Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 32 | Number 1 Article 1

2021

Algorithmic Parenting

Eldar Haber

Tammy Harel Ben Shahar

Algorithmic Parenting

Cover Page Footnote

* Associate Professor, Faculty of law, University of Haifa; Faculty member, Center for Cyber, Law and Policy (CCLP) and Haifa Center for Law and Technology (HCLT), Faculty of law, University of Haifa. We are grateful to Gabriel Focshaner, Naama Shiran and Tal Tamches for their excellent assistance in research. This research was supported by a grant from the German-Israeli Foundation for Scientific Research and Development. ** Senior Lecturer, Faculty of law, University of Haifa; Academic Director of Haifa Legal Clinics.

Algorithmic Parenting

Eldar Haber* and Tammy Harel Ben Shahar**

Growing up in today's world involves an increasing amount of interaction with technology. The rise in availability, accessibility, and use of the internet, along with social norms that encourage internet connection, make it nearly impossible for children to avoid online engagement. The internet undoubtedly benefits children socially and academically and mastering technological tools at a young age is indispensable for opening doors to valuable opportunities. However, the internet is risky for children in myriad ways. Parents and lawmakers are especially concerned with the tension between important advantages and risks technology bestows on children.

New technological developments in artificial intelligence are beginning to alter the ways parents might choose to safeguard their children from online risks. Recently, emerging AI-based devices and services can automatically detect when a child's online behavior indicates that their well-being might be compromised or when they are engaging in inappropriate online communication. This technology can notify parents or immediately block harmful content in extreme cases. Referred to as algorithmic parenting in this Article, this new form of parental control has the potential to cheaply and effectively protect children against digital harms. If designed properly, algorithmic parenting would also ensure children's liberties by

* Associate Professor, Faculty of law, University of Haifa; Faculty member, Center for Cyber, Law and Policy (CCLP) and Haifa Center for Law and Technology (HCLT), Faculty of law, University of Haifa. We are grateful to Gabriel Focshaner, Naama Shiran and Tal Tamches for their excellent assistance in research. This research was supported by a grant from the German-Israeli Foundation for Scientific Research and Development.

** Senior Lecturer, Faculty of law, University of Haifa; Academic Director of Haifa Legal Clinics.

neither excessively infringing their privacy nor limiting their freedom of speech and access to information.

This Article offers a balanced solution to the parenting dilemma that allows parents and children to maintain a relationship grounded in trust and respect, while simultaneously providing a safety net in extreme cases of risk. In doing so, it addresses the following questions: What laws should govern platforms with respect to algorithms and data aggregation? Who, if anyone, should be liable when risky behavior goes undetected? Perhaps most fundamentally, relative to the physical world, do parents have a duty to protect their children from online harm? Finally, assuming that algorithmic parenting is a beneficial measure for protecting children from online risks, should legislators and policymakers use laws and regulations to encourage or even mandate the use of such algorithms to protect children? This Article offers a taxonomy of current online threats to children, an examination of the potential shift toward algorithmic parenting, and a regulatory toolkit to guide policymakers in making such a transition.

INTRODUCTION

Growing up in today's world involves an increasing amount of interaction with technology. The rise in availability, accessibility,

and use of the internet, along with social norms that encourage internet connection, makes it nearly impossible for children to avoid online engagement. The internet undoubtedly benefits children socially and academically, and mastering technological tools at a young age is indispensable for opening doors to valuable opportunities. However, the internet is risky for children in myriad ways.[1] Parents, educators, and policymakers worry that children will be exposed to sexual, violent, or other inappropriate content, or harassed, bullied, or otherwise harmed. Even absent foul play, internet and social media use may create risks for children and teens, such as addiction, a higher tendency toward anxiety and depression, the development of eating disorders, and even suicide.[2]

Parents and lawmakers are especially concerned with the tension between important advantages and risks technology bestows on children. As a vulnerable population, children are afforded many forms of legal protections, both internationally and domestically.[3] Parents are tasked with providing children their basic needs (e.g., food, clothing, housing, medical care, and education) and protecting them from physical and mental harm.[4] In some instances, the state directly regulates the protection of children from unnecessary harm, such as compulsory childhood vaccination laws, abuse-reporting statutes, and the provision of specific shelters.[5] However, other than failed regulatory attempts to reduce exposure to indecent websites,[6] policymakers have focused their attention on protecting the privacy or, more accurately, preventing datafication of children. The American regulatory framework under the Children's Online Privacy

---

1 *See infra* Part I.

2 *Id.* Notably, this Article generally uses the term *children* in reference to a variety of minors, from early childhood (ages three to five) to late adolescence (ages sixteen to eighteen). The differences between age groups will be discussed throughout the Article as necessary.

3 *See infra* Part II.A.

4 *See infra* Part I.

5 *See* Vincent R. Johnson & Claire G. Hargrove, *The Tort Duty of Parents to Protect Minor Children*, 51 VILL. L. REV. 311, 324 (2006) (listing legislation that protects children from harm); Steve P. Calandrillo, *Vanishing Vaccinations: Why Are So Many Americans Opting Out of Vaccinating Their Children?*, 37 U. MICH. J.L. REFORM 353, 381–82 (2004) (discussing compulsory vaccination laws); BRIAN H. BIX, THE OXFORD INTRODUCTIONS TO U.S. LAW: FAMILY LAW 110–17 (2013).

6 *See infra* Part II.A.

Protection Act ("COPPA") requires companies to provide adequate data collection procedures, retention practices, and information accessibility and security, thereby allegedly securing both parents' and children's privacy interests.[7]

While important, privacy is merely one aspect in which children require protection. In addition to advising children how to properly navigate the digital world, many parents opt for more concrete forms of protection against online risks. Today, the options most available to parents involve filtering software and limitations on screen time through either software or house rules.[8] Some parents engage in full parental monitoring—constantly surveilling their children's online engagement.[9] The array of choices and day-to-day implementations create a perpetual dilemma for parents regarding the scope of their children's autonomy with respect to online activity. Further, parents are tasked with the challenging choices of when and how to intervene in their children's online activity to promote their well-being and protect them from harm.

New technological developments in artificial intelligence ("AI") are beginning to alter the ways parents might choose to safeguard their children from online risks. Recently, emerging AI-based devices and services can automatically detect when a child's online behavior indicates that their well-being might be compromised or when they are engaging in inappropriate online communication.[10] This technology can notify parents or immediately block harmful content in extreme cases.[11]

Referred to as *algorithmic parenting* in this Article,[12] this new form of parental control has the potential to cheaply and effectively protect children against digital harms. If designed properly, algorithmic parenting would also ensure children's liberties by neither excessively infringing their privacy nor limiting their freedom of speech and access to information. This Article offers a balanced solution to the aforementioned parenting dilemma that allows parents

---

7 *See* Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506.
8 *See infra* note 137 and accompanying text.
9 *See infra* note 145-50 and accompanying text.
10 *See infra* note 144 and accompanying text.
11 *Id*.
12 *See infra* Part III.

and children to maintain a relationship grounded in trust and respect, while simultaneously providing a safety net in extreme cases of risk.[13] For children who lack meaningful relationships with their parents or caregivers, algorithms can at least protect against acute risks by blocking explicit sexual content or alerting parents to content that may suggest the child is contemplating self-harm.[14]

Despite this appeal, algorithmic parenting poses several challenges that must be discussed and analyzed. In addition to certain practical complications (e.g., ensuring children do not bypass the system and detecting implicitly risky behavior), algorithmic parenting must overcome several legal hurdles before such measures can be implemented. First, algorithmic parenting retains comprehensive amounts of children's data, which must be secured. While regulations can somewhat allay this fear, other questions regarding the implementation of algorithmic parenting remain unanswered: What laws should govern platforms with respect to algorithms and data aggregation? Who, if anyone, should be liable when risky behavior goes undetected? Perhaps most fundamentally, relative to the physical world, do parents have a duty to protect their children from online harm? Finally, assuming that algorithmic parenting is a beneficial measure for protecting children from online risks, should legislators and policymakers use laws and regulations to encourage or even mandate the use of such algorithms to protect children?

This Article offers a taxonomy of current online threats to children, an examination of the potential shift toward algorithmic parenting, and a regulatory toolkit to guide policymakers in making such a transition. The Article proceeds as follows: Part I introduces and discusses the risks and harms that children face today on the internet. Part II examines potential modalities for regulating children's protection online. It first discusses the legal regime currently governing children's online protection and its limitations. Then, it turns to non-legal modalities, namely social norms, the market, and technology, and scrutinizes how parents use technology to monitor children. Part III describes and evaluates a potential transition toward algorithmic parenting. After discussing the benefits and

---

13 *See infra* Part III.

14 *See infra* Part III.

drawbacks of algorithmic parenting, Part III then addresses the state's role and the legal interventions policymakers must consider in light of potential drawbacks and effects on children's rights. Finally, Part IV summarizes the discussion and stresses that, despite this Article's endorsement of algorithmic parenting for protecting children online, algorithmic parenting should never replace open communication between parents and children.

I. CHILDREN'S SAFETY ONLINE

Children are a vulnerable population in need of special care, assistance, and protection. While children's capacities evolve as they gradually gain autonomy over their lives, protecting children from harm and making decisions on their behalf are two of the most fundamental goals of parenting.[15]

The online world is an especially challenging arena for parents to help navigate children's growth and oversee their safety. The digital world greatly influences children's lives.[16] Children vary, of course, but connecting to the internet often begins at a very young age,[17] first as passive consumers of online content and then becoming more active as they grow. Teens are often fully integrated online participants, consuming content independently, using search engines, playing games, communicating with others, participating in

---

[15] *See* Danielle J. Garber, *COPPA: Protecting Children's Personal Information on the Internet*, 10 J.L. & POL'Y 129, 132 (2001); Dorothy A. Hertzel, Note, *Don't Talk to Strangers: An Analysis of Government and Industry Efforts to Protect a Child's Privacy Online*, 52 FED. COMMC'NS L.J. 429, 434 (2000); Eldar Haber, *Toying with Privacy: Regulating the Internet of Toys*, 80 OHIO ST. L.J. 399, 411 (2019). For the principle of the child's evolving capacities, see generally Daniel P. Keeting, *The Evolving Capacities of the Child*, *in* HANDBOOK OF CHILDREN'S RIGHTS: GLOBAL AND MULTIDISCIPLINARY PERSPECTIVES 184 (Martin D. Ruck et al. eds., 2017).

[16] *See, e.g.*, Jennifer Bremer, *The Internet and Children: Advantages and Disadvantages*, 14 CHILD & ADOLESCENT PSYCHIATRIC CLINICS OF N. AM. 405, 411–18 (2005); Martin Valcke et al., *Internet Parenting Styles and the Impact on Internet Use of Primary School Children*, 55 COMPUTS. & EDUC. 454, 454 (2010).

[17] *See* DONELL HOLLOWAY ET AL., ZERO TO EIGHT: YOUNG CHILDREN AND THEIR INTERNET USE 4 (2013); Antigone Davis, *Hard Questions: So Your Kids Are Online, But Will They Be Alright?*, FACEBOOK (Dec. 4, 2017), https://about.fb.com/news/2017/12/hard-questions-kids-online/ [https://perma.cc/NY4F-SJQD].

multiple social media networks,[18] and uploading original content.[19] Given the increased introduction of technology at school, online activity is a necessary component of everyday learning.[20]

While children have always been exposed to hazards and risks, the internet dramatically exacerbates the potential for harm.[21] Parents and regulators who are not digital natives must be aware of these new risks and challenges and understand how to appropriately address them.[22] For example, one such danger involves data-mining children's viewing habits and using the data for marketing purposes.[23] Another threat is potential exposure to harmful content, such as violent, hateful, commercial, or sexual content.[24] Unfortunately, legislators' attempts to address these concerns and protect children's privacy in the face of such practices have proven ineffective.[25]

From a safety and protection perspective, the gravest risks likely arise when children transition from passive to active online users.[26] Depending on their level of activity and participation online,[27]

---

[18] *See* HOLLY BENTLEY ET AL., NAT'L SOC'Y FOR THE PREVENTION OF CRUELTY TO CHILD., HOW SAFE ARE OUR CHILDREN? 3 (2019) (finding that ninety percent of eleven to sixteen-year-olds surveyed in the UK say they have a social media account).

[19] *See generally* Sonia Livingstone, *Maximising Opportunities and Minimising Risks for Children Online: From Evidence to Policy*, 37 INTERMEDIA 50 (2009) (outlining six tenants to internet safety for children with corresponding policy guidelines).

[20] *See* Yoni Har Carmel & Tammy Harel Ben-Shahar, *Reshaping Ability Grouping Through Big Data*, 20 VAND. J. ENT. & TECH. L. 87, 103–04 (2017).

[21] *See* JOHN PALFREY ET AL., BERKMAN CTR. FOR INTERNET & SOC'Y, ENHANCING CHILD SAFETY AND ONLINE TECHNOLOGIES: FINAL REPORT OF THE INTERNET SAFETY TECHNICAL TASK FORCE 7 (2008); Sonia Livingstone & Ellen J. Helsper, *Parental Mediation of Children's Internet Use*, 52 J. BROAD. & ELEC. MEDIA 581, 584 (2008).

[22] For a comparison between digital "natives" and digital "immigrants," see generally JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES (2008).

[23] *See infra* Part II.A. (addressing the regulation of children's online data further).

[24] *See* Leslie Haddon, *Parental Mediation of Internet Use: Evaluating Family Relationships*, *in* GENERATIONAL USE OF NEW MEDIA 13, 15 tbl.1.1 (Eugène Loos et al. eds., 2012).

[25] *See infra* Part II.A.

[26] Passive use includes consuming content—usually audiovisual content. For young children, parents or other caregivers direct this use. Active use involves a wide range of activity, including interaction with others and uploading content.

[27] *See, e.g.*, Seth Safier, *Between Big Brother and the Bottom Line: Privacy in Cyberspace*, 5 VA. J.L. & TECH. 6, paras. 59–64 (2000); *see also* Garber, *supra* note 15, at

children begin to experience solicitation,[28] harassment,[29] and bullying[30] and are exposed to more obscene,[31] violent,[32] and illegal content.[33] This easily accessible, online information can vitally influence a child's development and education. However, with thousands

---

140–45 (discussing the value of children's data). A transition to active use also increases privacy concerns as more information about the child is created. *Id.*

[28] According to San Diego County District Attorney, over 45 million children ages ten through seventeen use the internet, and among them, one of four encountered unwanted pornography, one in five had been sexually solicited, and close to sixty percent of teens have received an email or instant message from a stranger and half have communicated back. *See Protecting Children Online*, SAN DIEGO CNTY. DIST. ATT'Y, https://www.sdcda.org/preventing/protecting-children-online/facts-for-parents#facts [https://perma.cc/X95H-MZ84]; Sheri Madigan et al., *The Prevalence of Unwanted Online Sexual Exposure and Solicitation Among Youth: A Meta-Analysis*, 63 J. ADOLESCENT HEALTH 133, 137 (2018) (stating one in nine youth experienced unwanted online sexual solicitation).

[29] Online harassment is defined as "rude, threatening or offensive content directed at others by friends or strangers, through the use of information communications technology." May O. Lwin et al., *Stop Bugging Me: An Examination of Adolescents' Protection Behavior Against Online Harassment*, 35 J. ADOLESCENCE 31, 31 (2012).

[30] In some instances, bullying could lead to dire outcomes like suicide. Take the case of Megan Meier as an example—a thirteen-year-old girl who committed suicide after she was cyberbullied by the mother of a classmate, while believing that it was a sixteen-year-old boy who lived nearby. *See* Christopher Maag, *A Hoax Turned Fatal Draws Anger but No Charges*, N.Y. TIMES (Nov. 28, 2007), http://www.nytimes.com/2007/11/28/us/28hoax.html [https://perma.cc/J757-UH2Z]. Interestingly, this case led Rep. Linda Sanchez (D-CA) to introduce the "Megan Meier Cyberbullying Prevention Act," making cyberbullying a federal felony. *See* Megan Meier Cyberbullying Prevention Act, H.R. 1966, 111th Cong. (2009). For more on cyberbullying, see generally ROBIN M. KOWALSKI ET AL., CYBER BULLYING: BULLYING IN THE DIGITAL AGE 46 (2008) (defining cyberbullying as "bullying through the use of technology such as the Internet and cellular phones").

[31] *See* Madigan et al., *supra* note 28, at 137 (stating approximately one in five youth was exposed to unwanted sexual content).

[32] Some platforms block certain content. Facebook, for instance, has mechanisms for reporting content that does not meet its community's standards and thus could be removed. This mechanism, however, has proven only partly helpful, as violent and offensive images sometimes remain visible for a while or are not removed at all. *See* Devin Coldewey, *Graphic Video of Suicide Spreads from Facebook to TikTok to YouTube as Platforms Fail Moderation Test*, TECHCRUNCH (Sept. 13, 2020, 1:47 PM), https://techcrunch.com/2020/09/13/graphic-video-of-suicide-spreads-from-facebook-to-tiktok-to-youtube-as-platforms-fail-moderation-test/ [https://perma.cc/27AE-KLBT].

[33] Children might, for instance, be exposed to problematic online "games" that could in turn drive them into self-harm and even suicide. *See* David Mikkelson, *How Much of a Threat Is the Purported 'Momo Challenge' Suicide Game?*, SNOPES (Feb. 26, 2019), https://www.snopes.com/news/2019/02/26/momo-challenge-suicide-game/ [https://perma.cc/SVX5-3V55]; *see also* PALFREY ET AL., *supra* note 21, at 7.

of websites discussing different methods of committing suicide[34] or concealing eating disorders,[35] it can also be dangerous by discouraging readers from seeking professional help.[36] Active online communication also poses the risk that children will engage in inappropriate sexual conduct[37] or become vulnerable to various forms of exploitation, such as having previously-shared content maliciously repurposed.[38] Further, social media "challenges," particularly on TikTok, encourage potentially dangerous behavior.[39]

---

[34] *See* Adekola O. Alao et al., *Cybersuicide: Review of the Role of the Internet on Suicide*, 9 CYBERPSYCHOLOGY & BEHAV. 489, 490 (2006) (finding over 100,000 websites discussing different methods of committing suicide and tips for maximum effectiveness and even posting suicide notes and bulletins and chatrooms in which people receive encouragement or even engage in suicide pacts). Some websites even block participants who dissuade others from committing suicide. Research shows that these types of conversations are especially dangerous for children and adolescents. *See* Tony Durkee et al., *Internet Pathways in Suicidality: A Review of the Evidence*, 8 INT'L J. ENV'T RSCH. & PUB. HEALTH 3938, 3938 (2011).

[35] *See* Dina L. G. Borzekowski et al., *e-Ana and e-Mia: A Content Analysis of Pro-Eating Disorder Web Sites*, 100 AM. J. PUB. HEALTH 1526, 1531 (2010).

[36] *See* Durkee et al., *supra* note 34, at 3939; Alao et al., *supra* note 34, at 490.

