TO STOP SHARENTING & OTHER CHILDREN'S PRIVACY HARMS, START PLAYING: A BLUEPRINT FOR A NEW PROTECTING THE PRIVATE LIVES OF ADOLESCENTS AND YOUTH (PPLAY) ACT

*Leah Plunkett**

In December 2019, the Federal Trade Commission (FTC) hosted a public workshop to explore updating the federal Children's Online Privacy Protection Act (COPPA) Rule.[1] The workshop followed on the heels of

* Leah A. Plunkett is an associate dean & associate professor at University of New Hampshire Franklin Pierce School of Law and a faculty associate at the Berkman Klein Center for Internet & Society at Harvard University.

[1] Taken together, the federal Children's Online Privacy Protection Act and the Children's

alleged COPPA Rule violations by Google's subsidiary YouTube, including a violation of taking personal information from children under thirteen without getting parental consent.[2] A financial settlement for $170 million reached with YouTube and Google is the highest to date for COPPA non-compliance,[3] but some lawmakers believe the tech giant should have paid more.[4] Senators on both sides of the aisle are raising an alarm that the FTC might be looking to make revisions that favor tech companies and "ultimately weaken[] children's privacy instead of improving it."[5]

The senators are right to worry, but they are wrong to think that guarding, or even improving, the COPPA Rule will provide comprehensive protection for children's digital data privacy. Since the Rule was last updated in 2013, the "online environment for children continues to evolve at a rapid pace," according to the FTC.[6] The nature and the pace of this evolution necessitate more than Rule revision. Federal lawmakers should start from scratch to enact new federal legislation that puts safeguards on what technology companies and other gatekeepers can do with the information they collect about all children under the age of eighteen, whether that information is collected directly from children or from parents, teachers, and other adults. Currently, there is no digital privacy law that regulates all forms of "sharenting," which occurs when a "parent, teacher, or other adult caregiver . . . who publishes, transmits, stores, or engages in other activities involving private information about a child in her or his care via digital channels."[7] A new law that would complement, but not repeal existing federal and state privacy protections (some of which do address some types of sharenting, most significantly by teachers),[8] would address sharenting in all its forms, as well as private information that minors share about themselves.

Online Privacy Protection Rule are referred to as "COPPA." 15 U.S.C. §§ 6501-06 (1998); 16 C.F.R. § 312 (2013).

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

[3] *Id.*

[4] Emily Birnbaum, *Bipartisan Senators Warn Against Efforts to Weaken Children's Online Privacy Law*, HILL (Oct. 4, 2019), https://thehill.com/policy/technology/464413-bipartisan-senators-warn-against-efforts-to-weaken-childrens-online-privacy.

[5] *Id.*

[6] Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, 84 Fed. Reg. 35842 (proposed July 25, 2019).

[7] LEAH A. PLUNKETT, SHARENTHOOD: WHY WE SHOULD THINK BEFORE WE TALK ABOUT OUR KIDS ONLINE xv (2019).

[8] *See infra* Part II.

This new federal law, Protecting the Private Lives of Adolescents and Youth (PPLAY), would create a lifelong prohibition on technology (or "tech") companies from using all private digital data collected from any source about children under eighteen for targeted advertising or marketing, as well as decision-making about major life opportunities. If another law or regulation permits a particular use of the data, or the child's parent (if the child is under sixteen) or the child themselves (if over sixteen) has specifically opted into the use, then that limited use would suffice.

Under PPLAY, even once children turn eighteen, the private data collected about them as children remains prohibited with regards to targeted advertising or marketing. However, these companies can use information collected after they become adults for marketing and advertising purposes.

The same lifelong prohibition would apply to the use of private data to make predictions or decisions about children's opportunities (whether as minors or as adults) to gain access to major life activities, including education, employment, health care, life insurance, health insurance, and similar opportunities.

PPLAY would also create a nutrition-label style disclosure system for digital tech products and services, which will give users comprehensive and consistent privacy information to better inform decision-making. In addition, it would create a limited "right to erasure" of content posted about children by parents, grandparents, teachers, or other trusted adults, so long as that content is not legally protected by another law or supported by a compelling interest.

There are privacy law reform efforts at the state and international levels that could inform the development of PPLAY.[9] In recent years, many states have taken a small step towards removing digital gate-keeping from parents' hands by passing new student privacy laws that regulate educational technology companies directly rather than focusing on schools and the requirement that schools get parental consent to share data.[10] The European Union has enacted comprehensive digital privacy protection for its citizens of all ages,[11] and California has done so as well.[12] Our federal government can look to these and other recent privacy law innovations as inspiration for

[9] *See, e.g.*, Brenda Leong, *FPF Guide to Student Data Protections Under SOPIPA: For K-12 School Administrators and Ed Tech Vendors*, FUTURE OF PRIVACY FORUM (Nov. 7, 2016), https://fpf.org/2016/11/07/fpf-guide-student-data-protections-sopipa-k-12-school-administrators-ed-tech-vendors/; *see generally* Commission Regulation 2016/679 of Apr. 27, 2016, General Data Protection Regulation, 2016 O.J. (L 199) 1.

[10] *See, e.g.*, Leong, *supra* note 9.

[11] *See generally* Commission Regulation 2016/679, *supra* note 9.

[12] *See generally* California Consumer Privacy Act, Cal. Civ. Code §§ 1790.100–1798.199 (2020).

crafting PPLAY and giving our children privacy and life opportunity protections from the decisions of the adults in their lives.

This essay offers (1) a snapshot of the types of practices and categories of risks posed by sharenting; (2) a map of the limitations of the current federal legal landscape that addresses sharenting; and (3) a blueprint for a new, comprehensive federal youth privacy law (PPLAY) that protects youth privacy and, by extension, their current and future life opportunities.

I. SHARENTING: WHAT IT IS & WHY IT IS RISKY (AND ALSO WHY IT CAN BE BENEFICIAL)

A. Sharenting Snapshot

"Sharenting" is a term that is rapidly gaining traction in the popular lexicon. A portmanteau of "parenting" and "sharing," the term typically refers to what parents post about their children on social media.[13] While these activities are a critical part of sharenting, they are not the sum total of sharenting.

Fully understood, "sharenting" refers to all the ways in which parents, grandparents, educators, and other trusted adults engage in any and all digital activities with the private information about the children in their homes or otherwise in their care.[14] While social media may be the most visible of these activities, there are countless others.[15] From "smart diapers" and sensor-enabled baby booties, to giving a toddler a smart toy, having an Alexa at grandma's house, teaching elementary schoolers to read with an app, monitoring a tween or teen's whereabouts using a surveillance app and beyond, "sharenting" is the default setting of today's adults.[16]

Most of the time, adults fail to even realize that a particular activity constitutes sharenting. Upon recognition, we are likely to still proceed with the best of intentions. At worst, the sharenting may be negligent, but not malicious.[17] Digital technologies deceive us about their status with respect to inside the brick and mortar "castles" of our homes, schools, and other spaces. They masquerade as part of our everyday environs—objects we have

---

13 *See*, *e.g.*, Rachel L. Harris and Lisa Tarchak, *Mom and Dad, It's My (Digital) Life*, N.Y. TIMES (Sept. 2, 2019), https://www.nytimes.com/2019/09/02/opinion/children-internet-privacy.html.

14 PLUNKETT, *supra* note 7, at xxii.

15 *See generally* PLUNKETT, *supra* note 7, at 2.

16 *See generally* PLUNKETT, *supra* note 7, at 1–15.

