 16, 2025) (providing a nearly comprehensive list of federal privacy laws); INT'L ASS'N OF PRIV. PRO., *supra* note

world tighten enforcement, platforms face increasing costs for privacy failures.[155] Implementing PFP features proactively—before they are required—can mitigate these risks and help companies streamline their compliance efforts by providing the very data that is already required of them by piecemeal legislation across the country and around the globe.

Investors may also exert pressure. Privacy and data governance increasingly appear as key indicators in environmental, social, and governance (ESG) compliance.[156] A platform that can demonstrate robust protections for children's data may become more attractive to institutional investors and mission-driven capital. These pressures are especially relevant for publicly traded tech companies, which face scrutiny not only from regulators but also from shareholder advocacy groups concerned about long-term reputational risk.[157]

Finally, there's the matter of international harmonization. Even if the U.S. is slow to adopt national privacy legislation—for children or for all Americans—global companies must comply with stricter frameworks elsewhere. The European Union's Digital Services Act and AADC impose far-reaching obligations on platforms that serve minors, including requirements for privacy-by-default, data minimization, and age verification.[158] Adopting PFP features across markets may simplify compliance and help companies build a coherent global privacy strategy. To be clear, platforms likely won't altruistically adopt PFP. But they may adopt it for customer retention, brand positioning, regulatory relief, investor confidence, and competitive edge. Privacy advocates

94; Bradford, *supra* note 147, at 405 (stating that U.S. Fortune 500 companies collectively spent over $7 billion on GDPR compliance leading up to its effective date in 2018).

155 Bradford, *supra* note 147, at 405.

156 *A New Frontier: Data Protection and Privacy in ESG*, PRICEWATERHOUSECOOPERS (Oct. 9, 2023), https://www.pwc.com/ke/en/blog/data-protection-privacy-in-esg.html [https://perma.cc/52LV-KFPQ].

157 Zack Mukewa, *Shareholder Activism and Good Governance Hygiene for Publicly Traded Companies*, LAMBERT (Dec. 19, 2024), https://lambert.com/shareholder-activism-and-good-governance-hygiene-for-publicly-traded-companies/ [https://perma.cc/FX58-CXMM].

158 *See* Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC, 2022 O.J. (L 277) 1, 19, 65 (EU); Elizabeth Denham, *Age Appropriate Design: A Code of Practice for Online Services*, INFO. COMM'R'S. OFF., https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/ [https://perma.cc/K9AB-SQ66] (last visited Nov. 16, 2025).

have argued that it is better to build in privacy rather than "bolt it on . . . after the fact."[159]

A well-designed PFP system integrates privacy into the product, the process, and the pitch. But if designed poorly or deployed without safeguards, PFP systems can amplify the very harms they aim to mitigate. They may enable predatory pricing structures or obscure deeper data collection practices (especially if dark patterns remain pervasive). As such, any implementation of PFP must include a clear set of legal and ethical guardrails to prevent misuse and protect families from exploitation.

One major concern is that companies may use PFP offerings to justify excessive data collection in their "free" tiers. The danger here mirrors patterns seen in the digital advertising economy, where platforms optimize for engagement and data extraction, then upsell privacy as a premium feature, effectively turning user vulnerability into a revenue stream.[160] This is the dark side of privacy-by-design, generally, but also of PFP models in which manipulation is the default and autonomy costs extra. Without regulatory constraints, companies may treat PFP as a get-out-of-jail-free card: *We gave parents the option to pay for control; if they didn't, that's on them*. To prevent this, regulators must impose minimum privacy baselines that apply across all service tiers. Every child—regardless of whether their parent pays for the monthly privacy report—should benefit from core protections found in COPPA and its updated Final Rule, such as prohibitions against behavioral ad targeting, strict limits on data sharing, and accessible transparency about data collection.[161]

Additionally, PFP must not be allowed to circumvent consent requirements or obscure notice obligations. For example, a platform should not claim that by subscribing to a PFP plan, a parent has automatically consented to future data uses not clearly disclosed. Nor should a PFP subscription waive the child's rights under existing law. Strong guardrails must prohibit such tactics and ensure that every data practice is independently justified and subject to scrutiny. Moreover, parents, policymakers, and companies must remain attentive to evolving threats. As artifi-

159 ANN CAVOUKIAN, PRIVACY BY DESIGN IN LAW, POLICY AND PRACTICE: A WHITE PAPER FOR REGULATORS, DECISION-MAKERS AND POLICY-MAKERS 11 (2011).

160 *See* Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 634 (2014) (asserting that companies with freemium business models "devote remarkable amounts of attention and investment to the collection of data from and about free-riding consumers of their products").