[37] While this scenario could fit many incidents of children and teens who are sexually active, there have been some reported incidents of school children engaging in sexual activities with their teachers, made possible by technology. One such incident involved Brittany Zamora, a twenty-seven-year-old teacher at an elementary school, who used a school application to message one of her students, a thirteen-year-old boy, while exchanging explicit images and text messages. *See* Nika Shakhnazarova, *Twisted Miss: Predatory Married Teacher Brittany Zamora, 27, 'Romped with Boy, 13, After Grooming Him Using Her School's Own Social Media App*,*'* SUN (UK) (Jan. 23, 2019, 3:47 PM), https://www.thesun.co.uk/news/8262636/brittany-zamora-married-teacher-romped-boy-grooming-school-app [https://perma.cc/Q9NS-V67E].

[38] *See* Tasha Robinson, *Black Mirror's Arkangel Misses Out on So Many Story Opportunities*, VERGE (Jan. 8, 2018, 2:22 PM), https://www.theverge.com/2018/1/8/16864378/black-mirror-arkangel-season-4-jodie-foster-rosemarie-dewitt-review-analysis [https://perma.cc/J2BV-PPRK].

[39] *See Italy Blocks TikTok for Certain Users After Death of Girl Allegedly Playing 'Choking' Game*, GUARDIAN (Jan. 22, 2021, 8:47 PM), https://www.theguardian.com/world/2021/jan/23/italy-blocks-tiktok-for-certain-users-after-death-of-girl-allegedly-playing-choking-game [https://perma.cc/B82K-8J6Y]. The "choking challenge," however, was not the first reported, dangerous challenge on TikTok. *See, e.g.*, Jane Wakefield, *TikTok Skull Breaker Challenge Danger Warning*, BBC NEWS (Mar. 4, 2020), https://www.bbc.com/news/technology-51742854 [https://perma.cc/72TX-57LH]; Maggie O'Neill, *Why TikTok's #StandUpChallenge Is So Dangerous, According to a Trainer*, HEALTH (Nov. 5, 2020), https://www.health.com/mind-body/jeanette-jenkins-stand-up-challenge-tiktok [https://perma.cc/P8RC-CQLZ].

Online activity not only renders children victims of harm, but also affords children the opportunity to become perpetrators of harm, as frequently seen in online bullying situations.[40] Risks can also spill over to the physical world when predators obtain information from children that jeopardizes the child's or family's safety and property.[41]

To add to the alarming number of online risks, internet connectedness is problematic for children even in the absence of malicious, illegal, or abusive behavior. Research shows that children and adolescents are spending an increasing amount of time on the internet,[42]

---

[40] *See* Faye Mishna et al., *Cyber Bullying Behaviors Among Middle and High School Students*, 80 AM. J. ORTHOPSYCHIATRY 362, 365 (2010) (noting over one-third of respondents indicated they had bullied others online).

[41] *See* Sean Gallagher, *12-Year-Old's Online Life Brings an Abductor to Her Doorstep*, ARS TECHNICA (Nov. 20, 2014, 2:00 PM), http://www.arstechnica.com/tech-policy/2014/11/12-year-olds-online-life-brings-an-abductor-to-her-doorstep [https://perma.cc/DQR2-J5YC]; *cf.* LENORE SKENAZY, FREE-RANGE KIDS: GIVING OUR CHILDREN THE FREEDOM WE HAD WITHOUT GOING NUTS WITH WORRY 16 (2009) ("The chances of any one American child being kidnapped and killed by a stranger are almost infinitesimally small: .00007 percent."). Berin Szoka & Adam Thierer, *Cyberbullying Legislation: Why Education Is Preferable to Regulation*, 16 PROGRESS ON POINT 12, 3–4 (2009) http://www.pff.org/issues-pubs/pops/2009/pop16.12-cyberbullying-education-better-than-regulation.pdf [https://perma.cc/QL79-V5LW] (although children can be instructed "not to talk to strangers," this may be less effective online since deception is so much easier); *cf.* Charlotte Chang, *Internet Safety Survey: Who Will Protect the Children?*, 25 BERKELEY TECH. L.J. 501, 514–15 (2010) ("Just as children learn to not take candy from strangers, they can also learn to not share personal information and about the wrongs of internet harassment."). Notably, while online deception could also affect adults, this Article focuses on children, as this form of deception might carry greater risks. With the emergence of the Internet of Things (IoT)—the connecting of ordinary objects to the internet—these risks might be amplified. *See* Kevin Ashton, *That 'Internet of Things' Thing*, RFID J. (June 22, 2009), https://www.rfidjournal.com/that-internet-of-things-thing-3 [https://perma.cc/4GYR-S4JW]; *see also* Hertzel, *supra* note 15, at 434. The evolution of smart toys, such as toys that are communicative to children via the IoT, might further blur the distinction between a seemingly friendly toy that is communicating with a child and an adversary who hacked the child's smart toy and communicates through it. *See* Woodrow Hartzog, *Unfair and Deceptive Robots*, 74 MD. L. REV. 785, 787 (2015) (arguing that young children might become attached to robots "acting autonomously" and "disclose secrets to the robot that they would not tell their parents or teachers"); Haber, *supra* note 15, at 405–09, 427 n.177 (arguing that it is very difficult for children, especially young ones, "to distinguish what is real from what is not real").

[42] In a 2018 study of teenage engagement online, forty-five percent of participants said they used the internet "almost constantly," up from twenty-four percent a few years beforehand. *See* JOHN PALFREY & URS GASSER, THE CONNECTED PARENT 35 (2020).

to the extent that many experts insist such engagement constitutes addiction.[43] Some view online activity as a waste of time,[44] but online engagement can be highly valuable.[45] The problem lies in children's extensive internet use, particularly on social media, because such use is associated with severe physical and mental health issues. Adolescents who are heavy internet users are more likely to experience insomnia and other sleep disturbances, stress, loneliness, depression, and anxiety.[46] Time on Facebook is negatively associated with well-being,[47] and studies show that reducing time on the platform increases life satisfaction, alleviates depressive symptoms, and generally leads to a healthier lifestyle, including more physical activity and less smoking.[48] In contrast, more frequent social media use is correlated with higher rates of experiencing body dissatisfaction and developing eating disorders.[49] However, at the same time,

---

[43] The 2020 Netflix docudrama, *Social Dilemma*, detailed the insidious methods that social media platforms use to cause addiction and profit from it while taking up increasing amounts of people's time. *See generally* SOCIAL DILEMMA (Netflix 2020). However, the science of addiction is not conclusive because the definition of addiction includes not only frequent use, but also impairment of other areas of life by the extent of that use. Among other online activities, the *Diagnostic and Statistical Manual* refers to "gaming disorder" as a condition that may qualify as a mental disorder, but requires further research. *See* AMERICAN PSYCHIATRIC ASSOCIATION, DIAGNOSTIC AND STATISTICAL MANUAL OF MENTAL DISORDERS § 3 (5th ed. 2013). Gaming disorder involves a situation in which people are immersed in the game world, which takes precedent over other activities. PALFREY & GASSER, *supra* note 42, at 112–13.

[44] Many parents are extremely distressed about the time their children spend on screens because of their negative evaluation of this activity. PALFREY & GASSER, *supra* note 42, at 19, 127.

[45] Children can engage in online activities such as learning, activism, or maintaining valuable relationships with family and friends. *Id.* at 20, 23, 30, 162, 182.

[46] *See, e.g.*, Lee M. Cheung & Wing S. Wong, *The Effects of Insomnia and Internet Addiction on Depression in Hong Kong Chinese Adolescents: An Exploratory Cross-Sectional Analysis*, 20 J. Sleep Rsch. 311, 311 (2011).

[47] *See* Agata Blachnio et al., *Association Between Facebook Addiction, Self-Esteem and Life Satisfaction: A Cross-Sectional Study*, 55 Comput. in Hum. Behav. 701, 703 (2016) (finding that Facebook addiction was negatively linked to life satisfaction).

[48] *See* Julia Brailovskaia et al., *Less Facebook Use—More Well-Being and a Healthier Lifestyle? An Experimental Intervention Study*, 108 COMPUTS. IN HUM. BEHAV. 1, 5 (2020) (describing how 140 participants in the study reduced their daily Facebook time by twenty minutes and showed improvement in self-reported well-being relative to a control group who continued using Facebook as usual).

[49] Annalise G. Mabe et al., *Do You "Like" My Photo? Facebook Use Maintains Eating Disorder Risk*, 47 INT'L J. EATING DISORDERS 516, 519 (2014); Jaime E. Sidani et al., *The Association Between Social Media Use and Eating Concerns Among US Young Adults*, 116

the internet acts as an important source of mental health information and emotional support, which can be immensely helpful in treating these conditions.[50]

One might argue that introducing new technology has always posed new risks and altered existing ones, and that most concerns are just another form of *media panic*.[51] There is some merit to this argument; the world has never been completely safe for children, and a parent's role vis-à-vis this challenge is the same as it has always been—to guide and advise their child, build trust, and maintain an open channel of communication.[52]

While we acknowledge the importance of providing education and securing a parent–child relationship, we seek to illuminate the novel risks and challenges present in the modern, digital age.[53] Taken together, the broad scope of content,[54] the nearly infinite number of users around the world who can communicate with children, and the fact that children may be exposed to online dangers while out of their parents' sight, makes the internet a whole new ball game of threats to children. Since online activity is time-consuming

---

J. ACAD. NUTRITION & DIETETICS 1465, 1470 (2016) (finding participants in the highest quartiles for social media volume and frequency were significantly more likely to have eating issues).

50 Self-rating scales, for example, are available online and are important as they can encourage people with mental health issues to seek medical help. *See* Durkee et al., *supra* note 34, at 3946 (stating that children and adolescents are especially likely to seek emotional support on social media).

51 Based on this argument, adults might be panicking about the dangers of new media usage by their children because it is unfamiliar and threatening to them. *See* Kirsten Drotner, *Dangerous Media? Panic Discourses and Dilemmas of Modernity*, 35 INT'L J. HIST. EDUC. 593, 595 (1999); Michael Z. Newman, *Children of the '80s Never Fear: Video Games Did Not Ruin Your Life*, SMITHSONIAN MAG. (May 25, 2017), https://www.smithsonianmag.com/history/children-80s-never-fear-video-games-did-not-ruin-your-life-180963452/#aLUAvkSrMsR8ibwR.99 [https://perma.cc/9C6G-5PTB]; *see also* PALFREY & GASSER, *supra* note 42, at 82.

52 *See generally* SONIA LIVINGSTONE & ALICIA BLUM-ROSS, PARENTING FOR A DIGITAL FUTURE: HOW HOPES AND FEARS ABOUT TECHNOLOGY SHAPE CHILDREN'S LIVES (2020).

53 *See* BENTLEY ET AL., *supra* note 18, at 4–5.

54 As an example, some estimate that 720,000 hours of new content is uploaded to YouTube every day. *See* James Hale, *More Than 500 Hours of Content Are Now Being Uploaded to YouTube Every Minute*, TUBEFILTER (May 7, 2019), https://tubefilter.com/2019/05/07/number-hours-video-uploaded-to-youtube-per-minute [https://perma.cc/J8L3-8AWC].

and difficult to monitor, parents fear they may be completely unaware if their child is in trouble.[55] These unique circumstances make it more challenging to protect children against online risks.

This invites a regulatory question: how can we keep children safe? Should protection stay within the realm of parental discretion as part of a parent's general responsibility to protect and care for their child? Are there other modalities of behavioral regulation that could help protect children online, such as social norms, the market, or technology? Should the law step in and regulate children's safety? If so, how?

II. REGULATING CHILDREN'S PROTECTION ONLINE

Behavior regulation takes many forms. While the law is often a natural candidate for behavioral regulation, legal rules are but one modality for regulating behavior. Behavioral regulation may also be accomplished through social norms, the market, and technology, either independently or combined.[56] In choosing the optimal modality, one must consider the associated costs, the effectiveness in substantially reducing online risks to children, and the implications on existing rights and liberties (of both children and adults).

This Part examines how these modalities aid the regulation of children's protection online. It begins with a discussion of the current legal regime governing children's online protection and normatively assesses the challenges policymakers face. Then, it details current non-legal modalities, focusing on parental self-regulation,

---

[55] *See Protecting Children Online*, *supra* note 28 ("Over 75% of Internet crimes involving sexual solicitations of children and exposure to unwanted pornography is not reported to police or parents."); Oksana Caivano et al., *When You Think You Know: The Effectiveness of Restrictive Mediation on Parental Awareness of Cyberbullying Experiences Among Children and Adolescents*, *14* CYBERPSYCHOLOGY, no. 1, 2020, at para. 3. (stating that parents are not very good at evaluating their children's experiences; parents of children in elementary school underestimated their participation in cyber aggression, whereas parents of adolescents in high school overestimated their participation in cyber aggression).

[56] As suggested by Lawrence Lessig, four modalities could regulate behavior: the market, social norms, technology (code), and law. *See* LAWRENCE LESSIG, CODE: VERSION 2.0 120–37 (2006) [hereinafter CODE 2.0]; LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY 116–73 (2004) [hereinafter FREE CULTURE].

social norms, the market, and technological developments that preceded AI algorithms. After showing why existing modalities are insufficient to meet the current landscape, Part III will introduce and discuss the rise of algorithmic parenting, analyze its challenges, and offer a toolkit for policymakers to accommodate it.

A. Legal Framework Addressing Children's Online Safety

In the context of child safety, the law sets forth a general framework for distinguishing legal from illegal conduct, regardless of whether such activities occur online or offline. Criminal and civil laws set the playing field, identifying unlawful behavior and a corresponding threshold that determines when children become legally responsible for their actions.[57] In some instances, policymakers could strengthen existing laws to meet risks and address harms resulting from online activity. For example, lawmakers could pass a statute that explicitly criminalizes sending sexual communications to a child[58] or restricting convicted felons' access to social networking sites.[59] However, the general legal framework outlining illegal conduct does not advance children's safety very far without effective enforcement mechanisms in place to protect children who partake in online activity. While the law presupposes the existence of effective enforcement mechanisms, children are often reluctant to tell anyone, let alone their parents, about illegal activities they encounter,[60] if they even understand that a violation of law occurred.

More broadly, using the law to protect children requires more than general criminal restrictions and legislation targeting illicit conduct. Rather, a robust legal solution aimed at addressing the

---

[57] For more on the age of legal responsibility in various legal contexts, see generally Jonathan Todres, *Maturity*, 48 HOUS. L. REV. 1107 (2012).

[58] *See, e.g.*, Serious Crime Act 2015, c. 9, § 67 (UK) (criminalizing sexual communication with a child in England and Wales, an offence that carries a maximum two-year prison sentence). In the United States, few states have enacted laws that criminalize attempts to solicit a minor to engage in sexual activity through online communication. *See, e.g.*, Julie Sorenson Stanger, Comment, *Salvaging States' Rights to Protect Children from Internet Predation: State Power to Regulate Internet Activity Under the Dormant Commerce Clause*, 2005 BYU L. REV. 191, 193–97 n.11 (2005). Another example is cyberbullying, against which victims could try using existing harassment or criminal laws.

[59] *See* Chang, *supra* note 41, at 505–06.

[60] *See supra* note 55 and accompanying text.

challenges described above requires more intricate consideration of the class it aims to protect, the nature of the threats, and the potential consequences regulation may have on children's well-being, development, and relationships.

There is little doubt that the state has a duty to protect children from harm.[61] Not only has this duty been recognized in the domestic laws of all jurisdictions,[62] but also states have created systems and invested resources to fulfill the duty.[63] In 1989, the United Nations adopted the Convention on the Rights of the Child ("the Convention"), which was formally recognized in the international arena.[64] The Convention, which the United States abstained from ratifying,[65] marked the first international attempt to protect children under the age of eighteen by mandating, among other things: the protection of children's rights to life, survival, and development; the right to nondiscrimination; the right to education; the protection from violence and sexual exploitation; the right to privacy; and the right to freedom of expression, thought, and association.[66] Notably, in the context of this Article, the Convention granted children the right to the provision of assistance, protection, prevention of harm, and participation.[67] It required that "child[ren] ha[ve] access to information and

---

[61] *See* Prince v. Massachusetts, 21 U.S. 158, 165 (1944) (upholding the state's interest in protecting the welfare of children); Amitai Etzioni, *On Protecting Children from Speech*, 79 CHI.-KENT L. REV. 3, 6 (2004).

[62] *See, e.g.*, Tamar Ezer, *A Positive Right to Protection for Children*, 7 YALE HUM. RTS. & DEV. L.J. 1, 27–31 (2004) (giving examples of jurisdictions in which there is a positive legal duty to protect children).

[63] *See* CHILD PROTECTION SYSTEMS: INTERNATIONAL TRENDS AND ORIENTATIONS 6 (Neil Gilbert et al. eds., 2011). Different countries take different views on what they are required to do: those that take a narrow view "tend to focus on protecting children from the risk of harm and providing basic social safety nets; those that take a broad degree of responsibility also protect children from the risk of unequal life outcomes as a result of their social standing or upbringing." *Id.*

[64] *See* Convention on the Rights of the Child arts. 2, 3, Nov. 20, 1989, 1577 U.N.T.S. 3 [hereinafter Convention on the Rights of the Child].

[65] *See id.*; *Treaty Ratification*, ACLU, https://www.aclu.org/issues/human-rights/treaty-ratification [https://perma.cc/NPT5-2MUR] (the United States signed the convention on February 16, 1995 but has not ratified it).

[66] Convention on the Rights of the Child, *supra* note 64, at arts. 2, 3, 6, 8, 12–17, 19, 28–30.

[67] *See id.* These rights are often termed the "four P's" of the CRC (provision of assistance, protection, prevention of harm, participation) (sometimes referred to as the "three P's"). *See, e.g.*, Sonia Livingstone, *Reframing Media Effects in Terms of Children's*

material," while signatories could establish "appropriate guidelines for the protection of the child from information and material injurious to his or her well-being . . . ."[68]

Domestic legislation acknowledging online risks to children followed when Congress passed the Communications Decency Act ("CDA") in 1996.[69] The CDA included "indecency provisions" to protect children from online pornography.[70] However, these provisions were eventually struck down as unconstitutional for infringing free speech rights under the First Amendment.[71]

In 1998, Congress enacted the Children's Online Privacy Protection Act ("COPPA"), designed to protect children under the age of thirteen from unfair or deceptive acts or practices in connection with personal information.[72] The Federal Trade Commission ("FTC") was tasked with enforcing COPPA and promulgating and updating rules for compliance.[73] COPPA applies to online service

---

Rights in the Digital Age, 10 J. CHILD. & MEDIA 4, 5 (2016); *see also The UNCRC, Children's Rights and Should Children Make Decisions About Their Lives*, WE HAVE KIDS, https://wehavekids.com/parenting/Should-children-be-protected-from-Desicion-Making-in-their-Lives [https://perma.cc/NDJ3-WWNV] (Mar. 9, 2020) ("Within the UNCRC children's rights are divided into four groups, known as the four p's.").

68 *See* Convention on the Rights of the Child, *supra* note 64, at art. 17.

69 Notably, there have been a few attempts to shield children from other types of media consumption. One example is Section 505 of the Telecommunications Act of 1996, which is designed to require cable television operators to scramble, block, or limit sexual content. Eventually, the Supreme Court struck down this section because less restrictive means were available. *See* Telecommunications Act of 1996, Pub. L. No. 104-104, § 505, 110 Stat. 56 (1996), *invalidated by* United States v. Playboy Ent. Grp., 529 U.S. 803 (2000).