17 PLUNKETT, *supra* note 7, at xvii.

on our counters, in our hands, on our walls, and on our bodies.[18] They do not come equipped with a cigarette-style warning label or nutrition style information label, nothing that either shrieks a reminder that these devices are transmitting information outside of our immediate surroundings (warning label) or unpacks in a digestible way what that information is, where it is going, and why it is going there (information label). Thus, we may overlook or fail to properly understand the connectivity inherent in the device, even as we rely on that connective functionality to make the device or service useful to us. Even if we are mindful of the connectivity aspect, we are almost uniformly un-informed or under-informed of the scope, severity, and duration of the private information collection, aggregation, analysis, re-sharing, and action upon—because, as will be unpacked further in the legal landscape section, there is no reliable, accessible means for us to inform ourselves.[19]

Each child's digital journey is distinct and rapidly evolving, as both parental or other adult decision-making changes and the array of digital devices and services grows.[20] What follows is a snapshot-style profile of the areas in which a child born today will be digitized—using a fictional child and real-world new and emerging technologies. Kids today are conceived digital.[21]

As an example, imagine a fictional child Tommy, a nod to Mark Twain's canonical homage to youthful exuberance.[22] The U.S. Supreme Court has stated it is not in the business of determining when life begins.[23] But, tech companies are.[24] Fertility bracelets, fertility tracking apps, and similar devices engage precisely in that predictive space. Thus, digital tech is foreshadowing Tommy's evolution into existence. His mother's labor and delivery are videoed and shared on YouTube. His newborn pictures, complete with vital statistics (including full name and place of birth), are

---

18 PLUNKETT, *supra* note 7, at 79–80.

19 PLUNKETT, *supra* note 7, at 80.

20 PLUNKETT, *supra* note 7, at 2.

21 For the seminal work on the experiences of kids themselves in the digital era, *see* JOHN PALFREY & URS GASSER, BORN DIGITAL: HOW CHILDREN GROW UP IN A DIGITAL AGE (rev. ed. 2016). PLUNKETT, *supra* note 7 addresses the question of how the adults raising today's kids behave with respect to children's privacy.

22 The material set forth in Part I(A) offers a condensed version of the case study and accompanying discussion set forth in PLUNKETT, *supra* note 7, at 1–15. Where new information is included in this version that did not appear in Sharenthood, a specific reference for that information is provided.

23 *See* Planned Parenthood v. Casey, 505 U.S. 833, 851 (1992).

24 *See* PLUNKETT, *supra* note 7, at 2 (describing use of fertility tracking app and bracelet to determine best window for conception; the value to consumers of these and other fertility predicting products is to advise them on the best time for procreation to try to create new life).

posted on social media. Updates—detailed, regular—follow: "Tommy is having trouble sleeping, so we're using a sensor-enabled baby booty to track his sleep patterns!" "We're having trouble soothing Tommy, so we're using an AI-nanny to help!" "We think Tommy is getting woken up at night by wet diapers, so we're using a smart diaper that notifies us when it's time for a diaper change!"[25] Posting about Tommy's digital interactions constitutes two layers of sharenting: there is sharenting in the choice to use the digital device, like a smart diaper. Then there is sharenting in the digital reveal of information about the device use.

As Tommy enters the toddler years, his digital immersion continues. His parents put a video-enabled baby monitor in his nursery that they can monitor through an app on their phones. They use FaceTime, Skype, and other digital video channels to keep in touch with Tommy's grandparents, aunts, uncles, and other loved ones far away. They text and email updates, and chronicle Tommy's milestones through online photo-sharing and album-making services. They wonder why they can never find the picture they most want when they most want it, despite having thousands of them, so they get Tommy's face printed on mugs and silk-screened on canvas wall-art, pillows, and t-shirts through an online photo-service. Tommy promptly vomits on the pillow; his parents post a pic of the puke-stained fabric and tag the company that produced it, which sends them a new one, free of charge.

Tommy's parents put the digital fun right in Tommy's hands too. They give Tommy an Alexa designed for children.[26] They give him a smart teddy bear.[27] They give him their phones and iPads to watch YouTube Kids and play with apps. Eventually, they cave in and give Tommy an iPad of his own. Next, they give him an iPad potty to incentivize toilet training. Tommy's interactions with these and other digital technologies, as well as Tommy's parent's reflections on these interactions, are preserved and posted online through pictures, videos, and texts: "OMG! Tommy just said his first word to Alexa! It's the cutest!!"[28]

---

[25] *See* Samantha Murphy Kelly, *Pampers Is Making a 'Smart' Diaper. Yes, Really*, CNN (July 19, 2019), https://www.cnn.com/2019/07/19/tech/pampers-smart-diapers/index.html.

[26] *See* Megan Wollerton, *Amazon Launches New Alexa Device For Kids But Privacy Issues Will Still Scare Some Parents*, CNET (June 12, 2019, 10:30 AM), https://www.cnet.com/news/amazon-launches-new-alexa-device-for-kids-but-privacy-issues-will-still-scare-some-parents/.

[27] *See, e.g.*, Stacey Gray, *Federal Trade Commission: COPPA Applies to Connected Toys*, FUTURE OF PRIVACY FORUM (June 26. 2017), https://fpf.org/2017/06/26/federal-trade-commission-coppa-applies-connected-toys/ (listing "teddy bears" as a type of connected or smart toy available on the market).

[28] *See* Joshua McNichols & Carolyn Adolph, *Parenting in the Age of Alexa? It's Complicated*, KUOW (Oct. 21, 2019), https://www.kuow.org/stories/primed-season-3-episode-1.

Tommy also receives digital tech immersion from the other adults in his young life. His grandparents' love affair with digital tech makes his parents' affection for capturing, chronicling, and sharing look like amateur hour. His grandparents watch him a few afternoons each week when his parents are at work. They love sharing updates with their friends on social media—where their settings are not set to private.[29] At first, Tommy's parents barely notice the posts—so enmeshed are they in their own digital universes. But when they start hearing from distant cousins about how fetching their son looks when he is screaming and dumping his spaghetti dinner on his head, Tommy's parents begin to reconsider their position. They ask Tommy's grandparents to dial back their digital *kvelling*, prompting inter-generational friction that plays out over a text chain—one that will cause arthritis to flare up even for the participants who did not enter the back and forth with any pains in their joints. When Tommy's grandparents agree to learn how to make their social media settings private, détente is reached—although Tommy's mom continues to believe that her parents in-law would benefit from staging more flattering shots of Tommy. Tommy's aunts and uncles do a better job of showing their nephew in his best light. The only child in his generation, Tommy is the recipient of endless adoring attention. Tommy's parents are more comfortable with the pictures their siblings take; while their siblings have more friends than the grandparents, Tommy's parents' reason that the pictures are cuter, and their social media universe is set to private.

Tommy's parents start to lose track of who is taking pictures of Tommy and where those pictures are going. Tommy's babysitters think he is the cutest; they put him on their Instagram feeds. The parents of other babies in playgroup, other kids on the playground, and at playdates when Tommy is old enough to play at other kids' houses without parental chaperones—they are all taking and sharing pictures as well.

When Tommy starts at the public elementary school in his neighborhood, the sharenting starts to multiply. An app to track attendance. An app to teach him math. Another app to teach him reading. A software program to teach social-emotional learning. A swipe-card linked to an app to track cafeteria purchases. A sensor to track getting on and off the bus.

[29] *See* Julie Jargon, *Grandsharenting: When Grandparents Get Carried Away on Facebook*, WALL ST. J. (Nov. 26, 2019), https://www.wsj.com/articles/grandsharenting-when-grandparents-get-carried-away-on-facebook-11574764204.

Social media and messaging surveillance.[30] Facial recognition programs.[31] Databases that track school disciplinary actions and related school-to-prison pipeline consequences. A surveillance watch that Tommy's parents put on him which he wears throughout the day that allows him to contact them, his grandparents, and his aunts and uncles if he needs them; a watch that will alert Tommy's parents if he ventures beyond their designated parameters allowing him to walk to school, attend school, then walk home.[32] For some of the devices and services the school uses, the school sends home paperwork explaining the technology and seeking parental consent prior to use. For most tech choices, no notifications or opportunities for participation decision-making are needed. For a few products, Tommy's parents first learn about them after notifications arrive in the mail indicating they have been subject to a data breach.[33] Tommy's parents already have credit monitoring set up for the family, so they brush this off.