161 *See* 15 U.S.C. §§ 6501–6506; FTC Finalizes Changes, *supra* note 15.

cial intelligence tools become more sophisticated, companies will undoubtedly be (and already are) incentivized to use them to infer sensitive attributes about children from seemingly innocuous behaviors.[162] In 2025, the FTC noted a recent complaint against Amazon when its voice assistant, Alexa, retained children's voice recordings indefinitely and used the data to train Alexa's algorithm.[163]

But artificial intelligence can also be a benefit to companies and to children's privacy. For example, "emerging AI-based devices and services can automatically detect when a child's online behavior indicates that their well-being might be compromised" and "notify parents or immediately block harmful content."[164] Scholars have suggested that companies should voluntarily provide these tools by design in the absence of parental demand, and proposed "an indirect government approach that would *influence*—rather than oblige—the development, implementation, and education of algorithmic parenting technologies."[165] Perhaps more closely relevant to this Article's proposition, scholars have also suggested that algorithmic parenting technologies should be accessible to all, and a host of stakeholders—from schools to social programs and family courts to government agencies—can collaborate to make these technologies as accessible as possible (even if they never achieve accessibility for all).[166]

Ethical considerations, then, must guide the entire PFP ecosystem. Developers and designers should engage in privacy-centered design processes that foreground the needs and limitations of parents. User testing should include families from diverse socioeconomic and cultural backgrounds. Feedback loops should be built in, allowing parents to flag problems, suggest improvements, and participate in the governance of the tools they rely on. The long-term legitimacy of any PFP framework depends on trust—and trust cannot be commanded by parents, policymakers, or companies alone. It must be earned through shared transparency, usability, consistency, and responsiveness. That means platforms must not only meet their legal obligations but also treat privacy as a moral obligation, especially when it concerns children.

The PFP model this Article proposes is not a license to shift responsibility from companies to parents. It is an opportunity to

---

162 *See* FED. TRADE COMM'N, *supra* note 3, at v–vi.

163 *See* Atleson et al., *supra* note 36.

164 Eldar Haber & Tammy Harel Ben Shahar, *Algorithmic Parenting*, 32 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1, 4 (2021).

165 *Id.* at 49.

166 *See id.* at 54–63.

share that responsibility and empower parents without disempowering children, to offer options without creating inequities, and to build safer digital environments that don't depend on perfect vigilance or disposable income. With proper guardrails and accountability mechanisms, PFP can become a powerful tool for reform. But without those conditions, it's just another product, one that neither parents nor children want or deserve.

IV. A PATH FORWARD: REGULATING CHILDREN'S BEST PRIVACY INTERESTS

A. Divorcing Consent

For over two decades, American privacy law has leaned heavily on the deceptively simple premise that parents can meaningfully control their children's digital lives. At first glance, this premise seems both intuitive and empowering. After all, who knows a child better than their parent? But in the modern digital ecosystem, where parents often lack the time or understanding to meaningfully consent to certain data collection practices and intentionally or unintentionally act against their child's best interests, parental control alone—through parental consent regimes—does not suffice.[167] It is invoked to justify weak statutory protections, to offload corporate responsibility onto parents, and to mask the growing asymmetry between families and tech platforms. The law may say "*ask the parent*," but it rarely gives the parent the tools, time, or leverage to say anything meaningful in return.

This hollowing out of parental authority begins with the structure of consent and the lack of consideration for teens over thirteen under COPPA.[168] The statute assumes that, armed with appropriate disclosures, parents will exercise informed judgment about whether their child's data should be shared. But this assumption is wildly out of step with today's digital environment. COPPA may demand parental consent, but it does little to ensure that consent is informed, and it does little to protect the millions of teens over thirteen who provide their data to streaming services and social media platforms. Moreover, consent mechanisms often rely on frictionless clicks or passive opt-ins, which further dilute the idea of meaningful choice.[169] What's more, even if parents want to exercise control, their time and cognitive bandwidth are limited. For working-class families juggling jobs, transporta-

167 *See* Takhshid, *supra* note 5, at 1417, 1421; Steinberg, *supra* note 6.
168 *See* 15 U.S.C. §§ 6501–6506.
169 *See* Solove, *supra* note 23, at 607–10.

tion, childcare, and household demands, the idea of spending hours poring over settings, policies, and platform disclosures is simply unrealistic.

These challenges are compounded by design choices that frustrate parental engagement. Dark patterns are especially harmful in child-directed contexts.[170] For instance, parents may unwittingly agree to a host of coerced actions, subtly steering them toward the default that benefits the platform.[171] Some platforms even gamify the consent process, suggesting that limiting data access may reduce the child's experience or prevent certain features from working.[172] When consent is manipulated or obscured, the supposed control offered to parents becomes illusory.

Moreover, COPPA's age cutoff—under thirteen—reflects outdated assumptions about children's development and fails to reflect how kids actually engage with technology. Today, children under thirteen are frequent users of general-audience apps like YouTube, Instagram, TikTok, and Discord, which routinely avoid COPPA's requirements by claiming not to "knowingly" target minors.[173] This fiction allows companies to operate in a compliance gray zone, where they avoid responsibility unless they have actual knowledge of a child user. Parents are thus asked to consent on platforms that pretend their children aren't even there.

Complicating matters further is the asymmetry of knowledge between families and platforms.[174] Companies possess a level of information about user behaviors, preferences, vulnerabilities, and patterns of use that users—parents or children—could never hope to match. From a single child's usage, platforms can infer mood states, insecurities, and social anxieties.[175] They use these inferences to curate feeds, serve ads, and shape online experiences in ways that are invisible to parents and regulators alike.