70 *See* 47 U.S.C. § 223(d).

71 *See* Reno v. ACLU, 521 U.S. 844, 885 (1997); *see generally* Eugene Volokh, *Freedom of Speech, Shielding Children, and Transcending Balancing*, 1997 SUP. CT. REV. 141 (1997) (providing more discussion of this case).

72 *See* Children's Online Privacy Protection Act (COPPA), Pub. L. No. 106-170, 112 Stat. 2681 (1998) (codified as amended at 15 U.S.C. §§ 6501–6506 (2018)). Notably, in 1974, Congress protected children's privacy to some extent with the enactment of the Family Educational Rights and Privacy Act ("FERPA"), which regulates children's informational privacy and family privacy and applies to educational institutions' release of educational records to unauthorized persons. *See* 20 U.S.C. § 1232g(b)(1); *Family Educational Rights and Privacy Act (FERPA)*, U.S. DEP'T EDUC. (Aug. 25, 2021), http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html [https://perma.cc/5JXZ-3EYP].

73 *See* Children's Online Privacy Protection Rule, 16 C.F.R. § 312.9 (2013); 15 U.S.C. § 6505; 15 U.S.C. §§ 45(l)–(m), 53(b). The COPPA rule has been in effect since April 2000. For the latest update, see Children's Online Privacy Protection Rule, 78 Fed. Reg.

providers ("OSPs") that target or knowingly collect personal information from children under the age of thirteen.[74] It requires these actors to adhere to several legal principles—known as fair information practices—including notice, consent, access, data minimization, security, and enforcement.[75] With some differences, the European Union took a similar approach in enacting the General Data Protection Regulation.[76]

3972 (Jan. 17, 2013). *See* Andrew Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, 48 SAN DIEGO L. REV. 809, 817 (2011); *see also* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 599 (2014) ("An 'unfair or deceptive' act or practice is a material 'representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment' or a practice that 'causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.'"). Substantial injury, in this instance, could apply to both financial harms and unwarranted health and safety risks.

[74] *See* 16 C.F.R. § 312.2 (2013); 15 U.S.C. §§ 6501(1), 6502, 6501(8). Specifically, COPPA requires websites that fall under its scope to (1) include a notice containing what information is collected, how collected information is used, and the website's information disclosure practices; (2) obtain verifiable parental consent for the collection, use, or disclosure of such personal information; (3) grant parents the ability to obtain a description of the specific types of personal information collected from the child by that operator and have the opportunity to refuse further use or maintenance or future online collection of personal information from that child; (4) provide reasonable means, in the given circumstances, for the parent to obtain any personal information collected from that child; (5) adhere to data retention and deletion requirements; (6) not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity; and (7) establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. *See* 15 U.S.C. § 6502(b)(1); 16 C.F.R. §§ 312.4–312.10 (2013). *See also* Eldar Haber, *The Internet of Children: Protecting Children's Privacy in a Hyper-Connected World*, 2020 U. ILL. L. REV. 1209, 1224–25 (2020) (discussing COPPA further).

[75] FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 3–4 (May 2000); Garber, *supra* note 15, at 153.

[76] The General Data Protection Regulation (GDPR) protects all data subjects within the European Union (EU) and the European Economic Area (EEA), but also sets higher standards for all collection, use, and disclosure of data when children's data are involved. Under Article 8, parental consent is required for all children younger than sixteen when online services are offered directly to them; EU member states can lower the age threshold to thirteen. Consequently, Recital 38 requires prior parental consent before processing children's personal data. *See* Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the

A final legislative measure relating to children's risks online is the Children's Internet Protection Act ("CIPA").[77] Enacted in 2001, CIPA conditions the allocation of certain federal funds to K–12 schools and libraries upon the use of filters and other measures aimed at protecting children from obscene and harmful online content.[78] CIPA, however, is highly limited, as it merely targets internet access in specific schools and libraries and defines harmful content relatively narrowly.[79]

COPPA is the primary regulation in the United States for protecting children's privacy rights.[80] While not designed for the

---

Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 8, 2016 O.J. (L 119) 1. For further reading on the EU's perception of protecting children's privacy, see generally Milda Macenaite, *From Universal Towards Child-Specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation*, 19 NEW MEDIA & SOC'Y 765 (2017); Sonia Livingstone, *Children: A Special Case for Privacy?*, 46 INTERMEDIA 18 (2018).

77 *See* Children's Internet Protection Act (CIPA), Pub. L. No. 106-554, 114 Stat. 2763A-335 (2001) (codified as amended at 20 U.S.C. § 9134(f) and 47 U.S.C. § 254(h)). Other legislative acts enacted to protect children could also apply online in some instances. *See, e.g.*, Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003, Pub. L. No. 108-21, 117 Stat. 650-93 (2003) (providing, *inter alia*, protection of children from sexual exploitation). Notably, this Act also incorporated the Truth in Domain Names Act (TDNA), which made unlawful the use of deceitful domain names for the purpose of attracting individuals to pornographic websites. *See* Truth in Domain Names Act of 2003, S. 800, 108th Cong. (2003), 18 U.S.C. §§ 2252B(a)–(b). For further reading on the CIPA and TDNA, see generally Susan Hanley Kosse, *Try, Try Again: Will Congress Ever Get It Right? A Summary of Internet Pornography Laws Protecting Children and Possible Solutions*, 38 U. RICH. L. REV. 721, 738–59 (2004); Christopher G. Clark, Note, *The Truth in Domain Names Act of 2003 and a Preventative Measure to Combat Typosquatting*, 89 CORNELL L. REV. 1476, 1512–13 (2004); Michael Honig, Commentary, *The Truth About the Truth in Domain Names Act: Why This Recently Enacted Law Is Unconstitutional*, 23 J. MARSHALL J. COMPUT. & INFO. L. 141 (2004).

78 *See* 47 U.S.C. § 254(h)(1)(B).

79 CIPA was challenged on constitutional grounds but was eventually upheld by the Court. *See* United States v. Am. Libr. Ass'n, 539 U.S. 194, 214 (2003). For more on CIPA, see generally Felix Wu, *United States v. American Library Ass'n: The Children's Internet Protection Act Library Filtering, and Institutional Roles*, 19 BERKELEY TECH. L.J. 555 (2004). Notably, some states have enacted laws that also relate to filtering in publicly funded schools or libraries. For a list of these state laws, see *Laws Relating to Filtering, Blocking and Usage Policies in Schools and Libraries*, NAT'L CONF. STATE LEGISLATORS (July 10, 2020), http://www.ncsl.org/research/telecommunications-and-information-technology/state-internet-filtering-laws.aspx [https://perma.cc/58ZN-ZDZ2].

80 *See* Haber, *supra* note 74, at 1224–25.

protection of children's safety *per se*, COPPA indirectly promotes safety (albeit in a limited way) for several reasons. First, it applies to the collection of personal information online, which includes, *inter alia*, names, addresses, telephone numbers, and other identifiers that make it possible to contact children, either online or physically.[81] By regulating the collection of personal information, COPPA mitigates some of the safety risks facing children.[82]

COPPA also helps protect children by requiring "verifiable parental consent" before engaging in data collection.[83] This provision requires parents to engage with the technology their children use and strengthens parents' involvement in their children's internet activity.[84] Similarly, COPPA addresses children's safety by protecting the confidentiality, security, and integrity of children's personal information. It requires OSPs to establish and maintain reasonable procedures specifically protecting children under thirteen.[85] Strict security requirements help reduce the risk of adversaries gaining unauthorized access to databases or websites that store children's data.

Perhaps the most significant feature of COPPA in the context of children's safety is parents' right to review personal information provided by their child.[86] OSPs must provide "reasonable means" for parents to review personal information collected from a child and prohibit further use or maintenance of the data.[87] Essentially, this grants parents a monitoring right.[88] If policymakers extend the scope of this monitoring right and apply it (with proper modifications) to children's safety, then perhaps parents will be granted more than just a mere legal right to monitor their children's communications. Rather, OSPs may have a legal obligation to equip parents with monitoring technology while also acknowledging children's autonomy and the limits of parental monitoring.

---

81 *See* 15 U.S.C. § 6501(8).

82 *See* Haber, *supra* note 74, at 1235–36.

83 *See* 16 C.F.R. § 312.5 (2013).

84 For example, this can be done by zoning their children's use of the internet—namely, which websites they are allowed to visit or content they are allowed to share.

85 *See* 16 C.F.R. § 312.8 (2013).

86 *See id.* § 312.6.

87 *Id.* § 312.3(c).

88 For more on the problems that stem from such monitoring right, see Haber, *supra* note 15, at 443–53.

The current regulatory framework is highly important for protecting children from data-mining.[89] The problem, however, is that COPPA was crafted to achieve a different goal and is limited in scope.[90] Because the law primarily addresses privacy concerns arising from data-mining, it fails to address most other risks that children encounter online.[91] This is true even in the face of exceptions for child-data related activity, such as abusing children's data to deceive and interact with them. Like many other countries, the United States focuses mostly on protecting children's data from collection and manipulation, which, though important, represent merely a fraction of online risks, and hardly the worst of them.[92]

Another crucial shortcoming of COPPA is that it applies only to children under the age of thirteen.[93] While children are entitled to increasing independence and autonomy as they age, the dangers detailed above are not limited to children under the age of thirteen. To the contrary, some dangers are especially acute in adolescence as children begin owning smartphones and other connected devices, become independent internet users, and create profiles on social media platforms.[94]

This is where our policymakers must step in. They must assess the scale and extent of risks facing children online and adapt current legislation to offer better protection for children. Admittedly, it is not that American policymakers have never attempted to regulate online risks for children.[95] Congress and state legislatures have tried various legal measures aimed toward reducing risks to children

---

89 For more suggestions on how to recalibrate COPPA to meet new challenges that the internet poses to children, see *id.* at 428–43; Haber, *supra* note 74, at 1233–48.

90 For instance, COPPA applies only to commercial websites or online services targeted to children or with actual knowledge that they are collecting personal information from children. *See* 15 U.S.C. §§ 6501(10), 6502(b)(1)(A).

91 *See* Haber, *supra* note 74, at 1232.

92 *See supra* notes 27–49 and accompanying text; *see generally supra* Part I.

93 *See* Haber, *supra* note 74, at 1224.

94 *See supra* notes 27–49 and accompanying text; *see generally supra* Part I.

95 For examples of failed congressional acts and other forms of children-related regulation struck down by the court, see generally Adam Thierer, *Congress, Content Regulation, and Child Protection: The Expanding Legislative Agenda*, PROGRESS ON POINT (Feb. 2008), http://www.pff.org/issues-pubs/ps/2008/ps4.4childprotection.html [https://perma.cc/L8JJ-EEM6].

online, especially relating to harmful content.[96] For instance, Congress attempted to ban social media use in places where children can access computers, such as in schools and public libraries.[97] State legislatures have also pushed for regulation requiring social media sites to implement reliable age verification algorithms.[98] However, by now these proposed solutions are obsolete given the exponential growth in internet accessibility (via smartphones, for instance).[99] Further, some solutions are highly limited in scope, focusing mostly on social media[100] or merely preventing access to pornography.[101]

A potential legal solution is imposing responsibilities on intermediaries like OSPs to reduce online risks.[102] This could include holding OSPs liable for failing to identify harmful content—and either blocking or reporting it—or misconduct by children.[103] This

---

96 *See supra* notes 69–71 and accompanying text.

97 *See, e.g.*, the Deleting Online Predators Act (DOPA) of 2006, H.R. 5319, 109th Cong. (2006) (proposing to ban social networking sites in public schools and libraries).

98 *See* Szoka & Thierer, *supra* note 41, at 3.

99 In Britain, for instance, "[s]martphone ownership by children in particular has risen sharply, with close to half of all 5 to 15 year olds owning a smartphone according to Ofcom" while "the average age of children getting a smartphone in the UK is 10." *See* THE CHILD.'S SOC'Y & YOUNGMINDS, SAFETY NET: CYBERBULLYING'S IMPACT ON YOUNG PEOPLE'S MENTAL HEALTH 13 (2018), https://www.youngminds.org.uk/media/dp0mu4l5/pcr144b_social_media_cyberbullying_inquiry_full_report.pdf [https://perma.cc/J8ZK-PU53].

100 *See* Deleting Online Predators Act, *supra* note 97.

101 *See supra* notes 69–71 and accompanying text.

102 For further reading on intermediary liability, see generally Giancarlo F. Frosio, *Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy*, 112 NW. U. L. REV. 19 (2017).

103 See, for instance, the Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act (SAFETY) for an attempt to require service providers to retain information about users' IP addresses. Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act (SAFETY), H.R. 837, 110th Cong. § 6 (2007). For another legislative attempt to incentivize private sector cooperation with internet safety initiatives, see the Internet Safety Act. SAFE Internet Act, S. 1047, 111th Cong. § 4 (2009). Perhaps the most famous example is the Child Online Protection Act (COPA), which was designed to reduce the exposure of children to inappropriate materials online by limiting commercial computer communications deemed harmful to minors. COPA eventually failed to pass constitutional muster as it placed an impermissible "burden" on speech. *See* Child Online Protection Act, Pub. L. No. 105-277, 112 Stat. 2681-736 (1998), *invalidated by* Ashcroft v. ACLU, 542 U.S. 656 (2004). For more on regulatory attempts to shield children from sexual content and the Supreme Court's decision in *Ashcroft*, see generally Steven E. Merlis, *Preserving Internet Expression While Protecting Our Children: Solutions Following Ashcroft v.*

solution sounds promising upon first glance given OSPs' ability to identify harmful content on their networks and their position as the cheapest (or least) cost avoiders.[104]

However, this is not an ideal solution. From a practical perspective, OSPs may have trouble deciding whether specific content is actually risky or harmful to children. Although some instances may be relatively uncontested—such as pornographic websites—others would prove ambiguous.[105] Even more concerning, a legal duty to restrict harmful content could threaten constitutionally protected speech. OSPs currently enjoy immunity under Section 230 of the CDA.[106] While some propose reducing Section 230 immunity,[107] it is unlikely that such legislation would pass constitutional muster due to its potential infringement of First Amendment rights.[108]

The result is current legislation and regulations that do not offer viable solutions to the various risks that online life entails. Can the law do more to protect children? Or would other modalities, such as market forces or education, be more effective? We now move on to examining how online safety could be promoted without legal intervention.

B. Online Safety Without Legal Intervention

Legal rules are but one modality of regulating behavior. Other modalities, like social norms, the market, and technology—either

---

ACLU, 4 NW. J. TECH. &. INTELL. PROP. 117 (2005); Michael B. Cassidy, Note, *To Surf and Protect: The Children's Internet Protection Act Polices Material Harmful to Minors and a Whole Lot More*, 11 MICH. TELECOMM. & TECH. L. REV. 437 (2005).

[104] The cheapest (least) cost avoider is known in tort law and generally refers to the capability of preventing an accident at the lowest cost. For more on this theory in the context of online intermediaries, see generally Assaf Hamdani, *Who's Liable for Cyberwrongs?*, 87 CORNELL L. REV. 901 (2002).

[105] *See* Chang, *supra* note 41, at 521–22.

[106] *See* 47 U.S.C. § 230(c)(1).

[107] For instance, Bradley Areheart suggested enacting "notice and takedown" liability for "tortious cyberbullying," wherein failing to remove the content could lead to liability. *See* Chang, *supra* note 41, at 521 (quoting Bradley A. Areheart, *Regulating Cyberbullies Through Notice-Based Liability*, 117 YALE L.J. POCKET PART 41 (2007)). Joan Lukey proposed a system whereby OSPs would be obliged to remove some harmful content upon the filing of a lawsuit. *See* Chang, *supra* note 41, at 522–23.

[108] *See* U.S. CONST. amend. I. The main fear would arise from its potential vagueness and over-inclusiveness, which could lead to a chilling effect. *See* Chang, *supra* note 41, at 522.

separately or in combination—might be optimal for achieving online safety. One might argue that children's safety both online and offline could, and perhaps should, be protected through non-legal interventions.

Parents are first and foremost tasked with protecting children. This is not only a legal duty, but a moral one,[109] and is a defining characteristic of the family as a social construct. Like the physical world, it is no surprise that many parents seek ways to keep their children safe online without any legal obligation to do so.[110] Many parents invest significant time and thought into planning how to best prepare their children for the digital world. This involves making decisions about what online activities their children will be able to

[109] *See generally* John Eekelaar, *Are Parents Morally Obliged to Care for Their Children?*, 11 OXFORD J. LEGAL STUD. 340 (1991) (discussing parental obligations); Nellie Wieland, *Parental Obligation*, 23 UTILITAS 249, 255 (2011) ("Biological parents, *being causally responsible for the existence of their children*, presumably inherit a moral responsibility to care adequately for their dependent children . . . ."); James Lindemann Nelson, *Parental Obligations and the Ethics of Surrogacy: A Causal Perspective*, 5 PUB. AFFS. Q. 49, 50–57 (1991) (discussing "intentional" versus "causal" parental obligations). For more context on parental responsibilities and genetics, see generally PARENTAL RESPONSIBILITY IN THE CONTEXT OF NEUROSCIENCE AND GENETICS (Kristien Hens et al. eds., 2017).

[110] At least some statistics have shown that parents are not using parental control tools because many trust their children online to follow the rules they have set. Other parents, however, do not use parental controls because they are unsure how to use those tools, don't realize those tools exist, are concerned about costs of the tools, or have doubts about their effectiveness. *See* FAM. ONLINE SAFETY INST., WHO NEEDS PARENTAL CONTROLS? A SURVEY OF AWARENESS, ATTITUDES, AND USE OF ONLINE PARENTAL CONTROLS 3–8 (2011).

participate in,[111] limitations on screen time,[112] and guidelines for behavior—in other words, deciding the dos and don'ts.[113]

However, most modern approaches to good parenting involve more than rule-setting and decision-making. For example, parents focus on nurturing a trusting relationship with their children by opening communication channels where parents can offer guidance through dilemmas, and consolation or encouragement through heartbreak and disappointment. These relationships are extremely valuable to parents and children alike. More specifically, these relationships are crucial for recognizing and addressing the risks children face.[114] Engaging in dialogue and building trust over the years

---

[111] For many parents, this involves educating themselves about the internet and its opportunities and risks; it also depends on the different values parents hold. *See* LIVINGSTONE & BLUM-ROSS, *supra* note 52, at 11–14 (recognizing three typical parental reactions to technology depending on their values, abilities, and preferences: embrace, balance, and resist).

[112] *See, e.g.*, FAM. ONLINE SAFETY INST., ONLINE SAFETY ACROSS THE GENERATIONS 6 (2018), available at http://fosi-assets.s3.amazonaws.com/media/documents/2018Report_FR_d6_web.pdf [https://perma.cc/A7DY-96MA] ("To keep their connected children safe online, 91% of parents set household rules, 63% report using at least one of a variety of parental control tools, and 64% frequently discuss online safety with their child."); LIVINGSTONE & BLUM-ROSS, *supra* note 52, at 45–46 (arguing that the content and context of online activity was more important than screen time). For a similar argument and practical recommendations concerning screen time limitations for children of different ages, see PALFREY & GASSER, *supra* note 42, at 29–33 (citing Press Release, American Academy of Pediatrics, *American Academy of Pediatrics Announces New Recommendations for Children's Media Use* (Oct. 21, 2016) https://www.aap.org/en/news-room/news-releases/aap/2016/aap-announces-new-recommendations-for-media-use [https://perma.cc/Q83S-FVE4]) (recommending that children from birth to eighteen months of age avoid screens altogether; eighteen months to two years—fifteen minutes a day; two to five years—one hour a day; six to twelve years—up to two hours a day; twelve to fifteen—no more than four hours a day).