Tommy's baseball team uses an app to schedule practice. His summer camp uses an online program for registering—complete with facial recognition technology so pictures of Tommy and his fellow campers can be easily identified, tagged, and flagged for parents who want to see them.[34] Tommy's parents install a RING doorbell surveillance system—which happens to share data with local law enforcement—so they know who is coming and going from their house; the system also captures footage of Tommy returning home one night past curfew, slightly inebriated, after a celebration with his baseball team descended into debauchery.[35] Tommy's parents install an app on his phone to provide them with around-the-clock updates on Tommy's whereabouts. Tommy is fine with the app, but he

---

[30] *See* Benjamin Herold, *Schools Are Deploying Massive Surveillance Systems. The Results Are Alarming*, EDUC. WEEK (May 30, 2019), https://www.edweek.org/ew/articles/2019/05/30/schools-are-deploying-massive-digital-surveillance-systems.html.

[31] *See* Davey Alba, *Facial Recognition Moves To a New Front: Schools*, N.Y. TIMES (Feb. 6, 2020), https://www.nytimes.com/2020/02/06/business/facial-recognition-schools.html.

[32] *See, e.g.*, *GizmoWatch*, VERIZON, https://www.verizonwireless.com/connected-devices/verizon-gizmowatch/ (last visited Mar. 13, 2020) (describing one surveillance watch marketed for parents to use for child surveillance).

[33] *See* Catherine Shu, *Education Software Marker Pearson Says Data Breach Affected Thousands of Accounts in The U.S.*, TECHCRUNCH (Aug. 1, 2019), https://techcrunch.com/2019/07/31/education-software-maker-pearson-says-data-breach-affected-thousands-of-accounts-in-the-u-s/.

[34] *See* Julie Jargon, *Facial Recognition Tech Comes to Schools and Summer Camps*, WALL ST. J. (July 30, 2019, 12:19 PM), https://www.wsj.com/articles/facial-recognition-goes-to-camp-11564479008.

[35] *See* Matthew Guariglia, *Five Concerns About Amazon Ring's Deals with Police*, ELECTRONIC FRONTIER FOUND. (Aug. 30, 2019), https://www.eff.org/deeplinks/2019/08/five-concerns-about-amazon-rings-deals-police.

remains frustrated with the home's smart thermostat which keeps out-smarting him by overriding his attempts to keep the house at eighty-five degrees Fahrenheit so he can wear shorts and tank tops all winter.

Tommy's parents suggest that he apply to colleges somewhere warm if that is his preferred attire. Tommy agrees. He asks his school guidance counselor how to put his best, flip-flop covered foot forward. She advises him to clean up his own social media, avoid entering into any online conversations that are offensive to prevalent shared cultural norms or could appear that way,[36] and to be an active visitor on the websites of the schools he is most interested in. Tommy starts to feel paranoid that schools are watching him, and he is not even there yet. And much to his dismay, they in fact are watching to determine whether or not he gets in. Tommy tunes out as she starts to describe the range of potential predictive analytics, they could run to determine his fit and likelihood of success in a school. His counselor abandons her explanation before she reaches the ways in which whichever college he does attend is likely to track his progress to make predictions—and, if necessary, pursue interventions—around his academic outcomes, mental health, and other domains. For example, his dorm room could be "smart" and extract data about Tommy in his quotidian activities, including through giving him an Alexa.[37]

In college, Tommy gets his first part-time job after taking an online employment temperament fitness test.[38] He finds working in an office stultifying, so he quits and joins the gig economy, running random errands for strangers for pennies on the dollar. Tommy fits in well at college, making friends and embracing the freedom away from his parents' gaze. But his parents continue to insist he use a monitoring app so they know his whereabouts at all times.[39] Tommy resigns himself to that requirement. One night, Tommy comes home from delivering food to find pictures of him as

---

[36] *See, e.g.*, Anya Kamentz, *Harvard Rescinds Admission Of 10 Students Over Obscene Facebook Messages*, NPR (June 6, 2017), https://www.npr.org/sections/ed/2017/06/06/531591202/harvard-rescinds-admission-of-10-students-over-obscene-facebook-messages (providing example of youth shared content that led to negative outcome for the youth).

[37] *See* Elizabeth Weise, *Alexa, When's My Next Class? This University Is Giving Out Amazon Echo Dots*, USA TODAY (June 20, 2018), https://www.usatoday.com/story/tech/talkingtech/2018/06/20/amazon-echo-dots-link-student-accounts-northeastern-university/715360002/.

[38] *See* CATHY O'NEILL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY 105 (2016).

[39] *See* Abby Ohlheiser, *Don't Leave Campus: Parents Are Now Using Tracking Apps To Watch Their Kids At College*, WASH. POST (Oct. 22, 2019), https://www.washingtonpost.com/technology/2019/10/22/dont-leave-campus-parents-are-now-using-tracking-apps-watch-their-kids-college/.

an infant—pudgy, diaper-clad, screaming—printed out and plastered up and down the hall of his dorm room. Enraged, he calls his parents, who trace the images back to old posts by his grandparents when they used to baby-sit him. His parents promise to look into how to deactivate the Facebook pages that belonged to his grandparents, now deceased. Tommy's parents, concerned about his potential to derail positive social relationships, attempt to distract him by sending him a smart pet: a robotic dinosaur which can roam the halls. While it cannot destroy the posters, it at least offers a distraction from them.[40]

Is the dinosaur gift a form of sharenting? At this point, Tommy is an adult, legally (for most purposes) if not yet emotionally and psychologically. He is certainly capable of deciding whether, when, how, and why to use a smart toy given to him as a gift. Because Tommy is making the decision on his own terms about whether and how to use the toy, the dinosaur should not constitute sharenting. The equation is different, of course, when parents or other trusted adults place a smart toy or other digital device or service in the hands of an infant or child who has not yet attained the legal age of majority and do not yet have an adult range of decision-making capacities available to them.[41]

Determining when a digital interaction constitutes "sharenting" versus direct youth engagement with a digital offering can be a complex equation. As Tommy grows up, the variables are less clear: at what point are his parents facilitating his digital tech use (such that his use is a sharenting decision), and at what point is he in command? An infant or young child lacks the agency and other capacities to procure, set-up, and engage with a smart stuffed animal. Digital tech use in these early years thus can only reasonably be understood as sharenting: actions by a parent, grandparent, or other trusted adult to transmit children's private digital information by putting the child in a position where the information is conveyed to one or more digital tech providers—as well as any unwanted third-parties who might be in a position to intercept it.

In the elementary, middle, and high school years, the calculation shifts dramatically. Tommy's parents more or less still control the purse strings, especially in the earlier part of that life-stage spectrum. Their control over Tommy obtaining and using digital tech is no longer so absolute. Tommy may circumvent access or content controls at his school, for instance, and

---

[40] *See, e.g.*, PLEO, https://www.pleoworld.com/pleo_rb/eng/products.php (last visited Feb. 24, 2020) (displaying a smart dinosaur toy).

[41] *But see* Michael S. Lewis, *Pervasive Infancy: Reassessing the Contract Capacity of Adults in Modern America*, U.N.H.L. REV. (publication forthcoming) (Jan. 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3526991 (arguing that adults are actually no differently situated from children when it comes to today's complex contracts of adhesion in big tech and other consumer domains).

access digital content his parents might have told him is off limits.[42] Tommy is likely to obtain a device of his own at a fairly young age and no amount of in-person or digitally-based parental surveillance is sufficient to fully lock down what he does, where he does it, or with whom he does it on that device.

In such instances, many interactions are best understood as multi-faceted: there is a parental choice to give a device,[43] followed by choices by the youth user of that device about how to use it.[44] It is unnecessary to taxonomize every decision, or for every decision to need to be one hundred percent sharenting, to accept as accurate this descriptive point: across the life-stages of youth, there are actions parents can and do take that are theirs and theirs alone, or theirs primarily, to reveal their children's private information digitally, such as posting on social media or choosing to have a smart device in their home that picks up private data about everyone in the family.