This reality undermines the feasibility of parental control and its moral and legal coherence. How can a parent's one-time consent satisfy the obligation to protect a child's privacy over

170 *See* BUREAU OF CONSUMER PROT., *supra* note 112, at 3, 11.

171 *See id.* at 24–25.

172 *Id.* at 23–25. In the FTC's chart of common dark patterns, these types of dark patterns would likely be considered interface interference or coerced actions. *Id.*

173 *See* MacDonald, *supra* note 92, at 594.

174 *See* Vagle, *supra* note 90, at 79.

175 Fed. Trade Comm'n, Comment Submitted by Fairplay and Center for Digital Democracy (Dec. 1, 2022), https://www.regulations.gov/comment/FTC-2022-0053-1144 [https://perma.cc/76CU-HEQC].

time if platforms are building profiles based on recurring behavioral analytics?

While consent mechanisms remain the primary vehicle through which privacy is ostensibly protected in the U.S.,[176] their effectiveness is further hampered by the piecemeal and outdated nature of federal and state privacy regulation. COPPA remains the central statute governing online data practices for children under thirteen, but it was enacted in 1998—long before the explosion of mobile apps, social media platforms, behavioral advertising, or AI-powered recommendation engines.[177] The statute's definitional scope, enforcement structure, and technological assumptions no longer align with the realities of how children engage with digital services. Although the FTC has taken steps to modernize the rule through updates such as the 2013 Final Rule and the most recent 2025 revisions, these amendments have not been sufficient to close the structural gaps that leave children exposed to pervasive surveillance and manipulation.[178] Without a single statute to govern the full spectrum of data collected from children across platforms, apps, and devices, some states have proposed children-focused privacy laws.[179] Unfortunately these laws have been temporarily enjoined as likely violative of the First Amendment, as most of them restrict children's and teens' speech on these platforms, and it seems likely that "privacy laws aimed at protecting children online have difficulty passing constitutional muster."[180]

B. Regulation as a Surrogate

The FTC's role as enforcer is admittedly limited. Although the Agency has brought high-profile enforcement actions against TikTok, YouTube, and Epic Games for COPPA violations, its overall capacity to investigate and penalize misconduct remains modest. The Agency's budget is small compared to the scale of the surveillance economy, and its authority to penalize violators is handicapped by its statutory authority and procedural hurdles.[181] Moreover, the FTC's reliance on consent orders and negotiated settlements often fails to produce systemic reform. Yet the FTC has been the most active and effective privacy regulator at

176 *See* Solove, *supra* note 23, at 593.
177 *See* 15 U.S.C. §§ 6501–6506; MacDonald, *supra* note 92, at 594.
178 *See* FTC Finalizes Changes, *supra* note 15.
179 *See* MacDonald, *supra* note 92, at 596.
180 *Id.*
181 *See* Solove & Hartzog, *supra* note 130, at 609.

the federal level, and it has shown a renewed commitment to protecting children's privacy.

This Article contends that these realities produce an unclear path forward for children's privacy. The current system could remain because Congress is unable to pass comprehensive privacy legislation and regulate unethical data practices, leaving parents as the sole gatekeepers of their children's privacy through consent-based regimes at the federal and state level—a system that has been well-documented as clearly harmful to parents, children, and society.[182] Or a new system could emerge that refuses to accept a false dichotomy (where privacy is either a commodity or not) and refuses to isolate one or two of the stakeholders as responsible for children's privacy and instead distributes responsibility among parents, regulators, and companies. This Article argues that privacy's value is intrinsically diminished by its commodification and market norms alone cannot dictate privacy regulation.[183] However, this Article also suggests—and the PFP model it proposes would require—a holistic approach to regulating children's privacy centered on accessible, symmetrical information given to the parent, a reasonable fee paid to the company to provide this information, and a proven regulator capable of ensuring equity and fairness.

An emphasis on parental notice and choice, especially in the context of children's privacy, is unrealistic and fundamentally inadequate. What is needed instead is a regulatory paradigm that moves beyond the transactional logic of consent and incorporates structural constraints on data flows, algorithmic practices, and platform design. A PFP model, if properly constructed, could contribute to this shift, but only if it operates within a broader legal framework that limits exploitative defaults and imposes meaningful accountability.

C. Collective Custody of Children's Privacy

In Part I, this Article introduced some of the guardrails that must be in place before a PFP model can be taken seriously. These guardrails will largely fall on the companies to design and the FTC to enforce, in an effort to ease the burden placed on parents, guardians, and caregivers. A functional PFP model requires

182 *See supra* Part II.

183 Vagle, *supra* note 90, at 108 ("[P]rivacy's value is intrinsically diminished by its commodification, and an antitrust approach to addressing information privacy harm depends, at least in part, on the acceptance of user data solely as a commodity to be bought and sold.").

strong regulatory guardrails to prevent coercion and ensure equity. These essential guardrails include design restrictions, pricing caps, public subsidies, and some baseline protections. Companies must not manipulate users into upgrading through dark patterns, misleading designs, or degraded default options. Companies should price PFP services low enough—around three to five dollars per month—for most families to afford them. Low-income families should receive discounted or free access to PFP tools, which schools, social welfare programs, or federally funded nonprofits could help provide. And companies cannot deny essential privacy rights to those who choose not to pay. PFP services must expand transparency and control rather than replace some of the emerging data subject rights found in American privacy laws. With these protections in place, the PFP model offers a transitional tool to help families navigate a complex digital environment while broader reforms continue to take shape.