[113] *See* Szoka & Thierer, *supra* note 41, at 19–20 (offering the following rules: (1) "treat others you meet online with the same respect that you would accord them in person"; (2) "do not bully or harass your peers"; (3) "avoid using lewd or obscene language online or in communications"; (4) "do not post negative comments about your teachers or principals online"; (5) "do not post or share inappropriate pictures of yourself or others"; (6) "be extremely careful about talking to strangers online"; (7) "do not share your personal information with unknown parties"; and (8) "talk to parents and educators about serious online concerns and report dangerous situations or harassing communications to them").

[114] *See, e.g.*, Elise R. DeVore & Kenneth R. Ginsburg, *The Protective Effects of Good Parenting on Adolescents*, 17 Current Op. Pediatrics 460, 463 (2005) (demonstrating the significant, enduring, and protective influence of positive parenting practices on adolescents).

makes it more likely that a child will confide in a parent upon encountering online bullying or inappropriate internet behavior.[115] Ongoing dialogue between parents and children about the digital world and its challenges will allow children to understand and reflect on matters before they arise, such as appropriate online behavior and truth versus falsehood in online expressions. Some parents are directly involved in their children's online activity[116] by using technology to bond with their children, share experiences, and create overlapping areas of interest.[117] Shared online activity can also help model appropriate content and behavior.[118]

Children's safety and well-being increases when parents shape online behavior and habits using education and rule-setting.[119] Moreover, knowing what constitutes prudent online behavior is a valuable asset that children will enjoy into adulthood.[120] While recognizing the importance of digital education, this solution is imperfect on its own. Parental involvement varies family to family and

---

115 *See* Josephine Kearney & Kay Bussey, *The Longitudinal Influence of Self-Efficacy, Communication and Parenting on Spontaneous Adolescent Disclosure*, 25 J. RSCH. ON ADOLESCENCE 506, 516 (2015) (finding that perceived openness in relationship with mother predicted the amount of information shared); PALFREY & GASSER, *supra* note 42, at 12.

116 Scholars often use the term *parental mediation* to describe the methods parents use to regulate and educate their children's experiences with media. *See, e.g.*, Claudia van Kruistum & Roel van Steensel, *The Tacit Dimension of Parental Mediation*, 11 CYBERPSYCHOLOGY, no. 3, 2017, at para 1. Regarding parental mediation of television watching, some scholars have offered three styles of such mediation: instructive mediation, restrictive mediation, and social co-viewing. *See* Patti M. Valkenburg et al., *Developing a Scale to Assess Three Styles of Television Mediation: "Instructive Mediation," "Restrictive Mediation," and "Social Coviewing*,*"* 43 J. BROAD. & ELEC. MEDIA 52, 52–53 (1999). In the context of internet mediation, see Sook-Jung Lee & Young-Gil Chae, *Children's Internet Use in a Family Context: Influence on Family Relationships and Parental Mediation*, 10 CYBERPSYCHOLOGY & BEHAV. 640, 642–43 (2007); Livingstone & Helsper, *supra* note 21, at 584; Leslie Haddon, *Children's Critical Evaluation of Parental Mediation*, 9 CYBERPSYCHOLOGY, no. 2, 2015, at para 4.

117 *See* LIVINGSTONE & BLUM-ROSS, *supra* note 52, at 88–89 (describing a parent who "had embedded into her and [her son's] relationship their mutual fascination with all things technological.").

118 PALFREY & GASSER, *supra* note 42, at 13, 59, 62, 73.

119 *See* Chang, *supra* note 41, at 524–27; *see also* Szoka & Thierer, *supra* note 41, at 17–19 (listing advantages of an education-based approach).

120 In fact, although this Article is primarily concerned with the protection of children, adults obviously face online dangers too.

relates to a parent's capabilities and circumstances.[121] In addition to influences that hinder parental guidance, such as lack of time and limited emotional availability, not all parents have sufficient technological knowhow and skills to meaningfully engage their children in discussion on these issues.[122]

Technological literacy and parenting capabilities are not evenly distributed throughout society and often correlate with social class.[123] Despite the ubiquity of technology use in developed countries, the "digital divide" on the basis of socio-economic status has not disappeared. Rather, it has taken on different forms.[124] Children from advantaged backgrounds are less likely to spend excessive time online and more likely to engage in high-quality activity online such as coding, independent learning, and games that build skills.[125] The digital divide raises a concern that children from disadvantaged backgrounds are less likely to benefit from the kind of parental support likely to decrease risky and unsafe online behavior. Parenting styles are a matter of choice and ideology, but are also constructed and confined by social class and life circumstance. It is difficult for single parents, uneducated parents, and parents struggling

---

121 *See generally* LIVINGSTONE & BLUM-ROSS, *supra* note 52.

122 *See* Randall S. Davies, *Understanding Technology Literacy: A Framework for Evaluating Educational Technology Integration*, 55 TECHTRENDS 45, 49–50 (2011); *Parents Unaware of Dangers Faced by Children on Smartphones*, BBC NEWS (Feb. 11, 2014), https://www.bbc.com/news/technology-26121434 [https://perma.cc/2G8G-YAU4].

123 For a discussion of the digital divide, see Eszter Hargittai, *The Digital Divide and What to Do About It*, *in* NEW ECONOMY HANDBOOK 821, 821–38 (Derek C. Jones ed., 2003).

124 *See* Nellie Bowles, *The Digital Gap Between Rich and Poor Kids Is Not What We Expected*, N.Y. TIMES (Oct. 26, 2018), https://www.nytimes.com/2018/10/26/style/digital-divide-screens-schools.html [https://perma.cc/TB6Z-PPHF]; PALFREY & GASSER, *supra* note 42, at 101, 144.

125 *See* Courtenay Harris et al., *A Socioeconomic Related 'Digital Divide' Exists in How, Not If, Young People Use Computers*, PLOS ONE, Mar. 31, 2017, at 9; LIVINGSTONE & BLUM-ROSS, *supra* note 52, at 64–68, 78 (describing the limited possibilities for low-income parents to direct their children's use of technology; inequality persists also in advantage conferring activities such as coding classes because the well-off draw on their resources to access advanced courses whereas low-income children must rely on what is offered in school).

financially to engage in the type of parental practices necessary to nurture well-being-promoting behavior online.[126]

Further, differences in values and beliefs influence the kind of education parents may offer their children about online behavior.[127] For example, in past decades, many parenting styles involved intensive engagement. Referred to as "helicopter parenting," this style involved a parent's tendency to hover over children, overprotecting them not only from risks, but also disappointment, frustration, and mistakes.[128] A contrasting parenting trend provided a less structured environment for children and encouraged more freedom and autonomy.[129]

Given the reality and potential severity of harm stemming from online activity, relying solely on parents and social norms is an inadequate solution. The limitations of parental involvement might be mitigated by involving other agents in the educational setting.[130] Schools and institutions offering extracurricular education play a role in instilling appropriate norms. Research shows that discussing internet-related issues with teachers reduces online risks for teenagers.[131] Thus, schools could shoulder some of the digital education

---

[126] *See* LIVINGSTONE & BLUM-ROSS, *supra* note 52, at 64–68 (stating that "while [marginalized] mothers were positive about technology, they were not well placed to encourage their children toward more advanced independent or creative pursuits that would give them digital skills.")

[127] *See* LIVINGSTONE & BLUM-ROSS, *supra* note 52, at 14–17.

[128] Helicopter parenting is just one term for this phenomenon; others are "invasive parenting," "overparenting," and "snowplow parenting." This generally describes parents who are "obsessed with their children's success and safety [and] vigilantly hover over them, sheltering them from mistakes, disappointment, or risks . . . ." *See* Kathleen Vinson, *Hovering Too Close: The Ramifications of Helicopter Parenting in Higher Education*, 29 GA. ST. U. L. REV. 423, 424 (2013); Gaia Bernstein & Zvi Triger, *Over-Parenting*, 44 U.C. DAVIS L. REV. 1221, 1225 (2011).

[129] David Pimentel, *Protecting the Free-Range Kid: Recalibrating Parents' Rights and the Best Interests of the Child*, 38 CARDOZO L. REV. 1, 7–12 (2016).

[130] The proposed Internet Safety Act was designed, *inter alia*, to initiate a funded program to educate children and parents on internet safety. *See* SAFE Internet Act, S. 1047, 111th Cong. (2009).

[131] *See* Wonsun Shin & May O. Lwin, *How Does "Talking About the Internet with Others" Affect Teenagers' Experience of Online Risks? The Role of Active Mediation by Parents, Peers, and School Teachers*, 19 NEW MEDIA & SOC'Y 1109, 1121 (2017). Shin & Lwin also found that discussing these issues with peers increased exposure to risky behavior. *Id*. at 1121–22.

responsibility. In addition, companies like Disney, who create content for children, could address these issues in their shows as they do with other issues of social importance such as racial and cultural diversity.[132] Combining these efforts may raise awareness and shape social norms of online behavior, make children less prone to risky behavior (such as sending photographs of themselves), and less likely to commit online harm as perpetrators. Therefore, from a broader institutional perspective, one might suggest that the state should educate both children and parents on internet risks and proper online behavior.

However, even if variations among parental education are reduced and social norms improved, it is unlikely these risks will be eliminated. Undesirable activity will likely continue, such as online harassment or inappropriate content-sharing.[133] So, while digital education is crucial, reducing online risks necessitates combining digital education with other modalities.[134]

The final two modalities are closely linked – the *market* and *technology*. Technology is a promising candidate for reducing children's online risks. With sufficient demand, technology could have a significant market where commercial companies are incentivized to develop and offer risk-minimizing features in their products and services.[135] Indeed, OSPs respond to parental demand by providing

---

[132] *See generally* Ute Sartorious Kradey, *Sunny Days on Sesame Street? Multiculturalism and Resistance Postmodernism*, 26 J. COMMC'N INQUIRY 9 (2002) (discussing Sesame Street's role in education for multiculturalism); *cf.* Maja Rudloff, *(Post)Feminist Paradoxes: The Sensibilities of Gender Representation in Disney's* Frozen, 35 OUTSKIRTS, 2016, at 1–2 (arguing that despite the attempt to create "new" female characters, they are still archetypical, conservative, sexist, and even racist).

[133] For more context of selling pornographic magazines to minors under New York law, see Ginsberg v. New York, 390 U.S. 629, 634–35 (1968).

[134] *Cf.* Adam Thierer, *Rep. Bean's "SAFER NET Act": An Education-Based Approach to Online Child Safety*, 14.3 PROGRESS ON POINT (Feb. 2007), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=975507 [https://perma.cc/HQ98-9VNM] (arguing that "[t]here is simply no substitute for education").

[135] For example, Apple's parental controls can "block or limit specific apps and features on your child's device." *Use Parental Controls on Your Child's iPhone, iPad, and iPod Touch*, APPLE (Sept. 1, 2021), https://support.apple.com/en-us/HT201304 [https://perma.cc/8YGS-TZPK].

parental monitoring and control tools.[136] Policymakers suggested filtering harmful content[137] as one of the first technological means in protecting children from media risks.[138] However, this solution was criticized harshly, primarily because it limits free speech.[139] Further, filtering solutions are only partially effective. Parents are not always aware of them, may not know how to use them, and children are often able to bypass them.[140] Moreover, even if filtering

---

[136] See Keeping Children Safe Online, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.us-cert.gov/ncas/tips/ST05-002 [https://perma.cc/VNV3-3J9Q] (Sept. 2, 2021). One such attempt was made by MySpace (a social media platform) in 2008, which reached an agreement with attorneys general to "take significant steps to better protect children on its [website], including the creation of a broad-based task force to explore and develop age and identity verification technology." See Attorneys General Announce Agreement with MySpace Regarding Social Networking Safety, 2 NAAG, no. 1 (Jan. 18, 2008), https://web.archive.org/web/20200805021105/https://www.naag.org/publications/naagazette/volume_2_number_1/attorneys_general_announce_agreement_with_myspace_regarding_social_networking_safety.php [https://perma.cc/FNU3-9XGA?type=image]. Other social media sites also sometimes remove convicted sex offenders. See Chang, supra note 41, at 504–05.

[137] The use of filtering or screening technology (mainly for protection against pornographic websites) has gained much scholarly attention. *See generally, e.g.*, FRANK YORK & JAN LARUE, PROTECTING YOUR CHILD IN AN X-RATED WORLD (2002); SUSAN CHAMBERS & ANNE MEYERS, WEB GUIDE TO ONLINE SAFETY FOR KIDS (2003); Cheryl B. Preston, *Zoning the Internet: A New Approach to Protecting Children Online*, 2007 BYU L. REV. 1417, 1419, 1426 (2007) (offering a filtering mechanism for pornographic content she dubs "West Coast Code"). For examples of recent parental monitoring technologies that either filter or block content, see Nichole Cartmell, *Parental Control Apps to Track Your Child's Smartphone Habits*, (KFVS12 television broadcast July 30, 2019), https://www.kfvs12.com/2019/07/31/parental-control-apps-track-your-childs-smartphone-habits [https://perma.cc/UT3M-7MB6].

[138] The Telecommunications Act of 1996, for instance, requires that television sets over thirteen inches include something termed a "V-Chip"—a technological solution giving parents the ability to block violent and indecent programming. *See* Jack M. Balkin, *Media Filters, the V-Chip and the Foundations of Broadcast Regulation*, 45 DUKE L.J. 1131, 1131 (1996); Matthew L. Spitzer, *An Introduction to the Law and Economics of the V-Chip*, 15 CARDOZO ARTS & ENT. L.J. 429, 431 (1997).

[139] *See, e.g.*, Balkin, *supra* note 138, at 1132; R. Polk Wagner, *Filters and the First Amendment*, 83 MINN. L. REV. 755, 757 (1999); Lawrence Lessig, *What Things Regulate Speech: CDA 2.0 vs. Filtering*, 38 JURIMETRICS J. 629, 630 (1998).

[140] This includes instances of using unmonitored devices or technologies to bypass filtering. *See* PALFREY ET AL., *supra* note 21, at 34 ("Minors can circumvent these [filtering and monitoring] technologies most simply by using the Internet at friends' houses or in other places that do not use such technologies . . . .Increasingly, minors are also learning how to use proxies to circumvent filters or to reformat their computers to remove parental controls.").

mechanisms prove effective for certain forms of content, such as pornography, the filters may fail to protect children from less conspicuous harms. For instance, it would be difficult to detect inappropriate contact, personal information disclosure, cyberbullying, and internet usage detrimental to mental health, with filters alone.

Aside from practical difficulties and assuming that regulating filtering is constitutional, there remains a substantive concern that filtering will censor content parents would not want blocked, thus limiting their children's freedom of expression and information.[141] For example, filters may block valuable content related to sexual health, such as information about STDs and contraceptives, or even works of art.[142] Filtering software with an underinclusive design may alleviate concerns but not achieve the ultimate goal of limiting harmful content.

Another technological solution involves giving parents oversight mechanisms relating to their children's online behavior. This is how U.S. policymakers viewed COPPA in 1998.[143] While Part III addresses the possibility of AI-monitoring, parents can also monitor manually. Technological oversight mechanisms are not new in childcare, and many parents harness technology to monitor their children's vital signs, health, mental state, and safety.[144] Once

---

[141] The intention here is not to suggest that such filtering mechanisms, without the use of legal modalities, are unconstitutional—the First Amendment is not implemented without involvement of policymakers. But if the legal regime obliged OSPs to install filtering mechanisms, that would, in all probability, fail to pass constitutional scrutiny. On the other hand, promoting—rather than obliging—filters might be constitutional. *See* Ashcroft v. ACLU, 542 U.S. 656, 657 (2004) ("Promoting filter use does not condemn as criminal any category of speech, and so the potential chilling effect is eliminated, or at least much diminished. Filters, moreover, may well be more effective than COPA.").

[142] *See* Alan E. Garfield, *Protecting Children from Speech*, 57 FLA. L. REV. 565, 584 (2005).

[143] *See* Haber, *supra* note 74, at 1211.

[144] Many parents monitor their children's development even before birth via ultrasound screening. After birth, they might use technological tools to monitor their children's behavior and development directly, by watching and listening to them, or indirectly, such as through wearable devices and various types of sensors, cameras, and monitors. *See* Haber, *supra* note 15, at 444; Deborah Lupton & Ben Williamson, *The Datafied Child: The Dataveillance of Childrenand Implications for Their Rights*, 19 NEW MEDIA & SOC'Y 780, 783–84 (2017); Bernstein &Triger, *supra* note 128, at 1233 (2011). One of the main technological developments that helps parents monitor their children's development, vital signs,and safety is the IoT. IoT devices could allow parents to access various sensors that

children go online, parental monitoring takes a leap. Using available technology, parents can install technological mechanisms that allow them to identify the exact location of their child at any given time,[145] control the amount of time their child spends online, what sites the child can visit,[146] and keep track of rules or goals the parent sets for the child in the physical world, such as monitoring water intake or teeth-brushing habits.[147]

---

communicatesound, imagery, and other types of data to them, giving them control of what their children are doing and saying, along with monitoring their vital signs. For more on parental monitoring via technology, see generally *id.*; Lupton & Williamson, *supra* note 144, at 783–84; Abby Adams, *Parenting Life Hacks: Top IoT Products in Baby Care*, IOT EVOLUTION (Mar. 7, 2018), https://www.iotevolutionworld.com/smart-home/articles/437360-parenting-life-hacks-top-iot-products-baby-care.htm [https://perma.cc/2B3P-MS2S]; Margaret K. Nelson, *Watching Children: Describing the Use of Baby Monitors on Epinions.com*, 29 J. FAM. ISSUES 516 (2008) (examining reviews of baby monitors to elucidate parental anxiety).

145 For instance, parents can use GPS trackers on children's smartphones or wearables that give parents control over their children's activities and mainly, their location. *See* Alexei Czeskis et al., *Parenting from the Pocket: Value Tensions and Technical Directions for Secure and Private Parent-Teen Mobile Safety*, *in* SOUPS '10: PROCEEDINGS OF THE SIXTH SYMPOSIUM ON USABLE PRIVACY AND SECURITY (2010), https://dl.acm.org/doi/10.1145/1837110.1837130 [https://perma.cc/JDT6-PZTB]; Rebecca Edwards, *2018 Best Wearable GPS Trackers for Kids Buyers Guide*, SAFEWISE, https://www.safewise.com/resources/wearable-gps-tracking-devices-for-kids-guide [https://perma.cc/U6W4-7S6S] (Oct. 1, 2021).