Sharenting is ubiquitous and life-long (pre-life, as it were).[45] This is cause for concern because the nature of the information transmitted creates privacy harms,[46] as well as harms to children's current and future opportunities. In turn, these privacy and opportunity harms fundamentally alter children's experiences such that they are left without private places to play—to make mischief, make mistakes, and grow up better for having made them—and through that play, to develop the sense of agency and autonomy necessary to become the sequential selves they are meant to be.[47]

The sections below unpack these concerns: the impact of sharenting on privacy, opportunity, and sense of self. These over-arching concerns manifest in three types of risks: (1) criminal, illegal, or dangerous consequences; (2) legal—but invasive, opaque, and suspect consequences; and (3) identity formation consequences (reputation, sense of self, interpersonal relationships). There are also benefits from sharenting,

---

[42] *See, e.g.*, Nancy Willard, *Complying with Federal Law for Safe Internet Use*, AMERICAN ASSOCIATION OF SCHOOL ADMINISTRATORS, https://www.aasa.org/SchoolAdministratorArticle.aspx?id=10370 (Mar. 23, 2020) (explaining that children are able to get around blocked content and arguing for teaching children responsible Internet use for when they do access content they have been told is off limits).

[43] This is understood as sharenting. *See* PLUNKETT, *supra* note 7, at xv.

[44] This is understood as a youth decision. *See generally* PALFREY & GASSER, *supra* note 21 (documenting the myriad ways that youth make their own digital choices today).

[45] *See supra* note 24 and accompanying text (listing fertility predictive technologies).

[46] For this analysis, "privacy is about self-creation." PLUNKETT, *supra* note 7, at xvi.

[47] Sharenting raises other concerns as well that are beyond the scope of this analysis, including whether parental involvement with screens diminishes their interpersonal interactions with their children and whether parents are setting a poor example for how to engage the world by prioritizing device-time over face-to-face time.

discussed below, following the risk assessment. Both the threats and the upside are offered in encapsulated form to establish the contours of the landscape on which the call for new legislative action is predicated.

B. Criminal, Illegal, or Dangerous Ramifications[48]

Digital transmission of intimate information—including, but not limited to, a child's geographic location, identifying information (full name, date and place of birth, address, and similar details), and preferences (likes, dislikes, hopes, fears)—expose children to the risk of wrongdoing by intended recipients who misuse or abuse the information or by unintended third parties who intercept the information.

These harms include adults in the social media orbit of a parent, grandparent, or other trusted adult who use sharented information to threaten, stalk, abuse, or otherwise engage inappropriately with a child. Perpetrators of child abuse or mistreatment often seek victims whom they know.[49] Sharented information arms these bad actors with intimate information about where and how to seek out children for misconduct. Sometimes, even parents themselves are the bad actors, subjecting their children to abuse or other egregious conduct for sharenting purposes, such as creating a YouTube family prank channel.

Unintended third-party recipients may also acquire and act upon sharented information; notably, many pornographic or abusive images of children online have their origins in real photos that bad actors then manufacture into illicit content. Sharented information can also be used to perpetrate identity theft or fraud against children, as well as to track, stalk, or otherwise act against children based on their location or related information, such as hacking into a digital baby-monitor and talking to a child.

C. Legal—Invasive, Opaque, and Suspect[50]

Once information is sharented, the institutions and individuals who

---

[48] The material set forth in Part I(B) offers a condensed version of the analysis forth in PLUNKETT, *supra* note 7, at 21–25. Where information is set forth that appears in Sharenthood, no additional specific reference is provided beyond this footnote. Where new information is included in this version that did not appear in Sharenthood, a specific reference for that information is provided.

[49] *See, e.g.*, Francis M. Williams, *The Problem of Sexual Assault*, *in* SEX OFFENDER LAWS: FAILED POLICIES, NEW DIRECTIONS *13-49* (Richard G. Wright ed., 2009) (stating that over half of child abuse survivors knew the perpetrators).

[50] The material set forth in Part I(C) offers a condensed version of the analysis forth in PLUNKETT, *supra* note 7, at 25–38. Where information is set forth that appears in Sharenthood, no additional specific reference is provided beyond this footnote. Where new information is included in this version that did not appear in Sharenthood, a specific reference for that

lawfully receive it are subject to relatively few constraints on what they can do with it. The constraints that do exist typically come from criminal or other laws of general applicability, meaning that they are not specific to sharenting or children's digital privacy; for example, parents are bound by child welfare laws when they engage in sharenting, so they cannot engage in abusive or neglectful behavior, film their behavior, post the videos to YouTube, and have the behavior be legally protected by virtue of having been sharented.[51] There are a few specific areas where private information about youth is more protected against transmission, whether it is sharented or coming from youth themselves; notably, as discussed further below, schools represent one specific sector of enhanced youth privacy regulation (although the protections there are not as robust as needed for comprehensive privacy protection).

But most sharenting takes place within a legal framework under which parents, grandparents, educators, and other adults click "I accept" on terms and conditions of use, privacy policies, or other contractual policies from tech providers. Doing so reserves broad, unfettered discretion to the provider and its affiliated third parties over whether, how, why, and to what ends they act upon sharented information. Through this framework, sharented information can travel fast and far, well past the tech company with which the parent is aware they are engaging (like a social media company) and past the people whom the parent understands they are reaching through the tech company (like people in their friend circle). This porous chain leads to a rapid, wide-reaching, and multi-faceted transmission of information.

Here are some of the significant types of ways that tech providers, third parties, and other actors engage with sharented information: to profile children for advertising and marketing purposes; to use children's data for product development purposes;[52] to put information about youth who misbehave or engage in delinquent acts (meaning criminal if done by an adult) into law enforcement databases; to track a family for immigration enforcement action (law enforcement review of social media posts); to engage in predictive decision-making about a child's likely academic progress; to assess a teenager's application to college or other life opportunity where gate-keepers have both discretion and decision-making

information is provided.

[51] *See, e.g.*, PLUNKETT, *supra* note 7, at 63–64.

[52] *See, e.g.*, Kashmir Hill & Aaron Krolik, *How Photos of Your Kids Are Powering Surveillance Technology*, N.Y. TIMES (Oct. 11, 2019), https://www.nytimes.com/interactive/2019/10/11/technology/flickr-facial-recognition.html (explaining how pictures that parents posted of children on social media—sharented content—was used to develop facial recognition products).

authority; to help law enforcement engage in criminal investigations;[53] and to issue public health warnings based on an individual child's experience. These and similar types of behaviors may result in adverse or under-informed actions against or about youth-based on sharented data.

A prominent, yet often under-acknowledged, participant in the sharenting ecosystem is the data-broker industry. This industry, loosely regulated at the federal level (due to a lack of a specific federal law regulating data brokers as well as lax enforcement of existing consumer protection laws), exists to acquire, compile, analyze, and sell private information about people (including youth) to clients who are willing to pay. It is difficult, if not impossible, to obtain transparent, comprehensive data about the type and depth of data that data-brokers have. A study by the Center on Law and Information Policy (CLIP) at Fordham Law School looked at the marketing lists held by over a dozen data-brokers and found information about children as young as two years old in the brokers' holdings.[54] The researchers determined that the information was coming from schools, seemingly from surveys that staff and the students themselves were completing. The lists held by the brokers include names of adolescent girls for family planning services, Jewish kids in the United States, and "funny-looking" kids in the United States. One example of the granularity of the information is that the American Red Cross was able to identify, and then reach-out to, a minor as a strong candidate to be a specific type of blood donor based on data-broker information.

As today's "conceived digital" generation comes of age, it is reasonable to expect that gate-keepers' decisions about the opportunities available to youth will be increasingly data-driven—and that the data used will be increasingly invasive and expansive. Few legal barriers are in place to limit the aggregation, transmission, and action upon sharented information, and there is a trend toward algorithmically mediated outcomes in areas like employment.[55] Thus the market is open for products and services that inform decision-makers who their strongest candidates for employment are, education, certain insurance, and other major life opportunities. While there does not yet appear to be a publicly available "personal capital score" type of product that purports to amass, integrate, and analyze all the sharented information tech companies are able to acquire, the introduction of such an

---

[53] *See* Herold, *supra* note 30.

[54] N. Cameron Russell et al., *Transparency and the Marketplace for Student Data*, CLIP CENTER ON LAW AND INFORMATION POLICY 1–2 (June 6, 2018), https://www.fordham.edu/info/23830/research/10517/transparency_and_the_marketplace_for_student_data.