Of course, this Article describes a non-exhaustive list of guardrails, some of which are as unlikely to be adopted as it is that Congress will pass a drastic reformation of COPPA any time soon. However, this section will touch on some of these guardrails and how the FTC has the momentum and expertise to ensure a regulated, equitable PFP model.

1. Design Restrictions

The vulnerabilities of children in digital spaces are often the result of intentional platform design choices. Companies actively shape children's interests and exploit developmental psychology to maximize engagement and data extraction. As platforms compete for attention in an economy fueled by surveillance, children become both the product and the testing ground for increasingly sophisticated behavioral techniques. These practices raise serious ethical, psychological, and legal concerns, especially when children are treated not as autonomous beings with rights, but as passive data sources to be optimized and monetized.

One of the most pervasive tactics is persuasive interface design, because companies understand that it is hard for someone to prove a privacy harm if neither the user nor the regulator is able to understand how the company's systems or processes work.[184] Social media apps and streaming services deploy mechanisms like infinite scroll, autoplay, algorithmic recommenda-

184 *See* David Choffnes et al., *A Scientific Approach to Tech Accountability*, 37 HARV. J.L. & TECH. 1201, 1203 (2023).

tions, badges, streaks, and gamified rewards to sustain attention.[185] These features may seem innocuous, even entertaining, but their cumulative effect is to create digital dependencies that are difficult for children to recognize or resist. A child who stays up three extra hours to maintain a Snapchat streak or unlock a limited-time reward in Roblox is responding to a system engineered to override impulse control and not simply exercising free choice.[186]

Developmentally, children and adolescents are especially susceptible to such manipulations. Neuroscience research shows that the prefrontal cortex—the region of the brain associated with self-regulation, planning, and risk assessment—continues developing into early adulthood.[187] In contrast, the brain's reward system, which governs the response to novelty and gratification, is highly active during childhood and adolescence and can make adolescents take risks.[188] This mismatch creates a neurological window during which youth are particularly vulnerable to persuasive technologies that offer instant feedback and social reinforcement. Platforms design apps with this imbalance in mind.

For example, TikTok's "For You" page delivers a continuous, algorithmically curated stream of short videos based on micro-engagement data, and it brands itself as the leading destination for short-form mobile video.[189] While marketed as personalized content discovery, this design maximizes time-on-platform and increases exposure to advertisements that more than 70% of users consistently state they do not want.[190] Children cannot understand or control the algorithms that shape what they see, yet those algorithms shape their sense of self.

Compounding the problem is the rise of technologies that track and infer users' emotional states, something that even the United Nations Convention on the Rights of the Child recognizes as particularly harmful to children.[191] In child-directed contexts,

185 *See* FED. TRADE COMM'N, *supra* note 3, at 64.

186 *Id.* ("Further, some researchers believe that social media exposure can overstimulate the reward center in the brain and, when the stimulation becomes excessive, can trigger pathways comparable to addiction.").

187 Mariam Arain et al., *Maturation of the Adolescent Brain*, 9 NEUROPSYCHIATRIC DISEASE & TREATMENT 449, 459 (2013) ("The development and maturation of the prefrontal cortex occurs primarily during adolescence and is fully accomplished at the age of 25 years.").

188 *See id.* at 451.

189 FED. TRADE COMM'N, *supra* note 3, at 42.

190 *See id.* at 40.

191 *See* Comm. on the Rights of the Child, General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment, ¶ 42, U.N. Doc. CRC/C/GC/25 (Mar. 2, 2021).

this is even more problematic when algorithms are designed to detect when a child is sad, anxious, or bored and then serve content designed to validate those feelings to increase engagement.[192] It is a form of psychological exploitation that would be unthinkable in the physical world but remains largely unregulated online. Even when platforms offer "kid-friendly" versions of their services, such as YouTube Kids or Messenger Kids, the underlying design logics often remain the same. A parental dashboard may display what videos a child watched, but not why those videos were recommended, what data informed the algorithm, or what behavioral patterns were inferred from the session.

Attempts to mitigate these harms through design codes and voluntary standards have produced mixed results. This Article previously discussed the California AADC,[193] but the United Kingdom's AADC, for instance, requires platforms to consider the best interests of the child and minimize data collection.[194] In the U.S., companies may tout "child safety initiatives," but often those initiatives function more as PR than as substantive reform. Without binding legal standards and robust oversight, persuasive design remains a default rather than an exception.