146 While some of these technologies could be bypassed by children, parents could generally use technological solutions to block certain web content or at least be notified when sensitive content appears on the screen. *See* Czeskis et al., *supra* note 145. The video-sharing app, TikTok, recently announced that they will grant parents more control of their children's account. *See TikTok Expands Features to Give Parents More Control of Their Teenagers' Accounts*, REUTERS (Nov. 17, 2020, 10:07 AM), https://www.reuters.com/article/us-tiktok-privacy-children/tiktok-expands-features-to-give-parents-more-control-of-their-teenagers-accounts-idUSKBN27X20P [https://perma.cc/6SNM-XFBD]; *see also* Monica Anderson, *How Parents Feel About—and Manage—Their Teens' Online Behavior and Screen Time*, PEW RSCH. CTR. (Mar. 22, 2019), https://www.pewresearch.org/fact-tank/2019/03/22/how-parents-feel-about-and-manage-their-teens-online-behavior-and-screen-time [https://perma.cc/GPN5-MWC4] (arguing that "[n]early six-in-ten parents say they often or sometimes check which websites their teen visits or look through their child's cellphone call logs or messages (58% of parents say they do each of these things). A somewhat smaller share of parents (52%) say they at least sometimes use parental controls to restrict which sites their teen can access.").

147 *See This Electric Toothbrush Uses Games to Encourage Kids to Brush Their Teeth*, EXPRESS & STAR (July 30, 2018), https://www.expressandstar.com/news/science-and-technology/2018/07/30/this-electric-toothbrush-uses-games-to-encourage-kids-to-brush-their-teeth/ [https://perma.cc/B82N-3C7Z]. For more on current parental control apps, see

Parental oversight can take further intrusive forms, with parents opting for technology that enables them to monitor and control every aspect of their children's online behavior.[148] Similar to the *Black Mirror* episode, "Arkangel" (but luckily without microchip implants),[149] parents can install monitoring mechanisms, easily gaining control of their children's devices to assess the risks and choose appropriate intervention.[150]

However, parental monitoring is not as effective as one might expect and, perhaps more importantly, it is not always beneficial for children. Such conduct has the potential to infringe children's liberty, privacy, and autonomy and may negatively affect the child-parent relationship.[151] Adequate and robust parental monitoring necessitates tremendous knowledge, time, and attention,[152] and is

---

Simon Chandler & Mark Jensen, *The Best Parental Control Apps for Android and iOS*, DIGITAL TRENDS (Mar. 26, 2021), https://www.digitaltrends.com/mobile/best-parental-control-apps/ [https://perma.cc/BB3M-A35F].

[148] *See, e.g.*, Bernstein & Triger, *supra* note 128, at 1238–39 (listing examples of monitoring technologies).

[149] The second episode of the fourth series of anthology series *Black Mirror* (titled "Arkangel"), portrays a world in which parents could implant a chip to track and monitor their children and in which there exists pixelate images that cause them distress. *See* Robinson, *supra* note 38. The possibility of microchip implants to track the location of children has been around for a while. *See, e.g.*, Barbara J. King, *Tag Him, Track Him, Hug Him, Love Him*, NPR (Nov. 7, 2013, 6:18 AM), https://www.npr.org/sections/13.7/2013/11/07/243268350/tag-him-track-him-hug-him-love-him [https://perma.cc/PDV2-SCH5]. For further reading on body implants, see Ben Popper, *Cyborg America: Inside the Strange New World of Basement Body Hackers*, VERGE (Aug. 8, 2012, 10:37 AM), https://www.theverge.com/2012/8/8/3177438/cyborg-america-biohackers-grinders-body-hackers [https://perma.cc/SZT3-DCQ8].

[150] More than twenty years ago, Neil Howe and William Strauss argued that the Millennial generation is the most "watched over generation in memory." *See* NEIL HOWE & WILLIAM STRAUSS, MILLENNIALS RISING: THE NEXT GREAT GENERATION 9 (2000). For examples of parental monitoring applications, see Ann Brenoff, *Five Apps to Spy on Your Kids Without Them Knowing*, HUFFPOST (July 29, 2015, 7:59 AM), https://www.huffpost.com/entry/how-to-track-your-kids-without-them-knowing-youre-on-their-tail_n_55afaff1e4b07af29d56f544 [https://perma.cc/9MWR-ASXR]; Bernstein & Triger, *supra* note 128, at 1238–39 (listing examples of monitoring technologies).

[151] *See, e.g.*, Lupton & Williamson, *supra* note 144, at 786–89 (arguing that while "dataveillance can be understood as a new form of ethical care provision," it also carries negativeramifications); Haber, *supra* note 15, at 450–53.

[152] For statistics regarding parental monitoring of youth's online behavior, see Monica Anderson, *Parents, Teens and Digital Monitoring*, PEW RSCH. CTR. (Jan. 7, 2016),

practically impossible given the volume of online activity across social media platforms, apps, search engines, and streaming websites.[153] As mentioned, children might also be able to bypass parental surveillance measures.[154]

While surveillance may protect children from risks, it comes at the price of infringing children's well-being and fundamental rights.[155] There is no easy answer to the question of whether parental monitoring negatively affects children, and if so, to what extent. Parental involvement in a child's life is generally considered a good thing[156] and obtaining knowledge from one's child directly has proven advantageous for the child.[157] But there is a difference between getting involved in a child's life and spying on him.[158]

---

https://www.pewinternet.org/2016/01/07/parents-teens-and-digital-monitoring [https://perma.cc/49MM-KYRN].

153 Some research indicates that many parents wish they had more forms of control over theirchildren's internet use. *See, e.g.*, FAM. ONLINE SAFETY INST., *supra* note 112, at 6 ("56% [of parents] wish they had more control over content [their children see]; 42% wish they had more control over time [their children spend online]."). *See also* PALFREY ET AL., *supra* note 21, at 34 (opining that "monitoring technologies are a useful tool to assist parents and other responsible adults in determining their children's access to appropriate Internet content, particularly for younger children.").

154 Children trying to avoid parental surveillance can do so in various ways. First, they might use abbreviations or symbols their parents don't understand. *See Protecting Children Online*, *supra* note 28. Second, they can use other devices that are not monitored or use technology to bypass parental surveillance. *See* PALFREY ET AL., *supra* note 21, at 34 ("Minors can circumvent these [filtering and monitoring] technologies most simply by using the Internet at friends' houses or in other places that do not use such technologies. Also, many handheld devices, such as gaming devices, have WiFi capabilities, and unsecured wireless networks can be accessed in the child's bedroom, backyard, or elsewhere, allowing for greater opportunity to bypass parental controls. Increasingly, minors are also learning how to use proxies to circumvent filters or to reformat their computers to remove parental controls.").

155 *See, e.g.*, *supra* note 146 and accompanying text.

156 There is a lively debate on the benefits and drawbacks of parental involvement, especially in the field of education. *See* Kathleen V. Hoover-Dempsey & Howard M. Sandler, *Why Do Parents Become Involved in Their Children's Education?*, 67 REV. EDUC. RSCH. 3, 3 (1997).

157 *See generally* Margaret Kerr & Håkan Stattin, *What Parents Know, How They Know It, and Several Forms of Adolescent Adjustment: Further Support for a Reinterpretation of Monitoring*, 36 DEVELOPMENTAL PSYCH. 366 (2000) (showing through empirical study that parents' efforts cannot be effective when a child is not willing to share information).

158 *See* Haber, *supra* note 15, at 451–53 (noting that "promoting the use of sophisticated spying devices for parents to discover their children's secrets is not among the values embedded in COPPA regulation . . . .").

To address these problems, two distinctions must be drawn. The first distinction is between children *aware* of their parents' monitoring, versus children who are *unaware* of any parental surveillance. The second distinction is between *full* parental monitoring and *partial* parental monitoring—either monitoring some of the time, or monitoring all the time but only on specific platforms.

Full parental monitoring sounds promising from a child safety standpoint. If practical, such robust monitoring without the child's knowledge could eliminate any chance of concealed activity. Unlike filtering software, this form of monitoring does not impede upon children's freedom of speech or information because it is ex post by nature. The child can explore the digital world without ex ante limitations and only upon inappropriate behavior would parents decide what to censor.

However, this is only partially accurate. Although parental monitoring does not prevent activity ex ante, it produces a severe chilling effect.[159] If a child discovers she is being monitored, even if she agreed to it (perhaps to obtain permission from her parents to be online),[160] her freedom of expression and participatory rights are threatened. Even if the child's communications and explorations are completely benign and appropriate, knowing about surveillance leads to disengagement—chilling the freedom to explore, seek opportunities, and express oneself online—and infringing the right to associate.[161] This can stunt a child's ability to develop a unique identity and worldview.

---

[159] *See* Sidne Koenigsberg, *Library Records Open to Parental Scrutiny: A New Set of Internet Access Controls for Minors?*, 29 COLUM. J.L. & ARTS 361, 375–76 (2006) (arguing that parental access to children's library records creates a chilling effect).

[160] *See generally* Stephen Williams & Lynda Williams, *Space Invaders: The Negotiation of Teenage Boundaries Through the Mobile Phone*, 53 SOCIO. REV. 314 (2005) (explaining the use of mobile phones as a bargaining chip); Haddon, *supra* note 24, at 17 (stating that there might be situations where children accept this checking as a sign of parental interest, or else see it as a trade-off to obtain other rights).

[161] *See* BENTLEY ET AL., *supra* note 18, at 17. Research is inconsistent on whether being watched encourages prosocial behavior and what affects this tendency. *See*, *e.g.*, Stefanie B. Northover et al., *Artificial Surveillance Cues Do Not Increase Generosity: Two Meta-Analyses*, 38 EVOLUTION & HUM. BEHAV. 144 (2017). *But see also* Zoi Manesi et al., *Eyes Wide Open: Only Eyes that Pay Attention Promote Pro-Social Behavior*, 2016 EVOLUTIONARY PSYCH., Apr. 14, 2016, at 1 (asserting that "eyes that pay attention," the

Parental monitoring can also negatively affect a child's sense of privacy and autonomy. Such comprehensive and thorough parental monitoring creates the kinds of challenges associated with helicopter parenting.[162] Like helicopter parenting, parental monitoring denies children privacy, not from external adversaries, but rather from their parents.[163] It lacks the necessary separation between children and parents. Parents who are intertwined with every aspect of their children's lives curtail their children's autonomy and hinder their development of independence. These problems intensify as partial monitoring becomes full parental surveillance; the spaces for autonomy and privacy for children shrink.

To a great extent, parental monitoring resembles Jeremy Bentham's *panopticon* (an efficient prison architecture)—children who are uncertain of whether they are being watched will always assume they are.[164] Though some children are risk averse,[165] this model assumes that children will comply with rules because of a suspicion they are being watched.[166] In addition, when risky behavior goes undetected by parents engaging in robust monitoring, children may wrongly deduce that certain behavior is safe and acceptable. This false feeling of protection can result in increased exposure to risks and harms.

---

social signals that remind of reputation, potentially facilitate individuals' prosocial behavior).

162 *See supra* note 128 and accompanying text.

163 *See* Haber, *supra* note 15, at 443–53.

164 While Jeremy Bentham's proposal suggested the panopticon design as a form of efficient imprisoning, Michel Foucault later interpreted and developed this model and its implications as a surveillance device. *See generally* Bert-Jaap Koops, *Law, Technology, and Shifting Power Relations*, 25 BERKELEY TECH. L.J. 973 (2010) (explaining it is not the act of being watched, but instead that at any moment one *can* be watched, that causes people to internalize the watcher's knowledge system and adapt their behaviors accordingly).

165 Economic theory usually differentiates between those who are risk-neutral, risk-preferring, and risk-averse; each child, acting rationally, might act differently depending on his or her preferences. For more on risk preferences, see generally DAVID HILLSON & RUTH MURRAY-WEBSTER, UNDERSTANDING AND MANAGING RISK ATTITUDE (2005) (explaining how human factors such an individual's objective and emotion can form a different risk attitude than the others, resulting in differing risk management and behaviors).

166 *See* Koops, *supra* note 164.

Monitoring children without their awareness can be detrimental to children's rights and well-being. Undisclosed monitoring is grounded in deception and can erode trust between parents and children.[167] Further, invisible monitoring may hinder a child's general ability to trust[168] and skew a child's perception of privacy.[169] It is a misconception that digital natives do not care about their privacy.[170] Research shows the opposite—children are keenly aware of their online presentation and who is watching them.[171] Adolescents are especially preoccupied with maintaining privacy from adults as it relates to certain activities.[172]

In sum, current parental monitoring options are inadequate to address the problems relating to children's well-being, liberties, and privacy.[173] Moreover, such modalities have proven largely ineffective.

---

[167] *See* Kosse, *supra* note 77, at 775 (suggesting that parents using technology-based tools for filtering content should explain the reasons for monitoring in advance); Haddon, *supra* note 24 at 17 ("Arguably technical interventions in the form of filters and blocking . . . can be taken to indicate a lack of trust—it is the equivalent of the imposition of a rule.").

[168] *See* Bernstein & Triger, *supra* note 128, at 1274–78.

[169] For more on the normalization of surveillance, see David Murakami Wood & C. William R. Webster, *Living in Surveillance Societies: The Normalisation of Surveillance in Europe and the Threat of Britain's Bad Example*, 5 J. CONTEMP. EUR. RSCH. 259 (2009).

[170] Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, GUARDIAN (Jan. 11, 2010, 8:58 PM), https://www.theguardian.com/technology/2010/jan/11/facebook-privacy [https://perma.cc/PY6M-LGWV]. Mark Zuckerberg is not alone. Sun Microsystems CEO Scott McNealy reportedly told a group of reporters and analysts in an interview that, "[y]ou have zero privacy anyway. . . . [g]et over it." *See* Polly Sprenger, *Sun on Privacy: Get Over It*, WIRED (Jan. 26, 1999, 12:00 PM), https://www.wired.com/1999/01/sun-on-privacy-get-over-it/ [https://perma.cc/4DKF-VB85].

[171] *See* Danah Boyd & Alice Marwick, *Social Privacy in Networked Publics: Teen's Attitudes, Practices, and Strategies*, *in* A DECADE IN INTERNET TIME: SYMPOSIUM ON THE DYNAMICS OF THE INTERNET AND SOCIETY 1 (Sept. 22, 2011) ("[T]eens have a sense of privacy, although their definitions of privacy vary widely. Their practices in networked publics are shaped by their interpretation of the social situation, their attitudes towards privacy and publicity, and their ability to navigate the technological and social environment.").

[172] *See* PALFREY & GASSER, *supra* note 42, at 109 ("An insta is ordinarily the truthful and positive account that students create for themselves; their finsta—or fake insta—can be an alternate identity, often harsher and edgier."). This is sometimes related to testing out a (sexual or other) identity for themselves when they perceive their environment as intolerant of it. *See id*. at 66.

[173] *See* BENTLEY ET AL., *supra* note 18, at 5 ("After a decade of inaction, further self-regulation would simply not be a good enough response to the risks that children face.").

This Article suggests that technology has more to offer. It can automatically detect risky behavior and notify parents or block harmful content.[174] In light of rapidly developing technology, AI-based solutions can simultaneously reduce online risks and the need for parental intervention.[175] Would such technology create substantial change in the way parents safeguard their children from online risks? What are the benefits and drawbacks to children and parents using this technology? What role should the law assume in regulating AI's use and misuse? Part III introduces the shift toward algorithmic parenting and discusses these questions.

III. THE RISE OF ALGORITHMIC PARENTING

Automation is integrated into many aspects of life and "smart devices" can be found everywhere.[176] Children interact with smart devices in the forms of connected toys, AI devices that serve as tutors, cellphones, and more.[177] These devices could alter the ways parents protect their children, monitor them, and even make decisions on behalf of their children. Identified as *algorithmic parenting* herein, this novel phenomenon is relatively new to literature concerning both parenting and technology.[178]

To understand the ramifications of a transition to algorithmic parenting and the law's role in appropriately shaping this model, this Part will first introduce algorithmic parenting and discuss the potential benefits and drawbacks. Second, it will evaluate the normative

---

174 *See* Raphael Cohen-Almagor, *Online Child Sex Offenders: Challenges and Counter-Measures*, 52 HOW. J. CRIM. JUST. 190, 197–98 (2013) (listing examples of parental control technologies).

175 *See infra* Part III.

176 For more on automation and smart devices, see Eldar Haber, *The Wiretapping of Things*, 53 U.C. DAVIS L. REV. 733, 745–47 (2019).

177 Aside from connected toys, if a child lives in a so-called "smarthome," then she is surrounded by internet-connected devices and it will be difficult for her to notinteract with devices that are constantly connected to the internet. The child might use them for various reasons, like asking questions, playing music, or play games. In addition, a child might also gain online access in their school or in places where they engage in extracurricular activities. For more on children's interactions with IoT devices, see generally Haber, *supra* note 15.

178 For another proposition that we use AI to protect children from online harms, see BENTLEY ET AL., *supra* note 18, at 25–27.

reasons for legal intervention in algorithmic parenting and the execution of such intervention.

A. Defining Algorithmic Parenting

As used in this Article*, algorithmic parenting* refers to a parent's use of AI algorithms in parental practices. It can involve a parent monitoring data from specific social media platforms through add-on installations.[179] It can also take the form of a parent collecting information about every aspect of a child's online behavior on social media platforms, search engines, mailing applications, games, and smart toys. Analyzing this data could provide information on every detail of raising a child—from nutrition and health to educational development and social activities. Computational capabilities, such as natural language processing[180] and analysis of metadata and media, could potentially allow AI algorithms to "sense" when a child's online communication may be inappropriate, risky, or indicative of distress. When the AI detects suspicious communication or indicates a child may be facing risk, it would notify the parent, who decides how to tackle the problem from there. In extreme cases where the AI detects specific harmful content, the system could simultaneously block the content and alert the parent.[181]

AI monitoring technologies can have many features embedded to further reduce risks to children. For instance, the algorithm might include a feature that recognizes forms of personal identifiable information and report when a child communicates such information

---

[179] For a survey of parental add-ons, see Ben Moore & Kim Key, *The Best Parental Control Software for 2021*, PCMAG, https://www.pcmag.com/picks/the-best-parental-control-software [https://perma.cc/N799-AVYJ] (Aug. 2, 2021).

[180] Natural language processing is "a form of AI that extracts meaning from human language to make decisions based on the information." For recent examples of natural language processing as applied in practice, see Bernard Marr, *Five Amazing Examples of Natural Language Processing (NLP) in Practice*, FORBES (June 3, 2019, 12:23 AM), https://www.forbes.com/sites/bernardmarr/2019/06/03/5-amazing-examples-of-natural-language-processing-nlp-in-practice/#66b63e671b30 [https://perma.cc/8YEF-EBWP].

[181] Extreme cases could be those that clearly fall outside the First Amendment's scope, such as child pornography and obscenity. For more on the exceptions to protected speech, see KATHLEEN ANN RUANE, CONG. RSCH. SERV., 95-815, FREEDOM OF SPEECH AND PRESS: EXCEPTIONS TO THE FIRST AMENDMENT (2014), https://fas.org/sgp/crs/misc/95-815.pdf [https://perma.cc/5EB7-E5AR].

through a device.[182] Another possible feature is the identification of websites that contain harmful or age-inappropriate materials,[183] much like labeling systems for movies and television based on content.[184] AI algorithms may even detect the use of symbols, emojis, and covert communications harmful to children and alert parents, facilitating their ability to protect children from cyberbullying.