[55] *See* O'NEILL, *supra* note 38, at 107–08.

offering is not akin to science fiction.[56] Vast amounts of youth personal digital data have been and are being aggregated and put toward predictive ends by different gatekeepers. In the absence of comprehensive federal privacy laws to prevent sharenting, data-driven predictive products likely will continue to be introduced into the marketplace and adopted by decision-makers.

D. Identity Formation Consequences (Reputation, Interpersonal Relationships, Sense of Self)[57]

Even in real life, away from near-future hypothetical scenarios, sharenting can significantly impact the life experiences and opportunities of youth, both while they are young and as they grow up. These impacts strike in the spheres of children's lived experiences. People they meet, or people who hear about them, might form opinions of them based on sharented information. Youth have no legal right to consent (or not) to the sharing of this information—indeed, they might not even have known about the sharing. The most significant hit, however, lands at the core of children's personal experiences: how they come to understand their ostensibly private spaces (like home, school, the playground, and others) as far less private, far more public than they appear. This recognition impacts children's comfort with and ability to play, experiment, and explore without an outside gaze and the legitimate fear of exposure and reactions by others to exposed information, both in present and in the future.

In the brick and mortar era, what children did as children was far more protected than it is now. In the United States, there was no widespread cultural norm of parents posting ads in local newspapers or renting billboard spaces on the highway to tell readers and drivers that their offspring had completed a particular rite of passage, like sleeping through the night or starting their menstrual periods. When a child encountered social difficulties, like a schoolyard bully or cliquish behavior, the adults who got involved likely did so in ways that did not create a widely available written record, like picking up the phone to call another parent. If a child wanted to play pretend or make up dance moves with their friends, there was no AI-assistant with which to interact that would then be acquiring private information, as there would be nowadays.

---

[56] *See* PLUNKETT, *supra* note 7, at 101–02.

[57] The material set forth in Part I(D) offers a condensed version of the analysis forth in PLUNKETT, *supra* note 7, at 38–52. Where information is set forth that appears in Sharenthood, no additional specific reference is provided beyond this footnote. Where new information is included in this version that did not appear in Sharenthood, a specific reference for that information is provided.

In today's digital world, children meet people who already know information about them that the children did not share themselves. These people are able to make assumptions, judgments, and predictions on who children are and who they will become based on just this sharented information. Indeed, this processing of, responding to, and acting upon sharented information can take place without any mediation by digital technology. Once the sharented information is out in the world, it can travel by word of mouth as well as digitally. For instance, the parents of a high school student may find out from a friend who is the social media friend of the parents of their child's prom date that the date has oppositional and defiant tendencies—and judge the date based on that sharented information. Even when an adult who is sharenting information may perceive that information as positive, the child themselves might not see it as positive. Even when the child does see it as positive, the creation of youth identity by parents and other adults, rather than by the youth themselves, does impact the sense of agency and autonomy the child is likely to feel as they come of age and come into their own.

Privacy is essential for play: the space to experiment, to make mischief and mistakes and grow up the better for having made them. Play is essential for identity-formation. Absent spaces that children recognize and respect as private—in fact, not just in label—the "conceived digital" generation is and will continue to be challenged to explore who they are and how they want to be in the world. A perpetual gaze stifles creation, imagination, and learning. Having outsized consequences for mischief or a minor misstep, especially those that endure past a finite point in time,[58] erodes our children's freedom to be present in the moments that mark their lives without the anxiety or erodes the reality that those moments can and will somehow be recorded and used against them down the road.

This reality positions our children to understand themselves as the products of their parents' and other adults' reflections of them, rather than as agents or subjects of their own lives. Of course, the individual and actual experiences of this new reality for individual kids within the conceived digital cohort will vary. This individual variation, however, does not erode the societal transformation of our understanding of childhood and adolescence from protected spaces to tracked spaces.

[58] For instance, imagine a teen whose first day of middle school is marked by printouts of an embarrassing photo of them from their parents' old blog.

E. Benefits[59]

Even as it presents a new threat to the life-stages of childhood and adolescence, as well as to the lived experiences of individual kids and teens, sharenting may also confer some benefits. These benefits may redound to parents, grandparents, and other adults doing the sharenting; to youth being sharented; and to related individual and institutional actors.

Sharenting may foster connections by bridging physical or other distances between family members and friends or by fostering new relationships between those who share interests and affinities which identify and nurture digitally. These interests may arise in social or recreational points of connection. They may also go toward building networks or pursuing goals that transcend entertainment or other forms of enjoyment. For instance, parents raising children with disabilities or serious medical conditions might find both solace and sustenance in connecting with other similarly situated families. Such bonds may be emotional or be goal-directed, including sharing information about medical providers, or organizing to try to reform health care delivery and other essential services.

Sharenting may also foster positive experiences for kids and families that nurture innovation. Think about a family that is passionate about science, for example, and their child's science fair project is a blue-ribbon winner. The proud parents film the invention, put it on YouTube, and the child receives national attention for their innovation. That child has been sharented. People the child does not yet know, and may in fact never know, will form impressions about them. Yet, those impressions are likely to be positive and bring with them the creation of opportunities, such as a scholarship offer to a science camp. While not every child is a budding Einstein, sharenting as a pathway for building positive reputational attributes and constructive opportunities is available in less dramatic forms.

It is rare to eliminate these privacy harms within these and other beneficial paradigms. Rather, they are mitigated or outweighed by the value of the resulting benefit. For a family engaged in sharenting via a Facebook group for families of children with the same disability, the value is great. To these families, the value of finding information about new medical or other care providers, using collective action to impact the services offered in the public-school system, or making other progress toward greater health and well-being is likely to address a more immediate, more acute need than

[59] The material set forth in Part I(E) offers a condensed version of the analysis forth in PLUNKETT, *supra* note 7, at 18–21. Where information is set forth that appears in Sharenthood, no additional specific reference is provided beyond this footnote. Where new information is included in this version that did not appear in Sharenthood, a specific reference for that information is provided.

privacy protection. This is not to reduce sharenting decisions to a purely utilitarian calculus—an "ends justify the means" equation—but to position quotidian sharenting choices as multi-faceted, even as they are made with a swipe of a screen or a click of a mouse.

II. CURRENT FEDERAL LEGAL LANDSCAPE

A. Bedrock Sharenting Legal Framework[60]

Parents enjoy a super-charged, constitutionally protected liberty interest for most of the decisions they make around having and raising children. State law requires parents to provide basic support for their children and to send them to school. It is illegal and, in some instances, criminal for parents to subject their children to abuse or neglect. It is criminal for parents to subject their children to the manufacturing of child pornography. And it is of course illegal or criminal, depending on the underlying legal schema, for parents to violate laws of general applicability in their interactions with their children; for example, a parent could not commit arson against the family home, with children inside, and defend against prosecution because the parent was taking an action related to home and off-spring.

Within these broad parameters, however, parents have wide latitude to direct their children's upbringing. For today's "conceived digital" cohort, this direction includes decisions about whether, why, with whom, how, and when to sharent. For parents, unless the sharenting crosses a legal boundary that is not sharenting specific (like child abuse or child pornography), federal law and almost all state laws leave the sharenting choice to the parents and offer youth no comprehensive, nationwide legal recourse in response to sharenting.

B. COPPA[61]

To focus on federal law, it is important to address the apparent, understandable misperception that exists among some parents based on the

---

[60] The material set forth in Part II(A) offers a condensed version of the analysis forth in PLUNKETT, *supra* note 7, at 77–96. Where information is set forth that appears in Sharenthood, no additional specific reference is provided beyond this footnote. Where new information is included in this version that did not appear in Sharenthood, a specific reference for that information is provided.

[61] The material set forth in Part II(B) offers a condensed version of the analysis forth in PLUNKETT, *supra* note 7, at 87–89. Where information is set forth that appears in Sharenthood, no additional specific reference is provided beyond this footnote. Where new information is included in this version that did not appear in Sharenthood, a specific reference for that information is provided.

law's name that the federal Children's Online Privacy Protection Act (COPPA) and its accompanying Rule apply to all private information about minors transmitted online.[62] COPPA and the Rule only protect personal information collected directly from kids under thirteen. But, even if the age range for COPPA and the Rule were expanded to protect all minors—as lawmakers, regulators, and other stakeholders have recently discussed[63]—limiting privacy protection to personal information that comes directly from kids of any age leaves a vast amount of information about kids unprotected by COPPA. It also reveals that COPPA is built around a flawed premise: that parents can be the strongest protectors of their children's data privacy.