The U.S. has tried to address these design issues. KOSA would have imposed a duty of care, required platforms to eliminate dark patterns, and disclose algorithmic processes[195] but it unfortunately failed to pass. As a result, platforms can continue to use "opaque algorithms" that exploit developmental vulnerabilities under the guise of personalization and choice.[196] Perhaps the most insidious effect of these design choices is that they normalize surveillance and manipulation as a condition of childhood. Children raised in these environments may come to see them as

---

192 *See* Carolanne Bamford-Beattie, *Understanding Social Media Algorithms: A Guide for Concerned Parents*, KIDSLOX (Sep. 16, 2024), https://kidslox.com/guide-to/social-media-algorithm/ [https://perma.cc/ZU94-X84V] ("[B]ecause the platform's algorithm prioritizes engagement, it could soon start suggesting more extreme content, such as unhealthy dieting practices or body image challenges. Similarly, on YouTube, a child searching for a simple video on coping with anxiety could quickly be led to more distressing content about mental health struggles.").

193 *See supra* Section II.B.

194 *See* Denham, *supra* note 158.

195 *See generally* S. 1409, 118th Cong. (2023) (proposing federal duties of care, safeguards, and design restrictions for platforms used by minors).

196 *Id.* § 13(a)(7)(A) (defining "opaque algorithm" as an algorithmic ranking system that determines the selection, order, relative prioritization, or relative prominence of information that is furnished to such user on a covered internet platform based, in whole or part, on user-specific data that was not expressly provided by the user to the platform for such purpose); *id.* § 13(b)(2)(A) (requiring that platforms disclose when they use an opaque algorithm).

natural. This habituation erodes the very concept of privacy. Children may internalize the idea that being watched is the price of participation, and that their value lies in what they can produce for the algorithm.

This normalization also makes resistance more difficult. Parents who attempt to limit screen time or monitor app usage may be cast as authoritarian or out of touch. Children themselves may be reluctant to challenge the platforms they perceive as sources of identity, sociality, and escape. Without systemic change, the burden falls again on families to battle technologies that are specifically designed to outpace them.

Ultimately, protecting children from design-based manipulation requires a shift from user responsibility to developer responsibility. Platform companies must be held legally accountable for the foreseeable consequences of their design choices, particularly when those consequences exploit known developmental vulnerabilities. This includes obligations to disclose information about and provide audit results of algorithms and eliminate dark patterns that subvert parents' and children's autonomy.

As Part IV continues, it will explore what a regulatory framework might look like and how regulators, companies, and civil society can work together to build it.

2. Proactive Enforcement

A robust privacy framework for children cannot rest solely on the good faith belief that companies will design with children's privacy in mind simply because a parent paid for it. It requires a regulatory agency with the power and expertise to enforce children's privacy rights across platforms. In the U.S., that role falls largely to the FTC, which enforces COPPA and engages in broader consumer protection actions against deceptive or unfair data practices. While the FTC has remained an agency operating under structural constraints and insufficient resourcing,[197] its "privacy jurisprudence has become the broadest and most influential regulating force on information privacy in the United States"[198] and, at least in recent years, has "set out on a new path" through enforcement and rulemaking to secure baseline protections, combat harmful interfaces, and protect children and teens online.[199] Although the effects of *Loper Bright* and an administration

197 *See* Solove & Hartzog, *supra* note 130, at 605.

198 *Id.* at 583.

199 Khan, Levine & Nguyen, *supra* note 18, at 1380.

change remain to be seen for FTC activity and privacy, rebuilding a proactive enforcement regime should begin by reimagining the FTC as a proactive privacy regulator empowered to investigate systemic risks and impose meaningful consequences.

To establish this paradigm, the FTC would need to promulgate binding rules governing data collection, profiling, algorithmic transparency, and age-appropriate design. Such authority would allow the FTC to go beyond the general "unfair and deceptive acts and practices" framework and create sector-specific rules for services targeting or accessible to minors. Moreover, it would clarify the boundaries of compliance, making it harder for companies to feign ignorance or exploit gray areas.

In addition to formal authority, the FTC needs greater technical expertise and investigative capacity. As platforms employ increasingly complex machine learning systems to drive engagement and data extraction, the FTC must be able to audit and assess these systems effectively. This includes hiring engineers, data scientists, child psychologists, and digital ethicists to supplement its legal staff. As Julie Cohen has argued, meaningful regulation of information systems demands an institutional apparatus capable of understanding and contesting the internal logic of algorithmic decision-making.[200] Without this, regulators will remain at a disadvantage—always one step behind industry innovation.

Further, enforcement must shift from post hoc punishment to proactive oversight. This could include requiring platforms to conduct and submit child impact assessments, similar to the data impact assessments, envisioned in the GDPR and in recent children's privacy bills,[201] prior to launching new features or modifying data practices. These assessments should evaluate foreseeable risks to children's privacy and development, be subject to an FTC audit, and result in penalties if the harms are not adequately mitigated. Public transparency around these documents would also enable civil society to hold platforms accountable and promote a culture of anticipatory responsibility.

---

200 JULIE E. COHEN, BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM 171 (2019).

201 Commission Regulation 2016/679, art. 35, 2016 O.J. (L 119) 1 (EU) ("[T]he controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."); *see also* S. 1409, 118th Cong. § 6(a)–(f) (2023) (providing that this section would have required several assessments describing the reasonably foreseeable risks of material harms to minors).