Unlike full parental monitoring, parental notification via AI could be designed to respect children's privacy. For example, the system need not disclose the *specific* content triggering an alert. Instead, the AI could include several pre-defined categories of risk—such as disclosure of sensitive information, explicit sexual content, metadata or content analysis indicating emotional distress, and excessive or irregular hours of online activity—and alert a parent that one or more of these categories had been detected. Parents would then have the choice to talk to their children and share concerns. This option alerts parents to activities they cannot see while leaving children to decide how much detail to share with their parents through direct communication. This constitutes a significant departure from helicopter parenting and full online parental monitoring without abandoning a parent's duty to safeguard children.

Technologically, the tools that can enable algorithmic parenting are already in use and are expected to become readily available due to AI developments.[185] Studies show that data analysis from social

---

[182] Exceptions to this rule could be set—when, for instance, the information is shared with a whitelisted person.

[183] Kevin Saunders proposed making it possible for anyone who posts things online to choose whether to make the content available to everyone or just to adults. Under this proposition, if the content contains a signal, parents who have filtering software could block the content. *See* Kevin W. Saunders, *The Need for a Two (or More) Tiered First Amendment to Provide for the Protection of Children*, 79 CHI.-KENT L. REV. 257, 259 (2004).

[184] These include G (General Audiences), PG (Parental Guidance Suggested), PG-13 (Parents Strongly Cautioned), R (Restricted), and NC-17 (Adults Only). *See Film Ratings*, MOTION PICTURES ASS'N, https://www.motionpictures.org/film-ratings/ [https://perma.cc/CH4Z-VCHT]; Etzioni, *supra* note 61, at 24–25.

[185] Several companies are currently advancing the use of AI, along with big data analysis, to provide better monitoring tools for parents—for instance, CUJO AI, which has parental control mechanisms for parents. *See e.g.*, CUJO AI, https://cujo.com [https://perma.cc/8TNG-ESV4]; Rehan Ijaz, *Big Data Simplifies Child Monitoring in an Age of New Safety Concerns*, SMARTDATA COLLECTIVE,

media platforms can accurately detect and predict suicidal ideations,[186] eating disorders,[187] and depression.[188] These studies used data from a single social media platform, implying that algorithms with access to data from multiple sources would be even more accurate, including social media, search engines, and metadata concerning duration and hours of use. Accuracy improves through accumulation of data over time, which would enable further detection of changes and irregular behavior indicating distress or onset of crisis.[189]

---

https://www.smartdatacollective.com/big-data-simplifies-child-monitoring-in-an-age-of-new-safety-concerns [https://perma.cc/8WP2-JB87]; Cathy Habas, *The Best Parental Control Apps of 2021*, SAFEWISE (Sept. 21, 2021), https://www.safewise.com/resources/parental-control-filters-buyers-guide [https://perma.cc/4SDF-3XF8]. Another example is the Keepers app, which "allows you to monitor children's online activity, detect surprises behaviors and monitor their digital wellbeing—without invading your child's privacy" by monitoring "incoming and outgoing messaging on social media platforms, automatically tracking any suspicious, abusive, or inappropriate content, by referencing our smart, up-to-date phrases detection database." *See* KEEPERS, https://www.keeperschildsafety.net [https://perma.cc/2TBK-23VF].

[186] *See generally* Ramit Sawhney et al., *Exploring and Learning Suicidal Ideation Connotations on Social Media with Deep Learning*, *in* Proceedings of the 9th Workshop on Computational Approaches to Subjectivity, Sentiment and Social Media Analysis 167 (2018) (reviewing current capabilities of deep learning systems to build models for suicidal ideation detection); Bart Desmet & Veronique Host, *Recognising Suicidal Messages in Dutch Social Media*, *in* LREC 2014, Ninth International Conference on Language Resources and Evaluation 833 (2014).

[187] *See generally* Hao Yan et al., *Automatic Detection of Eating Disorder-Related Social Media Posts That Could Benefit from a Mental Health Intervention*, 52 INT'L. J. EATING DISORDERS 1150 (2019) (discussing a mistake rate of four percent in determining which posts were most in need of professional intervention).

[188] *See generally* Munmun de Choudhury et al., *Predicting Depression via Social Media*, *in* PROCEEDINGS OF THE SEVENTH INTERNATIONAL ASSOCIATION FOR THE ADVANCEMENT OF ARTIFICIAL INTELLIGENCE CONFERENCE ON WEBLOGS AND SOCIAL MEDIA 128 (2013). One study examined 476 Twitter users' activity in the year preceding the onset of a major depression episode and was able to identify user behavior associated with depression including content shared, hours of activity, decreased level of interaction, and focus on the use first-person pronouns. *Id.* at 133. The predictive model was able to accurately predict depression in 70% of cases. *Id.* at 135. On the other hand, a review of twenty-two studies concerning automatic detection of cyber bullying revealed less reason for optimism. *See* H. Rosa et al., *Automatic Cyberbullying Detection: A Systemic Review*, 93 COMPUTS. IN HUM. BEHAV. 333, 344 (2019) (explaining that definitions of cyberbullying used in these studies were often inaccurate, the quality of datasets was insufficient, and there were other methodological shortcomings).

[189] *See generally* Munmun de Choudhury et al., *Predicting Postpartum Changes in Behavior and Mood via Social Media*, *in* PROCEEDINGS OF THE SIGCHI CONFERENCE ON

A critical consideration regarding the algorithm's design is what level of risk to report to parents. Models can be designed in a stable and predictable manner to be sensitive and lower the bar for labeling risky content. This would decrease the likelihood of harms and risks going undetected and create more false positives. Setting such a standard would result in the algorithm reporting *any* disagreement the child has in a chat and *all* instances of individuals "unfollowing" the child's social media profile. These social interactions, while surely unpleasant for children, do not necessarily require parental intervention.

Oversensitive algorithms may also be counterproductive. Recall one of Aesop's fables, "The Boy Who Cried Wolf." If the algorithm floods parents with superfluous alerts, parents may stop taking them seriously and even turn them off, thereby defeating the purpose and potentially missing an alert warning of real danger to their child.

An algorithm designed to detect the most severe risks is beneficial for another reason. In response to "over-parenting" trends, experts recommend parenting strategies that are not based on surveillance, but instead involve dialogue, communication, and trust.[190] Algorithms that detect only severe cases maintain education and dialogue as the main parental strategy, with the algorithm merely acting as a supplement so parents do not miss something important. This also ensures that *children* do not miss something important because education is not always sufficient in circumstances where a child is unaware of the danger he is facing.[191]

HUMAN FACTORS IN COMPUTING SYSTEMS (2013) (generating a predictive model for new mothers' postpartum mood changes using social media); Myoungouk Park et al., *Depressive Moods of Users Captured in Twitter*, *in* ACM SIGKDD WORKSHOP ON HEALTHCARE INFORMATICS (2012) (studying whether word choice on Twitter between depressed users and non-depressed users varied); Nikhita Vedula & Srinivasan Parthasarathy, *Emotional and Linguistic Cues of Depression from Social Media*, *in* PROCEEDINGS OF THE 2017 INTERNATIONAL CONFERENCE ON DIGITAL HEALTH 127 (2017) (discussing research examining Twitter users for postpartum depression that was 70% predictive, with the rate rising to 83% if prenatal information was also included).

[190] For more on the importance of education in this context, see Kosse, *supra* note 77, at 774; PALFREY & GASSER, *supra* note 42.

[191] Thus, education will be almost useless against sophisticated adversaries disguised as trusted parties. *See, e.g.*, Awais Rashid et al., *Isis: Protecting Children in Online Social Networks*, *in* ADVANCES IN THE ANALYSIS OF ONLINE PAEDOPHILE ACTIVITY (2009)

Open communication is desirable because even in its best form, AI is unable to offer bulletproof protection against all online risks. Even assuming the algorithm could perfectly detect harmful online communication, the AI would not be of much help in instances of hackers gaining unauthorized access to a child's device or other types of deception.[192] In addition, bullying and harassment does not always contain explicit words, and interpreting language requires context.[193] Ideally, the algorithm would learn to become sensitive to consequential changes in habits that may indicate distress. Therefore, the combination of both strategies is optimal.

Regarding the parent-child relationship, algorithmic parenting is a better option than partial or full parental monitoring, blocking content, or doing nothing. As discussed in Part B, parental monitoring negatively affects the parent-child relationship and disrupts the trust in which it is grounded. Algorithmic parenting does not raise the same concerns because children are not under full parental surveillance. The algorithm alerts parents to their children's activity only when it recognizes cause for concern. The AI would not share the child's communications with parents when the child is simply sharing secrets with his best friend, or when teenagers are taking their first romantic steps.[194]

Further, algorithmic parenting has potential to strengthen the parent-child relationship. Even parents with high levels of awareness may find it difficult to have open, honest conversations about difficult topics with their children. These conversations are sometimes embarrassing and uncomfortable and both parents and children likely prefer to have as few of them as possible or even avoid them altogether. Algorithmic parenting would nudge parents to have

("Pedophiles and other child sex offenders often masquerade as children in order to establish contact with potential victims and gain their trust.").

192 Think of a hacked smart toy, which communicates with a child, asking questions or asking the child to act on his behalf, without the child knowing that the toy is hacked. *See* Haber, *supra* note 15, at 401.

193 *See* PALFREY ET AL., *supra* note 21, at 33 ("[O]ften the distinction between content that is part of social discourse and that which is harmful is context-dependent and technology is unlikely to be able to effectively recognize the "rumors" and "gossip" that make up the bulk of online harassment.").

194 Unless, of course, the algorithm recognizes some of this content as inappropriate or risky in other ways.

these conversations when parents inevitably receive an alert. While the alerts may turn out to be of little concern, they will encourage parents to speak with children about safe and ethical online behavior.

Another advantage of algorithmic parenting speaks to parents' challenge of maintaining a close, open relationship with their children. AI algorithms used for detecting online risks can offer protection for children whose parents are incapable of engaging in dialogue. Nurturing open conversations with children can be demanding, and some parents lack the time or skill to successfully do so.[195] Relationships also have their ups and downs, and even parents and children with meaningful, open relationships may go through times when children are reluctant to share their worries and dilemmas with their parents. Algorithmic parenting would provide a safety net to handle these concerns.

Algorithmic parenting can mitigate the current gaps and inequality in the way parents safeguard children from online harm, either through monitoring or education. Assuming that the software's installation and use is not prohibitively expensive or complicated, this safety measure could enable more parents to get involved in their children's online safety. We recognize that some parents are better equipped than others to use platforms as an opportunity to have open and educational conversations with their children. Nonetheless, the platform would offer even the least sophisticated users protection from severe online harms.

There are, however, several worries surrounding the effectiveness of AI algorithms for promoting children's safety. First, as noted above, algorithms may not be able to detect all cases of online risk.[196] Second, shielding children from risks or "bad" things, much like the aforementioned *Black Mirror* "Arkangel" episode, could arguably constitute overprotection.[197] It hinders a child's preparation for the real world. Further, there is concern that children will find ways to bypass the algorithm, use other devices, or conceal certain

---

[195] *See generally* PALFREY & GASSER, *supra* note 42 (acknowledging the difficulty of engaging in connected parenting).

[196] *See supra* notes 192–93 and accompanying text.

[197] *See* Robinson, *supra* note 38.

activities from the algorithm, especially those activities children think parents will object to.[198]

Another foreseeable issue is that parents may lower their personal levels of alertness to their children by relying too heavily on AI monitoring. Parents may assume that as long as the algorithm does not notify them, everything is in order. Further, parents may interpret historically concerning patterns, such as withdrawal, mood swings, or changes in appetite, as typical adolescent behavior rather than relying on intuition and taking action.

This feeds into a philosophical concern that using algorithms to monitor children's online activity delegates parental care to a machine. One of the most fundamental aspects of parenting is being the keeper of the child—the person responsible for the child thriving.[199] Worrying is not merely a side effect of parenting; rather, it is a functional pillar of parenting. Algorithmic parenting entails moving this responsibility to a third party—one that isn't even human. This can be counterproductive, and the problem of outsourcing care runs deeper than its effect: it might weaken the emotional bond between parents and children.[200] Parents foster an intimate parent-child relationship by trying to figure out, through conversation and other interaction, what a child is going through, how he feels, and what is on his mind. Besides enriching the parent-child relationship,

---

[198] One might argue that children will simply find technological ways to bypass the mechanism, for example, by connecting to a wireless network or, at some age, purchasing sim cards without parental safeguards. It is debatable, however, how prevalent that may be and there might also be some form of a tradeoff between children's abilities to bypass their parent's apps and the children's ability and maturity to better handle harmful communication.

[199] HARRY BRIGHOUSE & ADAM SWIFT, FAMILY VALUES: THE ETHICS OF PARENT-CHILD RELATIONSHIPS 88 (2014). ("The parent is charged with responsibility for both the immediate well-being of the child and the development of the child's capacities . . . the child has immediate interests in being kept safe, enjoying herself, being sheltered and well nourished, having loving relationships with proximate others, and so on . . . .The parents' fiduciary duties are to guarantee the child's immediate well-being . . . and to oversee her cognitive, emotional, physical, and moral development.").

[200] *See* Max van Manen, *Care as Worry or "Don't Worry Be Happy,"* 12 QUALITATIVE HEALTH RSCH. 262, 264 (2002) ("Worry is the active ingredient of parental attentiveness. Worry—rather than duty or obligation—keeps us in touch with the one for whom we care. Worry is the spiritual glue that keeps the mother or father affixed to the life of their child.").

concern for children's well-being is an important evolutionary tool that facilitates children's survival.[201]

To partially address these concerns and protect themselves from user dissatisfaction and legal challenges, platforms could explicitly warn users that they do not offer full protection and should be treated as an auxiliary parenting aide. Of course, this solution is limited because parents might overlook or misunderstand such warnings.

Thus, effectiveness is critical for adopting algorithmic parenting as a panacea to mitigate the digital world's inherent risks and harms. However, we believe this form of parenting is beneficial for more than just its effectiveness—it would also respect children's rights and liberties and, therefore, should be promoted by the state and private companies.

B. Algorithmic Parenting and Children's Rights and Liberties

There is no magic path to good parenting in the digital age. However, algorithmic parenting is a promising candidate for minimizing online risks facing children in the quickly-evolving digital age. Full exploration of this parenting style requires balancing the value of safety it provides against the potential implications for children's rights and liberties. This Part argues that algorithmic parenting can and should be designed to minimize such impositions.

Under the AI system, children's freedom of speech and freedom of information may be threatened. Mistakes made by automated systems might lead to reporting and blocking benign or beneficial content. For example, an algorithm programmed to block sexual content might prevent a child from accessing information about the human body or viewing works of art.[202] This issue would also arise if a child browses sites about sexual health he does not want his parents to know about. This is particularly important to young people, especially as it relates to LGBTQ youth who typically lack alternative

---

[201] *See* Robert Plutchik, *The Nature of Emotions: Human Emotions Have Deep Evolutionary Roots, a Fact that May Explain Their Complexity and Provide Tools for Clinical Practice*, 89 AM. SCIENTIST 344, 345 (2001) ("Those . . . studying the evolutionary origins of emotion have sought to understand how emotions increase evolutionary fitness for the individual. . . . Fear and anxiety in people closely parallel the state of heightened arousal of an animal who senses a predator or a threat to its offspring.").

[202] *See* Garfield, *supra* note 142.

sources of helpful, open-minded, and reliable information.[203] Such censorship raises free speech concerns and would likely face constitutional challenges if state-mandated.[204] It would also prevent children from accessing certain information instrumental to a child's development of identity and belief structure, allowing a child to shape his worldview, engage in activism, and connect with like-minded people.[205] Restrictions can inhibit a child's sense of and right to autonomy.

Foreseeable constitutional challenges may be a major barrier to legal intervention. In the context of regulating child protection online, the First Amendment has been invoked when a law incidentally denied adults' access to protected speech.[206] However, because these algorithms only target the child, impact on adults' First Amendment rights are of little concern. Other First Amendment issues that are often raised in the context of filtering technologies include prior restraint and compelled speech.[207] However, the algorithm can be designed to merely flag content rather than block access to it. This would alleviate any First Amendment concerns, even if algorithmic parenting becomes mandatory in certain cases—an option that will be explored below.

Additionally, the AI can be programmed to create and maintain an updated list of websites deemed high-quality resources for children to learn about sexuality and sexual identity. Content accessed

---

[203] *See* BENTLEY ET AL., *supra* note 18, at 17.

[204] As previously noted, Congress sought to regulate the exposure of children to inappropriate materials online by enacting the Child Online Protection Act (COPA) that eventually failed to pass constitutional muster since it placed an impermissible "burden" on speech. *See* Child Online Protection Act, *supra* note 103.

[205] *See* Koenigsberg, *supra* note 159, at 375.

[206] For more on free speech and the child-parent relationship, see generally KEVIN W. SAUNDERS, SAVING OUR CHILDREN FROM THE FIRST AMENDMENT (2003); Catherine J. Ross, *Anything Goes: Examining the State's Interest in Protecting Children from Controversial Speech*, 53 VAND. L. REV. 427 (2000); Garfield, *supra* note 142.

[207] "Prior restraint" refers to a governmental prohibition on speech ex-ante—something that does not occur under the algorithmic parenting model. "Compelled speech" rights could be somewhat summarized as a right not to speak or not to be forced to express yourself. For more on compelled speech, see, e.g., McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 348 (1995); Riley v. Nat'l Fed'n of the Blind of N.C., Inc., 487 U.S. 781, 796–97 (1988); Wooley v. Maynard, 430 U.S. 705, 716 (1977).

on these websites would not trigger the algorithm without additional indications of risk.[208]

Children's right to privacy is another important consideration. In its most comprehensive form, algorithmic parenting might involve collecting and analyzing data created by children's online activity. Companies would likely perform the process of data-mining, its analysis, and its retention. This creates a rather obvious risk: children's data might be used to further the company's commercial goals. Even if companies do not monetize such data, the servers that store this data could be breached or otherwise comprised, and the data could be released publicly, risking use for malicious purposes.[209] While these concerns are not unique to algorithmic parenting, the scope of collectable and assessable data could be huge, raising acute worries. As detailed in Part A, the current regulatory regime is insufficient to contend with this challenge, and legislators would have to reconfigure the current legal framework.[210]

The most critical and challenging privacy-related concern related to algorithmic parenting involves how much access parents should have to children's online activities and communications. Algorithms would be able to monitor a child's every click and assess activities, searching for signs of inappropriate behavior and indications of distress. The fact that these indications would be sent to children's parents raises clear privacy issues.

Some parents might condition the ability to go online, use a mobile device, or open a social media account on installing a monitoring application, so children might be under pressure to waive their privacy. Therefore, making children aware that monitoring takes place does not rectify privacy concerns. In turn, the extent of invasion of children's privacy should be minimized in advance. Algorithmic parenting could be designed to minimize privacy violations and offer children a relatively undisturbed online experience. Possible elements the design include limiting intervention to activity that

---

[208] For example, searching for information about sexual identity on a whitelisted website together with other indications might justify mental health concerns related to sexuality.