Around the clock, parents, grandparents, educators, baby-sitters, coaches, and other trusted adults are sharing personal information about the children in their care through digital technologies. As described above, these sharenting behaviors include posting about kids on social media, using tracking or surveillance devices on kids, and using digital programs to perform school functions like collecting lunch payments. They include using fertility tracking apps, smart diapers and baby booties, fitness trackers, and software portals to sign-up for summer camp.

COPPA and the Rule do not offer kids of any age comprehensive privacy protections from the adults who share their information in the course of their daily lives, often without realizing they are doing so. There is one key exception that exists at a blurry point along the spectrum of sharenting choices and youth choices: when a school is sharenting by offering or requiring students under thirteen to engage with a digital program from a provider covered by COPPA, the school either needs to get parental consent or meet the criteria for giving substituted parental consent. But COPPA is silent on when an educator is digitally transmitting children's personal information themselves, such as by using an app to track attendance, rather than putting a digital program in children's hands.

There are also online providers that COPPA does not regulate, even when a child under thirteen is engaging with that provider. COPPA and the Rule are limited to commercial online providers whose services target kids under thirteen or who know that kids under thirteen use their services. Non-commercial providers, such as non-profit corporations, are excluded from coverage, as are providers who offer general online services and do not

---

62 The existence of this misperception has been found by researchers doing qualitative focus-groups with families around privacy. Phone conversation between the author and Dr. Monica Bulger (winter 2020).

63 *See* Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, 84 Fed. Reg. 35842, 35846 (proposed July 25, 2019).

actually know that kids under thirteen use their products. As long as COPPA and the Rule have any sort of carve-outs for certain types of online providers, tech companies will have the incentive and ability to structure their activities to avoid being subject to COPPA.

Even when covered by COPPA, it is difficult, if not impossible, for parents to navigate the privacy policies, terms of use, and other information supplied by tech providers. With few exceptions, parental consent is the main requirement under COPPA for whether or not an online service provider can collect personal information directly from kids under thirteen.

C. Notice & Consent[64]

Parents are entrusted to be their children's digital privacy gatekeepers. However, parents often accept a company's policies and terms without being able to think through what a provider will be doing with their children's personal information. Policies, terms, and related content can be difficult even to find, especially for smart devices where a user might need to look at a package insert or on an app or website. Once located, this content is dense, complex, and typically retains significant loopholes for providers to take unspecified actions to improve products or share information with third parties that are providing product support or fulfilling another function. Thus, even parents who locate and read the relevant information are unlikely to understand the full extent of the activities which the company is asking for parental consent to engage in.

This superficial "notice and consent" construct forms the legal basis for all sharenting, not just the sharenting decisions that involve youth interaction with a COPPA-covered digital technology.[65] Whenever a parent uses a digital device or service for themselves without giving any use to their child as well, the general legal authority the tech provider has to collect, transmit, aggregate, or otherwise act upon the data is grounded in a manifestation of consent that the parent has already given. These contracts—sometimes called "click-wrap" or "click through"—are of dubious value given the information and bargaining asymmetries between the parties.[66] Yet, those are the legal underpinnings upon which parents transmit ultrasound pictures, birth announcements, video footage of a nursery, location data, and so much

[64] The material set forth in Part II(C) offers a condensed version of the analysis forth in PLUNKETT, *supra* note 7, at 79–83. Where information is set forth that appears in Sharenthood, no additional specific reference is provided beyond this footnote. Where new information is included in this version that did not appear in Sharenthood, a specific reference for that information is provided.

[65] For instance, this could happen with a parent giving a toddler an iPad then clicking "accept" for apps that the toddler is using.

[66] *See generally* Lewis, *supra* note 41.

more.

Adults other than parents—grandparents, aunts, uncles, baby-sitters, friends, coaches, teachers, and others—are also establishing these contracts that then serve as the basis for their sharenting. For non-parent adults, there are some professional roles in which federal and state laws (that do not apply to parents) apply. Education, a key area in which this occurs, is discussed further below. For sharenting by non-parents where no sector specific federal or state law applies, the notice and consent framework controls as between the adult doing the sharenting and the tech provider.

To the extent that any legal framework is relied upon to control the relationship between the non-parent engaged in sharenting, the child whose information is being sharented, and the parents of that child, it tends to be some form of notice and consent. Realistically, within close personal relationships like grandparents or friends, norms, or customs rather than contracts tends to govern. For more arm's length relationships like a coach or camp counselor, the best practice is to have a contract in place between the parent and the non-parent adult in which the parent authorizes the sharenting.[67] Absent such permission, the non-parent engaged in the sharenting runs the risk of garnering parental ire or providing the basis for a legitimate parental legal grievance for publicizing or transmitting information about a minor child without any authority to do so; for example, Facebook offers parents the ability to request removal of pictures posted of their children (if under the age of thirteen).[68] A child typically cannot give consent to information sharing about themselves outside of limited circumstances like certain types of medical treatment or, as of January 2020 in California, specific types of digital information sharing.[69] In some states, recording audio or video of a person without consent is a criminal act, rendering of heightened import compliance with consent requirements for activities covered by the criminal code.[70]

---

[67] *See generally* Leah A. Plunkett, *Summer in Cyberspace: Protecting Your Kids' Digital Privacy at Camp*, FERPA SHERPA (July 2017), https://ferpasherpa.org/plunkett1/.

[68] *See, e.g.*, Facebook, "*Photos or Videos That Violate Your Privacy*," FACEBOOK (last visited Apr. 15, 2020) (explaining process for parent to request removal of photo of child under 13).

[69] *See* CCPA Fact Sheet, California Attorney General (Winter 2019), https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf (explaining opt-in rights for personal information held by children ages 13–16).

[70] In New Hampshire, where I live and teach, this is a felony. N.H. Rev. Stat. § 570-A:2(I). *See also* Todd Feathers, *Do Ring Cameras Violate Wiretapping Laws? New Hampshire Is About To Find Out*, VICE (Jan. 30, 2020), https://www.vice.com/en_us/article/3a8k79/do-ring-cameras-violate-wiretapping-laws-new-hampshire-is-about-to-find-out.

D. FERPA[71]

In at least one state (Louisiana), violations of state student privacy law carry specific criminal penalties. While this heavy-handed approach to student privacy is an outlier, education is the sector specific area where non-parent professionals are subject to the most robust federal privacy law scheme focused on minors. The federal Family Educational Rights and Privacy Act (FERPA) applies to primary and secondary schools that receive federal funding.[72] Under FERPA, educators need parental consent to share "personally identifiable information" (PII) from "education records"—unless an exception applies.

The two exceptions to parental consent that tend to facilitate sharenting are the "directory exception" and the "legitimate school official exception." Through these avenues, parental consent can be bypassed in favor of an educator's decision to transmit PII to a third-party tech company in the course of providing classroom, extracurricular, office, or other education-related services. The avenues differ in scope of the information that can be provided. The "directory exception" permits a narrower scope of information to be released, allowing educators to share basic identification information, such as name, address, and class year (unless a parent has opted out of having their child's information included in these directory transmissions). The "legitimate school official exception" makes a broader swath of PII available for transmission—provided that certain criteria are met. Under this exception, the types of PI transmitted are not limited. To be valid, however, the PII must be shared with a third-party that is providing a service that would otherwise be done in house, is operating under the control of the educational institution, and is not re-sharing the information.

Effectuating proper use of the legitimate school official exception requires a directly negotiated contract (rather than a click-wrap), the use of template contractual terms that incorporate relevant FERPA and state student privacy law, or a similar approach that ensures the requirements for reliance on this exception are met. Despite schools' best efforts, it may prove challenging to implement this exception according to the letter of the law. Proper implementation is achieved best with multi-stakeholder review and input, including expertise from technologists and lawyers as well as

[71] The material set forth in Part II(D) offers a condensed version of the analysis forth in PLUNKETT, *supra* note 7, at 81–83. Where information is set forth that appears in Sharenthood, no additional specific reference is provided beyond this footnote. Where new information is included in this version that did not appear in Sharenthood, a specific reference for that information is provided.