The FTC could also benefit from building a tiered compliance framework, akin to financial sector regulation, in which platforms with greater scale or more intrusive data practices are subject to enhanced obligations.[202] In children's privacy, companies collecting biometric data or using predictive analytics on children could be required to undergo annual privacy audits, maintain dedicated compliance staff, and face higher penalties for violations, some of which are already recommended by the FTC.[203] This approach would create regulatory asymmetry that matches risk with oversight, rather than treating all digital services as equally benign.

Finally, enforcement must include individual redress mechanisms. One of the major criticisms of current privacy enforcement is that remedies rarely flow to those harmed.[204] While class action suits are theoretically possible under state privacy torts,[205] federal privacy law, like COPPA, lacks robust avenues for families to seek damages or injunctive relief when children's data is misused.[206] Congress should consider adding a private right of action under COPPA or a new comprehensive children's privacy statute, allowing parents and advocates to bring enforcement actions independently or in collaboration with the FTC.

These proposals are ambitious, but not unprecedented. The European Union's GDPR empowers national regulators to issue fines of up to 4% of global revenue for violations and grants data subjects enforceable rights over their personal information, including the right to access, correct, delete, and restrict the pro-

---

202 For example, in 2023, the FTC amended the Safeguards Rule—which requires non-banking financial institutions to develop, implement, and maintain a comprehensive security program to keep their customers' information safe—to expand regulation to non-banking financial institutions. The FTC previously only enforced the Rule and the Gramm-Leach-Bliley Act, generally, against banking financial institutions. *See* Press Release, Fed. Trade Comm'n, FTC Amends Safeguards Rule to Require Non-Banking Financial Institutions to Report Data Security Breaches (Oct. 27, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-amends-safeguards-rule-require-non-banking-financial-institutions-report-data-security-breaches [https://perma.cc/HL4L-8QWP] (announcing amendments to the Safeguards Rule that require nonbanking financial institutions to report certain data security incidents to the FTC). *See generally* Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809, 6821–6827 (imposing privacy and data security obligations on financial institutions).

203 FED. TRADE COMM'N, *supra* note 3, at vi–vii.

204 *See* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 861 (2022).

205 *See* Takhshid, *supra* note 5, at 1451–54.

206 *Id.* at 1420 ("COPPA was enacted in 1998, during a different era with simpler privacy concerns. . . . As such, new privacy initiatives at the federal level should also not rely primarily on parental consent but instead offer privacy protection laws that limit the overreach of . . . companies.").

cessing of data.[207] The United Kingdom's AADC includes requirements for data minimization, profiling restrictions, and high default privacy settings, with enforcement delegated to the Information Commissioner's Office.[208] While U.S. regulators are constrained by different institutional and constitutional contexts, these examples demonstrate that robust enforcement is possible—and that protecting children's privacy requires more than symbolic action. As the next section explores, this vision also requires a shift in how we conceptualize responsibility from individual decisions to structural accountability, and from technical fixes to societal commitments.

Moreover, FTC enforcement must also be equity-aware to prevent the pitfalls of PFP. The default settings that benefit privileged children may not serve others equally well. As previously discussed, children from lower-income families are more likely to rely on free platforms that monetize their data and have limited access to paid alternatives, and parents from underrepresented communities are less likely to have the time or the money to invest in a PFP model. Elvy has astutely argued that PFP models—while potentially valuable in structuring consumer choice—risk reinforcing inequality if privacy becomes a luxury good accessible only to affluent families.[209] To address this, the PFP model must be accompanied by "equity-by-default." Design practices and regulatory safeguards must assume children deserve equal protection regardless of their parents' resources or awareness. This requires baseline protections for all users, regardless of tier.

3. Baseline Protections

Default data minimization and limits on algorithmic personalization should be non-negotiable for platforms accessed by children. Companies can offer premium services on top of these standards, but the floor must be raised industry-wide.

Embedding privacy and equity into the design process requires interdisciplinary collaboration. Legal compliance teams must work with UX designers, engineers, ethicists, and child development experts to ensure that platforms are developmentally appropriate. This includes evaluating whether design choices support healthy habits, enable meaningful parental involvement, and avoid manipulation. When privacy decisions are siloed from product development, the result is often a compliance veneer atop

207 Commission Regulation 2016/679, art. 15–18, 83(5), 2016 O.J. (L 119) 1 (EU).

208 *See* Denham, *supra* note 158.

209 Elvy, *supra* note 31, at 1400–04.

exploitative functionality. Privacy by design demands that ethics be embedded, not bolted on.

Critically, these principles must be auditable. The FTC should be empowered to review a platform's design choices and assess whether the monthly privacy report or any other feature of the PFP model satisfies equity-by-default standards. This would require technical documentation, risk assessments, and transparency reports. These tools are already common in cybersecurity and financial services. However, they are underused in the consumer tech sector, particularly in social media and streaming services.[210] Public access to these materials would also empower researchers and advocates to evaluate claims of compliance and surface gaps.

Without enforceable design standards, companies will continue to optimize for engagement and profit rather than well-being. Dark patterns and interference interfaces will always outpace user education if not structurally curtailed. Protecting children's privacy in this context means confronting these design paradigms directly and insisting that technological systems serve developmental needs rather than exploit them.