[209] *See* Haber, *supra* note 15, at 423.

[210] For one suggestion on how to recalibrate COPPA, see Haber, *supra* note 15, at 428–43.

crosses a high threshold of risk and alerting parents only to the existence of seriously risky behavior. In addition, the design could limit the kind of information parents receive and leave children with the discretion to share the content itself with their parents.[211]

A final and more philosophical, privacy-related concern is whether AI's ability to fully access children's online activity constitutes an invasion of privacy. In other words, assuming the algorithm is independent, is the fact that the algorithm "knows" things about children a violation of privacy, or does such an infringement require human sentience and cognition?[212]

All in all, we find that, alongside more traditional practices of parental mediation and education, algorithmic parenting offers substantial benefits to children's safety. It protects children's liberties and privacy better than common parenting practices such as partial or full parental monitoring, content-blocking, or screen time limitations. Algorithmic parenting is also compatible with parenting styles that focus on fostering relationships of trust and open communication. As a result, a transition to algorithmic parenting is desirable for children's protection, well-being, and rights.

C. Regulating Algorithmic Parenting

Algorithmic parenting could pave the path for increased online safety for children. If safety-enhancing algorithms become ubiquitous, lawmakers must address new challenges that will arise. This section focuses on two such issues. The first is how to regulate algorithmic parenting and its design, marketing, and operation by commercial companies. The second is whether regulators should play a role in ensuring access to algorithmic parenting, especially for children from disadvantaged backgrounds who are more prone to both general and digital risks. The natural solution is direct legal intervention. Although there may be reluctance for the government

---

[211] Parents can undoubtedly put significant pressure on their children to share content. This, however, is not unique to the online world; it can happen in relation to any secret a child is pressured to disclose.

[212] Ian Kerr argued that robots and AIs that operate independently of human intervention can, and in some cases do, diminish our privacy. *See generally* Ian Kerr, *Schrödinger's Robot: Privacy in Uncertain States*, 20 THEORETICAL INQUIRIES L. 123 (2019).

to provide the service itself,[213] the state should create incentives for companies to develop appropriate AI algorithms and subsequently encourage people to use them properly.

The first challenge involves regulating the design, marketing, and operation of parental AI algorithms. If parental demand for such services is insufficient for development in the market, the state should push and incentivize companies to voluntarily provide such tools by design.[214] It is preferable to have an indirect government approach that would *influence*—rather than oblige—the development, implementation, and education of algorithmic parenting technologies.[215] This can take the form of incentives such as subsidies or tax benefits.[216] The government must carefully tailor such incentives to avoid the appearance of engaging in covert activity that violates constitutional rights.[217]

---

[213] This argument links to what we came to learn from Edward Snowden's revelations about the state's misuse of its powers. To clarify, it is not the fear of the state learning about what constitutes harmful communication, as such data might not be sensitive *per se*, but rather that algorithmic parenting tools could enable its controller to obtain data on what children are doing online. For more on the problems of procedural safeguards and governmental misuse of its powers in the context of national security, see generally Niva Elkin-Koren & Eldar Haber, *Governance by Proxy: Cyber Challenges to Civil Liberties*, 82 BROOK. L. REV. 105 (2017).

[214] One might argue that the Supreme Court encouraged Congress to grant parents filtering tools—which could be interpreted as monitoring tools as well. In the words of Justice Kennedy, "[b]y enacting programs to promote use of filtering software . . . " such as the ability to monitor what their children see, "Congress could give parents that ability without subjecting protected speech to severe penalties." *See* Ashcroft v. ACLU, 542 U.S. 656, 670 (2004).

[215] *See* Wagner, *supra* note 139, at 777–801 (discussing indirect government approaches that could pass constitutional muster).

[216] The main challenge here would be whether the government violates the unconstitutional conditions doctrine, by which the state is forbidden from conditioning the receipt of benefits on a waiver of a constitutionally protected right. For further reading on the unconstitutional conditions doctrine, see David Cole, *Beyond Unconstitutional Conditions: Charting Spheres of Neutrality in Government-Funded Speech*, 67 N.Y.U. L. REV. 675 (1992); Kathleen Sullivan, *Unconstitutional Conditions*, 102 HARV. L. REV. 1413 (1989).

[217] *See* Balkin, *supra* note 138, at 1159. Another solution might be to impose liability for not mitigating online risks for children. Under a limited liability regime, intermediaries that do not provide algorithmic parenting services could be held legally responsible for not identifying reasonably foreseeable risks to children when these risks accumulate to actual harm. But this solution might also raise constitutional issues.

Policymakers must also tackle the negative impact of algorithmic parenting on children's rights. The underlying rationale is similar to the policy underlying COPPA.[218] However, even though COPPA could be applied within certain AI platforms,[219] it is far too limited to mitigate the drawbacks of algorithmic parenting and necessitates additional legal protections for children.

The legal framework that would govern how private companies construct and operate their algorithms must first address potential security risks stemming from technology.[220] Policymakers should require that companies providing algorithmic parenting services adhere to adequate cybersecurity measures, protecting the platform and stored data. It is crucial that the system be as difficult to hack as possible. Platforms should implement security measures capable of detecting when the system or data has been compromised. In tandem with security measures,[221] companies should include features capable of detecting deviations from its preset preferences. While this would not prevent every unauthorized access, it would reduce the overall possibility of harm.

However, the impact on human rights and liberties must not solely rest in the realm of privately owned platforms.[222]

---

[218] COPPA was crafted to prohibit unfair or deceptive acts or practices in connection with personal information from and about children on the internet. *See* Garber, *supra* note 15, at 153.

[219] *See* Haber, *supra* note 74, at 1232 ("While COPPA might apply to some IoT devices, like IoToys, it will fail to apply to many other IoT devices that will effectively be used by children under the age of thirteen.").

[220] *See* Memorandum from UC Berkeley Hum. Rts. Ctr. Rsch. Team on A.I. and Child Rts. to A.I. and Child Rts. Working Grp. 63 (Apr. 30, 2019) [hereinafter *Memorandum on A.I. and Child Rts.*] (available at https://www.unicef.org/innovation/media/10501/file/Memorandum%20on%20Artificial%20Intelligence%20and%20Child%20Rights.pdfat [https://perma.cc/4PK8-SMSC]) (suggesting that policymakers must "[a]dopt a clear, comprehensive framework for corporations that imposes a duty of care connected to the handling of children's data, and provides an effective remedy (judicial, administrative or other) for breach.").

[221] For more on the risks of poor security measures, see generally BRUCE SCHNEIER, CLICK HERE TO KILL EVERYBODY: SECURITY AND SURVIVAL IN A HYPER-CONNECTED WORLD (2018).

[222] *See Memorandum on A.I. and Child Rts.*, *supra* note 220, at 1 ("As much of the underlying technology is proprietary to corporations, corporations' willingness and ability to incorporate human rights considerations into the development and use of such technologies will be critical.").

Policymakers must be prepared to tackle the negative consequences of algorithmic parenting by establishing a new framework for its proper use. The rationales undergirding child protection laws, such as COPPA,[223] must be applied here in a stricter form. Such data collection should not be allowed for any reason other than machine learning purposes and should lack identifying attributions. To avoid data-mining, the algorithm should prioritize using the endless data that is widely and freely available online to study inappropriate content or behavior. However, to work optimally, AI will need to learn from children using the particular platform and adapt to swift social changes. Thus, databases should store little to no personally identifiable data on children. This should not affect the algorithm's precision, because the algorithm merely needs to learn what constitutes risky behavior for each relevant age.

Otherwise, any preferences or data derived directly from children must be kept only locally (i.e., on the child's or parent's device). Here, too, the risk of a privacy violation is considerably low within the context of such data-mining. Eventually, if risks of exploiting such databases grow, it would still be advisable to require databases to implement strong and frequently-updated security measures and other forms of privacy enhancement techniques.[224]

Another concern might arise from the fact that many AI services are essentially proprietary black boxes—the algorithm is not revealed.[225] Therefore, platforms labeling behavior as inappropriate

---

[223] *See* Haber, *supra* note 15, at 446 ("The main rationale behind COPPA was not to foster parental surveillance of their children online but to aid parents who wanted their children to take advantage of the internet, while obtaining better control of the practices of the websites they visited and the information requested from them.").

[224] One potential solution is differential privacy—a mathematical method that strives to assure that the presence or absence of an individual in a dataset does not make any significant difference to the outcome of database queries. For more on differential privacy, see Cynthia Dwork et al., *Calibrating Noise to Sensitivity in Private Data Analysis*, *in* THEORY OF CRYPTOGRAPHY CONFERENCE 265 (Shai Halevi & Tal Rabin eds., 2006); Cynthia Dwork, *A Firm Foundation for Private Data Analysis*, 54 COMMC'NS ACM, no. 1, at 86, 91 (2011); *see generally* Dan Feldman & Eldar Haber, *Measuring and Protecting Privacy in the Always-On Era*, 35 BERKELEY TECH. L.J. 197 (2020) (suggesting computational solutions to protect privacy in the context of IoT devices).

[225] *See* Jay Stanley, *The Privacy Threat from Always-On Microphones Like the Amazon Echo*, ACLU (Jan. 13, 2017, 10:15 AM), https://www.aclu.org/blog/privacy-technology/privacy-threat-always-microphones-amazon-echo?redirect=blog/free-future/privacy-

could shape children's behavior and social norms with little or no external oversight. While feedback from parents signaling whether an alert was justified or not might ease some of the concern, this is not altogether the case. Analogizing to a different context, algorithms may replicate social prejudice and discrimination when assisting employers in choosing prospective employees or when used by law enforcement agencies or insurance companies.[226] The same might be true of child protection algorithms that perceive language associated with certain social groups as more likely to be risky, to give but one example.

Lacking the ability to understand how these platforms operate necessitates effective oversight of the technology's use and implementation. While oversight mechanisms should always be part of the law, it is especially crucial when it comes to AI and children's rights. Oversight must be transparent, articulating clear and ethical rules about the data collected and its storage, access, and potential use. The algorithm itself must also be transparent.[227]

Another necessary change to the COPPA framework is applying the law to children above the age of thirteen.[228] This Article will not take a strong position regarding the exact age cutoff of legal protections for children. The age limit will depend, *inter alia*, on developing social perceptions of childhood, but even more importantly on parental discretion regarding when to discontinue using this form of protection.[229] However, when policymakers draw the line, they must account for an adaptive framework to accommodate changes in the

---

threat-always-microphones-amazon-echo [https://perma.cc/RNR2-F8CH]. For more on AI as black boxes, see generally FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015).

226 *See generally* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. 671 (2016) (discussing unintentional discrimination arising from algorithmic computing techniques); Carmel & Ben-Shahar, *supra* note 20, at 91.

227 *See* Alexa Hasse et al., *Youth and Artificial Intelligence: Where We Stand*, BERKMAN CTR. FOR INTERNET & SOC'Y 7 (2019), https://dash.harvard.edu/bitstream/handle/1/40268058/2019-05_YouthAndAI.pdf?sequence=5&isAllowed=y [https://perma.cc/N5NS-PPC9] ("There is a risk of undermining youth privacy if the companies that design AI-fueled technologies are not clear and ethical about how they collect user data, where that data is stored, who can access it, and what can be done with it.").

228 *See* 16 C.F.R. § 312.2; 15 U.S.C. § 6501(1).

229 *See, e.g.*, Etzioni, *supra* note 61, at 42–47 (discussing children's age and maturity).

risks that children face online according to their age.[230] In any case, the current threshold of age thirteen falls short of sufficient online privacy regulation of children within the context of algorithmic parenting.[231]

In addition to regulating the companies creating, marketing, and operating the algorithm, regulation should be directed toward other relevant actors, namely the platforms and companies who grant online services. Because children and adolescents use many of these platforms, it is important to cover their activities on these platforms.[232] However, companies and platforms are disincentivized to operate in a manner that might make them less attractive to users.

Another issue involves discerning which profiles belong to children when reporting risky content on social media or search engines. When devices are used by more than one person, such as a computer

---

[230] In this respect, there should be differences between early childhood (ages three to five), childhood (ages six to nine), preadolescence (ages ten to twelve), early adolescence (ages thirteen to fifteen), and if applicable at all, late adolescence (ages sixteen to eighteen). For this dichotomy, see YOUTH, PORNOGRAPHY, AND THE INTERNET 116–17 (Dick Thornburgh & Hebert S. Lin eds., 2002). We might want to think of situations where social childhood is extended, with people living with their parents past age eighteen, and where some parental functions may, therefore, continue past age eighteen. *See* Richard A. Settersten Jr. & Barbara Ray, *What's Going on With Young People Today? The Long and Twisting Road to Adulthood*, FUTURE OF CHILDREN, Spring 2010, at 19, 20 (2010) (stating that "[t]he process of becoming an adult is more gradual and varied today[;] . . . young people are taking longer to achieve economic and psychological autonomy.").

[231] For example, it is estimated that more than seventy percent of parents in the United States cease supervision of internet use by their children after the age of fourteen, while statistics show that most internet-related missing children cases involve children fifteen or older. *See Protecting Children Online*, *supra* note 28. But it should also not be set too high, as it is crucial for youth (and children) to make mistakes, and parents should be cautioned against too much parental control that could undermine their safety goals by harming their children's development of autonomy. To clarify, algorithmic parenting should be flexible and account for age differences. Sexual content at the age of sixteen is not as harmful as at the age of eight. And at some developmental stage, it becomes important for children to explore and learn, within their capabilities and appetites, and any form of parental monitoring could be devastating to them.

[232] *See* PALFREY & GASSER, *supra* note 172, at 35 (citing a 2018 study of teenage engagement online in which forty-five percent of participants said they used the internet "almost constantly"); *see also* Brooke Auxier et al., *Parenting Children in the Age of Screens*, PEW RSCH. CTR. (July 28, 2020), https://www.pewresearch.org/internet/2020/07/28/parenting-children-in-the-age-of-screens/ [https://perma.cc/A6KA-LSEN] (offering data concerning use of digital devices and platforms—for example 80% of parents reported their children watch content on YouTube).

used in the family's home, it would be difficult to know what use to attribute to which family member. This could also cause unintentional surveillance of certain persons, resulting in privacy issues.

Algorithms that are installed as add-ons to a specific application, such as a social media account, are even more problematic in this regard, since children can set up their profiles without disclosing their age.[233] Even when platforms know of age, they typically do not have parents' contact information. Therefore, limited legal duties should be placed on platforms (such as social media, messaging apps, etc.), and instead could include, at the most, a duty to disclose children's data upon a validated request by parents or other legal guardians.

Accordingly, incorporating AI algorithms to protect children against online harm would depend on parents being aware of both the online risks and technological solutions, and being able to ensure that the child's significant activity is covered. As pointed out above,[234] this ability is not trivial, and therefore some children who perhaps need it most might be left unprotected. This leads to the second issue policymakers would need to address: making algorithmic parenting accessible to all.

As technology develops, parents are increasingly seeking ways to protect their children from online dangers, and the market responds to this demand.[235] Assuming these solutions will not be prohibitively expensive (and regulation could ensure they are not), algorithmic parenting could very quickly be used in every household. However, as with other parenting trends, not all parents would be equally on board. This creates a clear and wide divide between children in different circumstances.

This is not a complete legal void. Parents have a legal duty to care for their children, and abuse or neglect of children is a crime.[236] Criminal law imposes duties on parents to intervene in cases when

---

233 Alternatively, children may set up an "official" profile and a second, secret profile of which parents are unaware. *See* PALFREY & GASSER, *supra* note 42 and accompanying text.

234 *See supra* Part II.B.

235 For examples of such market responses, see *supra* note 135 and accompanying text.

236 Child Abuse Prevention and Treatment Act (CAPTA), 42 U.S.C. § 5106g.

they know that children are at risk from a third party.[237] Parents, for example, have been charged when leaving a child with a known sexual offender or abusive father, or charged with manslaughter when failure to provide medical care resulted in a child's death.[238] However, this applies to harm caused by third parties and not to self-inflicted harm.[239] Additionally, it does not necessarily impose duties to actively seek this information, for example, by monitoring children's communications. And while there is something to be said for widening parents' responsibilities,[240] it seems that liability will remain confined to cases of severe neglect.[241] Therefore, current doctrine is unlikely to impose additional criminal liability on parents in relation to children's online risks.

Tort liability is also not a promising source of parental duties to reduce online risks. Doctrine regarding parental autonomy renders parents practically immune from tort liability in cases of harm to children.[242] Most states have enacted statutes making parents liable for children's torts.[243] Yet despite these statutes, imposition of civil

---

237 *See* Laura King, Note, *Damned If You Do: The Rational Parent's Quandary Under Criminal Failure-to-Protect Statutes*, 13 LIBERTY U. L. REV. 121, 125–26 (2018). Twenty-nine states have enacted specific failure-to-protect statutes, and another nineteen have more general provisions that have basically the same effect. *Id.* at 126.

238 *See* Johnson & Hargrove, *supra* note 5, at 313.

239 *See generally* Vanessa Gardianos, Note, *Adolescent Suicide: A Call for Parental Liability*, 24 ST. JOHN'S J. LEGAL COMMENT. 201 (2009) (arguing that parents should be liable when they fail to prevent their children's suicide).

240 *Id.*

241 *See* King, *supra* note 237 (advocating for failure-to-protect legislation by outlining case studies of severe neglect); Gardianos, *supra* note 239, at 208–09 (referring to the case of *People v. Scruggs*, in which a mother was convicted on the basis of a risk-to-injury statute for failing to take action when her son showed signs of severe distress. The high court in Connecticut reversed the conviction, and the Connecticut Supreme Court found the statute was unconstitutionally vague). However, even in such a rare case such as *Scruggs*, the mother was arguably blameworthy not merely for failing to notice that her son was in acute distress, but also for actually neglecting him, including an extraordinarily problematic home environment and severe emotional neglect, that was arguably to blame for the child's suicide, at least in part.

242 *See* Elizabeth G. Porter, *Tort Liability in the Age of the Helicopter Parent*, 64 ALA. L. REV. 533, 535 (2013).

243 *See* Lisa Gentile, *Parental Civil Liability for the Torts of Minors*, 16 J. CONTEMP. LEGAL ISSUES 125, 128–32 (2007) (listing parental liability statutes and noting that two states—Hawaii and Louisiana—have gone further and enacted statutes that impose strict liability on parents for their children's torts).

liability on parents is still very rare,[244] and in the case of online harms, liability is even harder to substantiate because courts examine whether parents had the opportunity and ability to exercise reasonable control over their child's actions.[245] Courts have not found parents liable when they were not physically present at the scene in which damage was caused.[246]

The reluctance to find parents liable has several explanations, such as the traditional aversion toward government interference in the family.[247] Another concern is that parental tort liability will result in the legal adoption of excessively high parenting standards that characterize middle-class parents. In a time in which middle-class parenting trends have escalated into helicopter parenting, normalizing such standards could cause injustice toward parents who cannot live up to these habits or who believe in different styles of parenting.[248]

In any case, it is unlikely that parents could be held legally responsible under current laws for harm caused to their children or by their children through online engagement. Parents would have to be actively engaged in the online activity to be held responsible for such harm.[249] Although there may be extraordinary cases in which such circumstances transpire, they are unhelpful for our exploration, which involves the more typical case in which parents are unaware of their child's unhealthy and risky online behavior.