[72] 20 U.S.C. § 1232g(b); 34 C.F.R. §§ 99.1 *et seq.*

educators.[73] Assembling that type of team structure may be beyond the financial resources or bandwidth of a school system. The legal alternative—asking for parental consent—is unlikely to better protect children due to the challenges or failures of parents as privacy gatekeepers when accepting notice and consent terms. When students are in well-resourced, privacy-savvy school systems, they may enjoy more robust privacy protection in school than at home.[74] However, for those students in different circumstances, the depth and breadth of digital tech used in schools can compound privacy concerns when there are two layers of gatekeepers—the school with the parents in the background—without the tools necessary to consistently and effectively protect youth privacy.

E. PPRA[75]

There is an often-overlooked step-cousin to COPPA and FERPA: the Protection of Pupil Rights Act and Amendment (PPRA).[76] Under this federal law, schools that are administering certain types of survey instruments need to obtain parental consent when the instrument requires students to share certain types of sensitive personal information (PI), such as information about sexuality, religion, or similar topics.[77] PPRA also requires that parents be able to opt-out their children from PI collection that will be used to market to them.

PPRA is poorly drafted and poorly understood. In theory, it should have applicability to many more types of digital educational technology than those to which schools actually seem to apply it. For example, if a school is using software to teach social-emotional learning (involving questions around sexuality and psychology, for instance), then the school should

---

[73] *See* Leah Plunkett, Alicia Solow-Niederman, & Urs Gasser, *Framing the Law & Policy Picture: A Snapshot of K-12 Cloud-Based Ed Tech & Student Privacy in Early 2014*, BERKMAN KLEIN CENTER FOR INTERNET & SOCIETY 24 (June 2014), https://cyber.harvard.edu/publications/2014/law_and_policy_snapshot.

[74] To see top-flight privacy-protecting contractual resources for use in K-12 schools, please visit the Student Data Privacy Consortium at https://privacy.a4l.org/.

[75] The material set forth in Part II(E) offers a condensed version of the analysis forth in PLUNKETT, *supra* note 7, at 83. Where information is set forth that appears in Sharenthood, no additional specific reference is provided beyond this footnote. Where new information is included in this version that did not appear in Sharenthood, a specific reference for that information is provided.

[76] 20 U.S.C. § 1232h; 34 C.F.R. § 98.

[77] *See* Dalia Topelson Ritvo, *Privacy and Student Data: An Overview of Federal Laws Impacting Student Information Collected Through Networked Technologies* 16–17, CYBERLAW CLINIC (June 2016), https://dash.harvard.edu/handle/1/27410234.

follow PPRA in addition to COPPA[78] and FERPA.[79] Absent PPRA being followed, under federal student privacy laws, a school lawfully could have children under thirteen take a survey about sensitive topics, offered by a for-profit software company, without getting parental consent at any point, provided the legitimate school official exception under FERPA and the substituted parental consent path under COPPA are followed.

If adhered to, PPRA also provides an additional safeguard on marketing based on PI. Neither FERPA's legitimate school exception or COPPA's substituted consent should permit marketing based on personally identifiable information (FERPA) or personal information (COPPA); both avenues require that the third-party recipient of information use it as specified and not re-share it (FERPA) or only use it for purposes directly related to the school (COPPA). Loopholes remain, however, such as an education tech tool from a non-profit company into which a student over thirteen directly inputs personal information. FERPA does not control here because the student is inputting the information, rather than a school official. COPPA does not apply either since it is a non-profit tech company and the student is over thirteen years old.[80]

Despite the greater level of protection that more consistent and comprehensive PPRA adherence would provide, this benefit would accrue to a limited group of sharenting permutations: those occurring from the decisions of educators (not parents, grandparents, or other trusted adults) to use a certain sub-set of ed tech offerings in a defined set of ways.

F. Non-Federal Privacy Innovation

In the last few years, legislatures other than the U.S. Congress have made progress on comprehensive data privacy legislation for both minors and adults. Notably, the European Union (EU) implemented the General Data Privacy Regulation (GDPR) in May 2018 and California implemented its Consumer Privacy Act (CCPA) in January 2020.[81] Both GDPR and CCPA have population limitations: EU subjects and California consumers,

---

[78] COPPA compliance would be required if the software provider is for-profit and getting personal information directly from students under thirteen. *See supra* Part II(B) (explaining COPPA).

[79] FERPA compliance would be required if school officials themselves are inputting PII about students. *See supra* Part II(D) (explaining FERPA).

[80] *See generally* Ritvo, *supra* note 77, at 12 (comparing key coverage and terms of each of the big three federal student privacy laws).

[81] *See generally General Data Protection Regulation (GDPR)*, REGULATION EU 2016/679, https://gdpr-info.eu; California Consumer Privacy Act (CCPA), Title 1.81.5, https://oag.ca.gov/privacy/ccpa.

respectively.[82] Despite these restrictions, both are groundbreaking in terms of establishing key components that should undergird any new federal privacy law: the need for specific, informed, opt-in individual permissions around data sharing, the need for data use limitations, and the need for specific forms of removal.[83] While there has been a fair amount of federal legislative energy paid to privacy in recent years, lawmakers have not to date coalesced around a path forward.[84] By starting with children's privacy, PPLAY would address ongoing harms and ideally establish a foothold for crucial forward-looking privacy protections (along the lines of GDPR and CCPA) that could be developed further to include adults.

III. PPLAY

A. Why PPLAY?

Establishing robust, comprehensive federal data privacy protection for children requires consideration of the different roles, capacities, and existing legal constructions of the key stakeholders. Two overarching commitments emerge. For individual actors who have relationships to children (including both personal relationships, like parents, and professional relationships, such as educators), the priority is to empower them with accessible tools for personal decision-making. For institutional actors (chiefly tech companies), the priority is to establish and enforce firm limits on the activities in which they can engage with children's personal data. The new federal law proposed below looks to further both commitments.

This new federal law, Protecting the Private Lives of Adolescents and Youth (PPLAY), would have four main components. First, it would require a nutrition-style labeling system for digital technology products or services. This system would set out essential privacy and data collection information in clear, standardized terms to foster informed consumer decision-making. Second, it would create a lifelong prohibition on tech companies or other entities using all private digital data collected from any source about children under eighteen for targeted advertising or marketing to those children (as minors or adults). Third, PPLAY would place the same prohibition for any use of this data by key gatekeepers to determine access to major life opportunities. Fourth, it would require social media platforms to set up a

---

82 *Id.*

83 *Id.*

84 *See, e.g.*, Roger Ford, *With Digital Privacy Law, Don't Repeat Mistakes of the Past*, THE HILL (March 5, 2019), https://thehill.com/opinion/technology/432628-with-digital-privacy-law-dont-repeat-mistakes-of-the-past (arguing that federal government should continue to allow states to innovate around privacy even as it contemplates new national-level regulation).

removal review process for sharented content.

To enforce PPLAY, there would be rights of data access and review, rights of removal, and a private right of action (with meaningful financial penalties and attorney fee provisions) for children against digital tech providers who violate their rights under PPLAY.

B. Labeling System

It is reasonable to maintain parents, grandparents, teachers, and other trusted adults in children's lives on the front lines of deciding which tech devices or services belong in a home, school, or other environment. Re-configuring this decision-making process would threaten unnecessarily fundamental commitments to free consumer markets, as well as to protected spheres of personal or professional responsibility.

There is a structural imbalance, however, between the information that digital tech devices and service providers have, and the information held by parents, educators, and other users. As discussed above, it is difficult, if not impossible, for end users of digital tech to have complete and accurate notice upon which to give meaningful consent for data collection and use.

To move toward remedying this imbalance, PPLAY would require a nutrition-label style system of data collection and data privacy practices for all digital tech products and services used in inter-state commerce. This label would be analogous to food labels which let the consumer know, prior to purchase, the food's composition with respect to key categories of consumer health and wellness.[85]

The data labeling scheme would cover three main areas: the types of data collected, the categories of data use, and the parties the data is shared with. Although this scheme would still require consumer engagement and likely additional education around the meaning and value of the information conveyed, the information would become standardized and more readily accessible. This shift represents an essential step forward in empowering individual decision-makers in their consumer purchasing and use.