At the same time, embedding privacy by design must confront the asymmetry of power between technology firms and end users, particularly in the context of children. Even the most well-intentioned parents face substantial challenges when attempting to audit or adjust the privacy settings on platforms used by their children. The burden of understanding complex policies and maintaining controls across multiple devices and services is a structural design failure, not a reflection of parental inadequacy. By contrast, platforms possess not only vast technical knowledge but also the behavioral data to optimize against user resistance, nudging families toward options that benefit the company rather than the child.

This is particularly troubling when the platforms in question actively obscure their business models. As the FTC's 2024 6(b) report noted, companies—especially large social media platforms and streaming services—are incentivized by and routinely fail to disclose their data practices, including the extent to which children's data is used for algorithmic training, cross-device tracking, and third-party sharing.[211] In such an environment, any notion of meaningful consent is illusory. Embedding privacy and equity in-

210 FED. TRADE COMM'N, *supra* note 3, at v–vii.

211 *Id.* at ii.

to product design is, therefore, not just a better user experience, but a necessary corrective to power imbalances that render families effectively powerless in the face of complex digital systems.

Moreover, digital equity demands a more nuanced understanding of intersectionality in children's experiences online. Black, Latino, and LGBTQIA+ youth often face disproportionate surveillance and harassment online and may be subject to predictive profiling that amplifies systemic biases.[212] Design standards must therefore consider not only generic child safety, but also how different children may experience the same feature in vastly different ways. For instance, scholars have demonstrated that an AI-driven system may disproportionately reinforce feedback effects and provide little opportunity for error correction, leading to over-enforcement or exclusion.[213] Embedding equity into privacy design requires rigorous impact assessments and ongoing monitoring of disparate outcomes.

Educational institutions provide another key frontier for PFP models. As more schools adopt additional "learning" services through YouTube, Google, and other tech giants' services built into existing learning platforms, the risk of normalizing invasive data practices during childhood grows.[214] These technologies often lack transparency and are implemented without meaningful consent from families.[215] A regulated design framework would require schools and EdTech vendors to adopt the same standards applied to commercial platforms.[216] Perhaps more importantly, it would prompt a broader conversation about the role of surveillance in shaping educational environments and whether shifting

212 Samantha Lai & Brooke Tanner, *Examining the Intersection of Data Privacy and Civil Rights*, BROOKINGS INST. (July 18, 2022), https://www.brookings.edu/articles/examining-the-intersection-of-data-privacy-and-civil-rights [https://perma.cc/JFV6-MDW4] (arguing for federal legislation to prohibit "commercial surveillance practices that enable discriminatory advertising, racially biased policing, and the outing or surveillance of historically marginalized groups").

213 Pauline T. Kim, *Data-Driven Discrimination at Work*, 58 WM. & MARY L. REV. 857, 865–66 (2017) (noting these risks in the employment context).

214 Takhshid, *supra* note 5, at 1432.

215 *Id.* ("How can a parent use their judgment in deciding what is in the best interests of their child and make an informed choice when it may not even be clear what consequences the use of an application might have for their beloved child?").

216 *Id.* at 1454 ("[T]he EdTech industry is a for-profit industry, albeit one operating at schools, and the contracts between the school and the EdTech companies are of a commercial nature.").

away from parental consent and toward an ostensibly equitable PFP model would align with public policy.[217]

Finally, equity by default should be seen as a precondition for sustainable technological development and not as a constraint on innovation. Although some scholars have called regulatory responses to privacy norms "ill-advised" because technologies and norms constantly change,[218] others have advocated for abandoning the "false choice between regulation and innovation" and encouraging the "legal and institutional reforms that are necessary for tech companies to innovate and for digital societies to thrive."[219] Companies that build with children's rights in mind are better positioned to lead in a market increasingly sensitive to privacy concerns and changing consumer preferences.[220] In this way, embedding these principles becomes a form of risk mitigation, brand differentiation, and long-term value creation.

Equity-by-default is not a silver bullet. It requires clear regulatory mandates but also a meaningful cultural shift in how parents, policymakers, and companies think about childhood and technology. But without it, every other reform becomes more difficult because the default architecture of the digital world continues to undermine even the best intentions of law and policy. The future of children's privacy will depend on building a village of responsibility, one in which law, markets, and families all play coordinated roles in creating a safer digital world.

If the past three decades since the moral panic about children's online activities referenced at the outset of this Article have taught us anything, it's that no single actor can protect children's privacy alone. Parents cannot out-click or out-code billion-dollar platforms, and even when they do, they can hamper their children's autonomy.[221] Policymakers cannot write one law to neutralize every dark pattern. And even the most ethical corporations face market pressures that reward surveillance and

---

217 *Id.* ("[T]he EdTech industry has further become a necessary medium for acquiring education for many children, which underscores the public policy defense that necessitates stepping away from insufficient parental consent forms.").

218 Tal Z. Zarsky, *The Privacy-Innovation Conundrum*, 19 LEWIS & CLARK L. REV. 115, 125–26 (2015) (suggesting regulatory responses to privacy norms are "ill-advised" as technologies and privacy norms will rapidly change and instead advocating for both market innovation and social innovation).