While parents are practically immune from criminal and civil liability in cases where children are harmed,[250] third parties such as schools and colleges have been found liable by courts for harm

---

244 *See* Porter, *supra* note 242, at 545.

245 *See* Gentile, *supra* note 243, at 126.

246 *See* Porter, *supra* note 242, at 561.

247 *See* Emily Buss, *"Parental" Rights*, 88 VA. L. REV. 635, 647 (2002) ("[A] legal system that shows strong deference to parents' child rearing decisions serves children well. Parents' strong emotional attachment to their children and considerable knowledge of their particular needs make parents the child-specific experts most qualified to assess and pursue their children's best interests in most circumstances. In contrast, the state's knowledge of and commitment to any particular child is relatively thin.").

248 *Id.* at 636, 673–75.

249 This would include, for example, showing they had an "opportunity for exercising control" over their children. Porter, *supra* note 242, at 561.

250 *See generally* Gardianos, *supra* note 239; Porter, *supra* note 242.

caused to children when the school failed to report children's irregular behavior.[251] The duty to report is easily applicable to cases where a school is aware of a distressed online expression, but may be impracticable when the concerning online activity is invisible to school staff.

Still, regulators have managed to make schools partners in promoting the health, development, and protection of children, which can be applied in the case of algorithmic parenting as well. For example, schools across the country are very much involved in the nationwide struggle against childhood obesity by educating children on how to maintain a healthy lifestyle and what constitutes nutritious food.[252] Legislators in various states have even gone further, setting rules limiting snacks, fast food, and soft drinks in school cafeterias and vending machines.[253] Another example is sexual behavior. High schools engage in an effort to combat unprotected sex by teenagers and make condoms available in schools—a practice validated by courts.[254]

Schools can also promote digital safety. Most schools engage in some kind of educational work developing digital literacy, online

---

[251] *See generally* Joy Blanchard, *University Tort Liability and Student Suicide: Case Review and Implications for Practice*, 36 J.L. & EDUC. 461 (2007) (summarizing current case law related to student health and proposing recommendations for parental notification).

[252] *See Nutrition Education in US Schools*, CDC, https://www.cdc.gov/healthyschools/nutrition/school_nutrition_education.htm [https://perma.cc/C5PM-BMWK] (Feb. 15, 2021) (detailing the different measures incorporated by US schools, including standalone classes about nutrition combined with other subjects).

[253] *See* Michele Simon & Ellen J. Fried, *State Laws on School Vending: The Need for a Public Health Approach*, 62 FOOD & DRUG L.J. 139 (2007) (discussing rules used to prohibit selling beverages before the end of lunch period). A federal court overturned these regulations when a lawsuit was brought by the National Soft Drink Association (now called the American Beverage Association). This victory led to the increased availability of fast food, soft drinks, sugar, etc. in schools and the shift to state or local regulation. For more information on state and local regulation, see Lindsay F. Wiley, *"No Body Left Behind": Re-Orienting School-Based Childhood Obesity Interventions*, 5 DUKE F. FOR L. & SOC. CHANGE 97 (2013); *see also* Allison Nihiser et al., *Preventing Obesity Through Schools*, 41 J.L., MED. & ETHICS SUPPLEMENT, Summer 2013, at 27 (2013).

[254] *See* Dede Hill, Note, *Condom Availability Programs Belong in the Schools, Not in the Courts*, 1996 WIS. L. REV. 1285, 1286 (1996).

learning strategies, and ethical and safe behavior online.[255] We cannot stress enough that these are crucial for maintaining online safety and psychological well-being, and developing digital social skills. Schools could also be instrumental in implementing algorithmic parenting by offering free algorithmic monitoring as a default in all the devices they supply to children. For several years, school boards around the country have supplied electronic devices to assist and support learning.[256] During the COVID-19 crisis, distribution of electronic devices to students surged dramatically in an effort to ensure universal access to distance learning.[257] It is likely that the use of electronic devices by students will remain even after health restrictions enable the resumption of in-person learning. When schools provide devices, they could install the protective component as a default. Parents receiving these devices could also opt out so they would not be subject to this measure against their will. But parents would be more likely to use a free, default service.[258]

---

[255] This was stressed as an important goal in a Federal Report on School Safety presented to the President of the United States in 2018. Although the primary trigger for commissioning the report was acts of violence such as school shootings, the reports called more generally for prevention and education on topics of cyberbullying and preventing exposure to violent and inappropriate content online. *See* FED. COMM'N ON SCH. SAFETY, FINAL REPORT OF THE FEDERAL COMMISSION ON SCHOOL SAFETY 23, 65 (Dec. 18, 2018).

[256] Benjamin Herold, *Technology in Education: An Overview*, EDUC. WEEK (Feb. 17, 2016), https://www.edweek.org/technology/technology-in-education-an-overview/2016/02 [https://perma.cc/XKP3-5Y55] ("Increasingly, schools are moving to provide students with their own laptop computer, netbook, or digital tablet. Schools purchased more that 23 million devices for classroom use in 2013 and 2014 alone. In recent years iPads and then Chromebooks (inexpensive Web-based laptops) have emerged as the devices of choice for many schools.").

[257] *See Chicago Schools to Distribute Electronic Devices to Students for Remote Learning Amid Covid-19 Pandemic*, TIMES NW. IND. (Mar. 31, 2020), https://www.nwitimes.com/news/chicago-schools-to-distribute-electronic-devices-to-students-for-remote-learning-amid-covid-19-pandemic/article_ab611ee0-c22c-5b1d-9beb-a7c4f8e2a2ad.html [https://perma.cc/MWU9-MW73]; Benjamin Herold, *Schools Handed Out Millions of Digital Devices Under Covid-19. Now, Thousands Are Missing*, EDUC. WEEK (July 23, 2020), https://www.edweek.org/technology/schools-handed-out-millions-of-digital-devices-under-covid-19-now-thousands-are-missing/2020/07 [https://perma.cc/H342-6NMA].

[258] *See* Eric J. Johnson & Daniel Goldstein, *Decisions by Default*, *in* BEHAVIORAL FOUNDATIONS OF PUBLIC POLICY 417 (Eldar Shafir ed., 2013) (stating that people are likely to remain with default rules even if they are not beneficial for them).

For many children, devices supplied by schools would not be the only device they would use.[259] This might hinder the algorithmic oversight's effectiveness since some online activity would not be accessible to the algorithm. This problem can be solved by enabling parents to add additional devices apart from the school's device upon registering for the service.

Because schools are an important contact for children and parents, they could be instrumental in ensuring access to algorithmic parenting. But other governmental units interact with parents periodically and are specifically tasked with promoting children's well-being and protection. Some target specific families in need or crises,[260] while others are universal and supply services to all families.[261] These governmental units could also be used to promote online safety, among other things, through algorithmic parenting.

Governmental agencies that target families in need of help and children in need of protection are especially suitable candidates for encouraging algorithmic parenting. One such interface is the child welfare system, which is tasked with the protection and care of children who have been mistreated through various services such as in-home family preservation services, foster care, residential treatment, mental health care, substance abuse treatment, parenting skills classes, and more.[262] As part of these services, professionals could

---

[259] A study in 2015 found that three out of four teens have a smartphone, eighty-seven percent of teens have or have access to a computer, four out of five teens have or have access to a game console, and more than half of the teens have a tablet. Therefore, most children, especially older children, have access to at least three different connected devices. *See* Amanda Lenhart, *Teens, Social Media & Technology Overview*, PEW RSCH. CTR. (Apr. 9, 2015), https://www.pewresearch.org/internet/2015/04/09/teens-social-media-technology-2015 [https://perma.cc/Y9BF-PXXG].

[260] This includes, for example, the Child Welfare System or Family Courts. *See infra* notes 265, 267.

[261] This includes, for example, public libraries and health care centers.

[262] The Child Abuse Prevention and Treatment Act (CAPTA), originally passed in 1974, supplies federal funding to states to support prevention, investigation, prosecution, and treatment. *See How the Child Welfare System Works*, CHILD WELFARE INFO. GATEWAY (Feb. 2013), https://www.childwelfare.gov/pubPDFs/cpswork.pdf [https://perma.cc/2EHG-3KWY]; Josh Gupta-Kagan, *Toward a Public Health Legal Structure for Child Welfare*, 92 NEB. L. REV. 897, 899 (2014) (stating that a public health approach to child welfare would "provide a wider range of interventions to achieve the goal of preventing future maltreatment more effectively" and through less intrusion into families).

encourage parents to implement algorithmic parenting. The welfare system engages with the nation's most vulnerable children and youth, who are at especially high risk for those dangers algorithmic parenting is designed to detect. It would be relatively easy to implement safety measures that could help even those parents struggling the most to maintain some sort of control over their children's safety. Policymakers could issue instructions to the professionals working with families to encourage its use. Obviously, it would be crucial to universal accessibility to ensure this service is free or available at a very low cost.[263]

Family courts are another point of contact between official state agencies and families during divorce proceedings. Divorce is a moment of crisis in families' lives and a time in which both parents and children may suffer mental health difficulties.[264] It is also a moment in which the law intervenes in decisions that are otherwise parental prerogatives.[265] In the past few decades, several states have passed laws that require parents to participate in parent education or allow courts to mandate these programs for parents.[266] The goal of these

---

[263] The business model for free services often involves monetizing users' data. This would have to be addressed by regulators, as detailed above, by allowing some use of data but ensuring that it is not personalized. *See, e.g.*, Joe McKendrick, *Every Company a Data Company, Eventually*, FORBES (Jan. 8, 2019, 10:14 PM), https://www.forbes.com/sites/joemckendrick/2019/01/08/every-company-a-data-company-eventually/#31dad1515e33 [https://perma.cc/AB4L-37BC] (discussing the value of data to companies). Apple, for instance, systematically removed parental-control apps due to datamining practices. *See* Jack Nicas, *Apple Backs Off Crackdown on Parental-Control Apps*, N.Y. TIMES (June 3, 2019), https://www.nytimes.com/2019/06/03/technology/apple-parental-control-apps.html [https://perma.cc/DD52-4DLC].

[264] *See* John Guidubaldi & Joseph D. Perry, *Divorce and Mental Health Sequelae for Children: A Two-Year Follow-up of a Nationwide Sample*, 24 J. AM. ACAD. CHILD & ADOLESCENT PSYCHIATRY 531, 535 (1985) (stating that in a multifactored mental health assessment, children whose parents were divorced performed more poorly than children whose parents were not); Alan Booth & Paul Amato, *Divorce and Psychological Stress*, 32 J. HEALTH & SOC. BEHAV. 396, 404 (stating that adults going through divorce showed a rise in psychological stress in the period of time before and after the divorce).

[265] *See, e.g.*, Antony Baron Kolenc, *When I Do Becomes You Won't: Preserving the Right to Home School After Divorce*, 9 AVE MARIA L. REV. 263, 272 (2011) (explaining that courts make decisions in issues of child rearing because the parents are deadlocked).

[266] *See* Solveig Erickson & Nancy Ver Steegh, *Mandatory Divorce Education Classes: What Do the Parents Say?*, 28 Wm. Mitchell L. Rev. 889, 900 (2001); Susan L. Pollet & Melissa Lombreglia, *A Nationwide Survey of Mandatory Parent Education*, 46 Fam. Ct.

provisions is to improve cooperation between divorced parents and increase awareness of children's needs in relation to divorce.[267] Although mandatory parent education sessions are focused on other important issues, in times of crisis children's safety should receive priority; therefore information concerning algorithmic parenting could be included as an integral part of parent education.

There are several examples of governmental interactions with parents that could be used to encourage algorithmic parenting. These include processes in schools for determining eligibility under the Individuals with Disabilities Education Act ("IDEA"),[268] contending with chronic absenteeism,[269] and rehabilitating children through the juvenile criminal justice system,[270] to name a few.

However, using the suggested points of contact between parents and the state to encourage algorithmic parenting may result in disparity along socioeconomic and racial lines. On average, racial minorities and people who live in poverty are more likely to have

Rev. 375, 375 (2008); Peter Salem et al., *Taking Stock of Parent Education in the Family Courts: Envisioning a Public Health Approach*, 51 Fam. Ct. Rev. 131, 131 (2013).

267 *See* Erickson & Ver Steegh, *supra* note 266, at 900 ("The first purpose [of Minnesota's plan] is to educate parents concerning 'the impact that divorce . . . [can] have upon children and families.' The second purpose is to educate parents with respect to 'methods for preventing parenting time conflicts.' The third purpose is to educate parents about dispute resolution options.").

268 To be eligible for services under the IDEA, children receive an evaluation and an individualized educational program team is created to build the program, including deciding which services and accommodations the student needs. Parents have a right to be present at IEP meetings, as do children beginning at age sixteen. *See* Andrew M.I. Lee, *Ten Procedural Safeguards in IDEA*, UNDERSTOOD, https://www.understood.org/articles/en/10-key-procedural-safeguards-in-idea? [https://perma.cc/V4EH-NPQV].

269 *See generally* LAUREN BAUER ET AL., REDUCING CHRONIC ABSENTEEISM UNDER THE EVERY STUDENT SUCCEEDS ACT (2018) (offering strategies to reduce chronic absenteeism through implementation of statewide accountability plans under ESSA).

270 Juvenile criminal justice often puts a special emphasis on rehabilitation and therefore enables special flexibility and discretion in the measures used. Used wisely, algorithmic parenting could be integrated into the various tools used for empowering parents and rehabilitating child offenders. For a critical discussion of discretion in juvenile justice, see generally Catherine J. Ross, *Disposition in a Discretionary Regime: Punishment and Rehabilitation in the Juvenile Justice System*, 36 B.C. L. REV. 1037, 1046 (1995) (arguing that rehabilitation and proportionate retribution define the parameters of legitimate discretion in juvenile courts).

repeated interactions with state agencies, such as the welfare system[271] and family courts.[272] When schools distribute devices according to need, these students are also more likely to receive devices. This may cause a divide in which algorithmic parenting is applied more often to children from disadvantaged backgrounds.

On the one hand, this is a desirable outcome. If algorithmic parenting develops into an effective tool for protecting children from online risks without overly infringing children's privacy and liberties, we should not be concerned with such overrepresentation. Still, applying state incentives to algorithmic monitoring in such an unequal manner causes discomfort for several reasons. First, directing measures at marginalized communities runs the risk of unwanted and unjustified surveillance. However, this concern would ideally be offset by the fact that privileged parents, who are already seeking technological means for promoting online safety, are likely to be enthusiastic consumers. More importantly, alongside the targeted interventions detailed above, policymakers could design regulations that would encourage all families to shift to algorithmic parenting.

Most obviously, regulation could be instrumental in making algorithmic parenting easily accessible to all parents. In addition to regulating costs, regulations could ensure that information concerning online risks and tools for contending with them are available online and in printed brochures in schools, daycare centers, medical centers, public libraries, etc. However, brochures' effectiveness may be limited if lost in the abundance of information offered to parents in such settings.

Parents are more likely to engage in algorithmic parenting if it is offered a click away, by trusted agencies as a part of their services. Again, schools are a primary example. Not all schools provide children with devices, but many schools use learning management systems ("LMSs") for communicating with students, assigning tasks,

---

[271] *See Disproportionality and Disparity in Child Welfare*, NAT.'L CONF. STATE LEGISLATURES (Jan. 26, 2021), https://www.ncsl.org/research/human-services/disproportionality-and-race-equity-in-child-welfare.aspx [https://perma.cc/AK48-6EEC] (reporting the racial and ethnic disparity in children protection services).

[272] *See* R. Kelly Raley et al., *The Growing Racial and Ethnic Divide in U.S. Marriage Patterns*, 25 FUTURE CHILD., no. 2, at 89, 92 (2015) (stating that divorce rates are higher for Black women than they are for white women and lowest for Asian women).

delivering content, and managing students' activities and achievements.[273] When they do, all students enrolled in the school use these systems. LMSs require opening accounts and creating profiles for all users, and therefore could be programmed to automatically suggest algorithmic parenting applications, along with a recommendation from educators to use them.

Various other services that most parents consume are increasingly using online communications as well as mobile apps. For example, pediatric health care providers offering services through mobile apps could be instructed to create a default link to algorithmic parenting solutions.[274] Online services offered by public libraries[275] are another example of a service that many families access and that could be instrumental for encouraging parents to consider algorithmic parenting as a parenting tool.

Admittedly, all these measures will be unable to ensure that all children are protected. However, they can help increase parental awareness and therefore serve as an important step in the right direction. All in all, as we described in this Part, several legal measures must be taken into account with the rise of algorithmic parenting. While generally a desirable outcome, policymakers must not rely simply on the market or technology to properly advance this new form of parental monitoring, but instead must apply the suggested toolkit comprised of legislation and regulation.

---

[273] *See* Divna Krpan & Slavomir Stankov, *Educational Data Mining for Grouping Students in E-learning System*, *in* PROCEEDINGS OF THE 2012 34TH INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY INTERFACES 207, 208 (2012) (describing Moodle, a popular LMS). Most educators welcome the integration of technology into their classroom practices. *PBS Survey Finds Teachers Are Embracing Digital Resources to Propel Student Learning*, PBS (Feb. 4, 2013), https://www.pbs.org/about/about-pbs/blogs/news/pbs-survey-finds-teachers-are-embracing-digital-resources-to-propel-student-learning/ [https://perma.cc/UG7E-RNCV] (stating that according to one survey, three quarters of teachers expressed positive attitudes toward the integration of technology into the classroom).

[274] Susan Doyle-Lindrud, *Mobile Health Technology and the Use of Health-Related Mobile Applications*, 18 CLINICAL J. ONCOLOGY NURSING 634, 634 (2014) (discussing the various health-related mobile applications and their potential for oncological health care).

[275] *See, e.g.*, Louise L. Rutherford, *Building Participative Library Services: The Impact of Social Software Use in Public Libraries*, 26 LIBR. HI TECH 411, 413 (2008) (discussing the challenges and advantages of social software such as blogs, chats, forums, and picture-sharing applications for public libraries).

CONCLUSION

While parents have always been morally and legally responsible for ensuring the safety of their children, the shift to the digital world has made things significantly more complicated. Scientists in various fields have studied the changing risks and challenges, some of which remain unknown. Technology, however, may provide solutions to some of the problems it exacerbates. AI technology could facilitate the movement toward algorithmic parenting, which has potential to improve children's online safety and simultaneously safeguard their liberties, privacy, and well-being.

Since many parents are already seeking technological solutions for online protection, algorithmic parenting could easily become a new reality in many families. Therefore, the law governing the protection of children's rights must adjust to contend with its potential drawbacks. It must ensure that children's data is sufficiently protected and that this powerful tool is designed in a way that protects not only children's safety, but also their liberties, autonomy, and privacy. The law should also ensure that all children in society have access to algorithmic parenting, including those whose parents are least equipped to contend with the challenges children face in the digital world.

At the same time, social scientists must further research and evaluate the move toward algorithmic parenting and its effects on parents, children, and their relations. The regulatory regime must be highly attentive to these studies to ensure that technology is promoting children's safety, while also improving well-being, supporting development, and facilitating robust and nurturing parent-child relationships.