C. Prohibitions

Even with greater empowerment, parents, teachers, and other trusted adults are not well-positioned to ensure that sharented content will not succumb to commercial targeting of children or to shape or restrict their current and future life opportunities. The degree of commercial sophistication of individual adults varies greatly, with some being more

[85] *See* Plunkett et al., *supra* note 73, at 19–21 (exploring the nutrition label concept for educational technologies specifically).

sophisticated than others.[86] In addition, adults have different levels of commitment to protecting children's privacy and opportunity.[87] Respect does need to be maintained for parents' and other trusted adults' ability to establish what they believe to be the optimal digital privacy conditions for the children in their care. This agency should not become a justification for eroding children's privacy or opportunity.

To preserve childhood and adolescence as protected spaces to play—to make mischief, make mistakes, and develop agency and autonomy—it is crucial to establish limits on the uses to which children's private information can be put, either when they are still minors or when they have attained the age of majority. As discussed above, absent such protections, children are likely to experience constraints in how they inhabit ostensibly protected spaces (most notably home and school), either in the moment or once they have occasion to realize what information was taken from them. They are also likely to face limitations or barriers on their current or future life opportunities as sharented information is used by individuals or institutions to judge them—to make predictions or real-time decisions about them—in ways that they do not know and over which they lack legal control.

Giving minors a legal right to determine whether their parent, teacher, or other trusted adult can sharent information about them would lead to unworkable complexities. It is thus most efficient and most fair in terms of protection for all children nationwide to set the same baseline standard of non-consent for tech companies and other actors to use sharented information[88] or any other information collected about them as children for targeted advertising or marketing as well as for decision-making.[89]

Under PPLAY, even once children turn eighteen, the private data collected about them as children could not be used to target them with advertising or marketing, although information collected from them after they become adults could be used for marketing and advertising.

The same lifelong prohibition would apply to the use of private data to make predictions or decisions about children's opportunities (whether as

---

[86] *But see* Lewis, *supra* note 41 (arguing that adults as a whole lack the ability to meaningfully negotiate and enter into complex consumer contracts today).

[87] *See, e.g.*, C.S. Mott Children's Hospital National Poll on Children's Health, *Parents on Social Media: Likes and Dislikes of Sharenting*, vol. 23, issue 2, U. OF MICHIGAN HEALTH SYSTEM (Mar. 16, 2015), https://mottpoll.org/sites/default/files/documents/031615_sharenting_0.pdf (noting that 74% of poll respondents said that they knew of another parent who over-sharented).

[88] The types of information protected under PPLAY would track the definition of "personal information" in CCPA. *See* 1.81.5 CA. CIV. CODE, § 1798.140(o)(1) (2020).

[89] To limit this prohibition to sharented content only risks being unwieldy, as data source would need to be determined, and also would leave open a privacy protection gap where COPPA currently fails to protect.

minors or as adults) to gain access to major life activities, defined to include education, employment, health care, life insurance, health insurance, and similar opportunities.

If another law or regulation permits a particular use of the data, or if the child's parent (if the child is under sixteen) or the child themselves (if over sixteen) has specifically opted in the child for the use, then that limited use would be allowed under PPLAY.

Taken together, the terms of these prohibitions aim to establish a solid protective zone of digital data privacy for childhood and adolescence, while still allowing reasonable space for informed parental or youth opt-in to specific uses of their data for marketing or decision-making that they deem to be beneficial.

D. Removal

The labeling and prohibition components of PPLAY address tech use by adults and data use by tech providers and other third parties. They do not offer any recourse for children embarrassed, ashamed, or otherwise made uncomfortable by social media posts created by their parents, grandparents, or other adults.[90] To put it another way, they do not address the way that unwelcome content may be maintained online and viewed. Without addressing content maintenance and viewing, PPLAY would protect a child from having a college rely on analytics from their parents' embarrassing social media posts about them in an admissions decision, but would not protect the child from the posts' continued presence online such that their college roommates could view the material and form opinions about them based on it.

The balance in this domain is particularly complex. Parents, teachers, and other adults enjoy freedom of expression, both to the extent that certain free expression could be grounded in constitutional protections (especially for parents)[91] and because the default user experience across social media platforms is unfettered exchange. However, children (both as minors and upon attaining the age of majority) may experience significant distress or face interpersonal or reputational ramification as a result.

To balance adult free expression and child privacy protection, PPLAY would create a right to erasure for adult posts if that content created sharented infliction of emotional distress[92] and was unprotected by another source of

[90] This prohibition under PPLAY could be extended to content minors share about themselves or other minors.

[91] *See* PLUNKETT, *supra* note 7, at 113–15.

[92] *See generally* STUART M. SPEISER ET AL., THE AMERICAN LAW OF TORTS § II(16)(C)(1) (defining negligent infliction of emotional distress). The statutory term under

law or by a compelling adult interest. PPLAY would require that social media companies operating in interstate commerce include this right in their terms of service and display it prominently on the site, in addition to the terms of service, such that the adult user would have notice that this type of content could be subject to removal if it inflicted emotional distress.[93] Children subjected to the sharented content (ages thirteen and above, including after attaining the age of majority) would have a right to request erasure from the social media company for seven years after they knew or should have known about the content. Children under the age of thirteen would need to make the request through a "next friend," which could be a parent, grandparent, educator, other trusted adult, or a neutral, professionally qualified adult. Social media companies would be required to assign this neutral party to support removal requests from youth under the age of thirteen that came into the company without a next friend attached.

The company would be required to review and respond to sharenting removal requests in a reasonable period of time using trained, impartial professional staff (PPLAY would not specify if that staff would need to be human or whether it could be AI).[94] The first layer of inquiry would be whether or not the sharented content inflicted emotional distress that would be reasonable for a youth, young adult, or adult to experience as a result of the content, given the totality of the circumstances. The second layer would be a determination of whether another law permitted the content, such as constitutional free speech protections for posts involving religion, in which case no take-down could occur. The third layer would be a determination of whether a compelling interest—including such factors as business purpose—exists separate from another area of law that would tip the balance toward retaining the content. The PPLAY statute will broadly establish the factors giving rise to a compelling interest, including the mode of implementation, through the rule-making process.

E. Enforcement

In order to ensure compliance by tech companies, PPLAY would give children a right to access their digital records when they turn thirteen or

PPLAY would have its own definition, not be beholden to the general one.

[93] For previously sharented content, where the adult user would have lacked notice of this type of potential for take-down at the time of posting, the new provision would still be legally acceptable because of the catch-all language in click-wrap agreements that allows for updates to terms. For adults who have relied heavily on sharenting for a business interest, for example, that might be able to qualify as a "compelling interest" under PPLAY that would tip the balance against removal.

[94] Regulatory oversight would rest with the Federal Trade Commission (FTC), which already oversees COPPA.

through a parent or other next friend while they are under sixteen. There would be grounds for requesting removal or correction of digital data or for requesting an opt-in by the parent or digital guardian before a child is thirteen or by the child once they are thirteen—asking that the data be shared with tech companies, data brokers, schools, employers, or other gate-keepers for a specific reason. These rights would be enforceable through a private right of action so that a child could bring a lawsuit against a company directly, either through their parent, next friend if a minor, or in their own right if aged eighteen or over.

The penalties for violations would need to be set high enough to serve as an actual deterrent for PPLAY violations; the CCPA offers a starting point but would likely need revision to be effective. PPLAY would also include fee-shifting statutes to compensate successful attorneys for becoming private attorneys general.

IV. CONCLUSION

PPLAY offers a blueprint for striking a workable balance between preserving parent, grandparent, educator, and other adult autonomy while establishing comprehensive privacy and life opportunity protections for youth in the care of these adults. The implementing regulations would require multi-stakeholder input—or, to put it colloquially, be played around with—in order to precisely calibrate the balance between open online engagement, locked down privacy, and open future prospects for youth to figure out for themselves who they are meant to be.