219 Bradford, *supra* note 147, at 377.

220 *See id.* at 409.

221 Steinberg, *supra* note 6, at 470–71 (arguing that children's capacities evolve and any age-appropriate design and/or child-centered policies "must avoid treating all young people the same" and that "their need for protection must make way for their evolving need for autonomy").

personalization over restraint. The solution, then, must be collective. Protecting children's privacy in the digital age will require rebuilding a village around a robust ecosystem of shared responsibility among parents, companies, and regulators.

At the foundation of this village are parents, guardians, and caregivers, who remain children's primary gatekeepers. But the current system sets them up for failure because they—especially those from lower-income and otherwise underrepresented communities—lack the time and digital literacy to effectively manage the dozens of apps, platforms, and services their children use. Many default to blind trust, hoping that schools, regulators, or app stores have done their due diligence. Others attempt to monitor usage through screen time controls or family accounts, only to find themselves outmatched by evolving technologies and evasive interfaces.

The burden placed on parents reflects the broader fallacy of consent-based privacy models, which assume users can rationally evaluate risk and exercise rational decision-making about their privacy.[222] As scholars referenced throughout this Article have noted, this framework ignores both the sophistication of digital systems and the emotional and practical constraints of caregiving.

Parents cannot conduct nightly data audits. They cannot read forty-page privacy policies during dinner. And they should not be expected to navigate three webpages deep into a privacy dashboard just to opt out of harmful data collection, use, and disclosure that their children never asked for in the first place. Real privacy protection doesn't mean reducing the need for parental vigilance, but it means making it a little easier to act once vigilance reveals an issue.

Corporations, for their part, must abandon the myth that protecting children's privacy is bad for business. As the FTC's COPPA Final Rule amendments demonstrate, regulators are now willing to intervene where self-regulation fails and "recognize children and teens as a distinct category of consumers requiring strong protections."[223] But the real opportunity lies in embracing privacy as a market differentiator. Companies that adopt privacy-centric PFP models with accessible monthly privacy reports may be rewarded by consumers, too. A children's privacy arms race, spurred by increased revenue and increased privacy protec-

222 Solove, *supra* note 23, at 611–12 ("Human decision-making is fraught with irrationality and systematic biases and heuristics that can readily be exploited.").

223 Khan, Levine & Nguyen, *supra* note 18, at 1407.

tions, is both possible and overdue. That, combined with the FTC's new emphasis on targeting upstream data collection practices, can help make structural changes "focused on addressing business incentives and preventing injury rather than redressing it after the fact."[224] But more funding, technical staff, and legislative clarity are needed if the FTC is to function as a true digital watchdog. State Attorneys General can also fill gaps in enforcement, especially in states where recent attempts at regulating children's privacy through emerging age-appropriate design codes or social media moderation regimes have faced First Amendment challenges[225] or are reliant on parental consent or overinvolvement.[226]

This collective PFP framework may seem like a children's privacy utopia. Inequities will still arise. The FTC will lag in trying to correct those inequities. Companies will push back. And parents will make mistakes. But the goal is to reimagine shared responsibility between parents, regulators, and companies through a PFP model that recognizes parents as in need of accessible choices and children as developing citizens deserving of protection.

V. CONCLUSION

Children's privacy is a defining issue of our digital era, not just for privacy advocates but for society, generally. This Article has argued that protecting children in today's data-driven society requires more than consent-based and notice-and-choice mechanisms through inadequate federal privacy laws like COPPA and piecemeal, constitutionally problematic state privacy laws. It demands a reorientation of responsibility, one that distributes the burden across the full ecosystem of digital life. Privacy cannot be treated only as a commodity, and policymakers and companies cannot expect parents alone to police the perimeter of a playground they never chose for their children. As the failures of consent-based regimes and notice-and-choice frameworks have shown, the current model of privacy protection is fundamentally mismatched to the realities of how children engage with technology.

---

224 *Id.* at 1410.

225 MacDonald, *supra* note 92, at 591 (describing the recent laws in Arkansas, Texas, and California, all of which were either partially or totally blocked from enforcement "because they were enjoined as unconstitutional violations of the First Amendment").

226 Steinberg, *supra* note 6, at 443 ("State laws vary from state to state, some recognizing that young people need to be able to safely explore the internet while maintaining a right to privacy while other state laws prioritiz[e] giving parents control over a young person's internet use above all else. These varied laws are almost entirely in contrast with the international community's consensus on how children can be best protected in digital environments.").

The PFP model proposed in this Article offers a potential solution to the failures of federal and state privacy laws. It acknowledges the realities of market forces and consumer choice, while demanding baseline protections that ensure equity. A PFP floor must be guaranteed for all children, especially those whose families lack the economic leverage to buy their way into safety. Any framework that treats privacy as a premium feature will deepen existing inequities unless paired with equity-by-default and meaningful regulatory oversight. This Article calls for a collective framework that empowers regulators, equips parents, and enlists companies in shaping children's privacy norms. The village metaphor emphasizes that just as no caregiver can raise a child alone, no one institution can safeguard children's privacy.