

# Articles

## GATEKEEPING SCREEN TIME: CONFIGURING THE REGULATION OF ADDICTIVE TECHNOLOGIES AND KIDS' PRIVACY RIGHTS

GAIA BERNSTEIN\*

### ABSTRACT

We all, and especially our kids, spend many hours on screens. Many current studies uncover the harms of excessive screen time for kids. In reaction, legislatures in many states, as well as Congress, advanced laws to protect kids from addictive technologies. The tech industry, whose revenues depend on extending users time online, reacted by raising freedom of speech claims to repeal these laws. Through hijacking the debate and focusing it on the First Amendment, tech companies obstructed the real issue at stake—how can legislatures most effectively regulate addictive technologies to reduce kids' screen time?

This Article analyzes the legislative landscape to provide the answer to this question. It reveals that while different in their mechanisms, the laws converge into two models. Each model embraces different conceptions of who should be the gatekeeper of kids' screen time on social media, games, and other online platforms. One model—the Tech Liability Model—places the responsibility directly on tech companies. The second model—the Parent Gatekeeper Model—places the responsibility on parents by requiring tech companies to provide parents tools to block or monitor kids' online.

This Article argues that the Tech Liability Model is essential to successfully regulate addictive technologies and reduce kids' screen time. First, it explains that the Parent Gatekeeper Model risks shifting responsibility from the party to blame—the tech companies—to parents. Second, it cautions that years of experience with parental controls indicate that parental gatekeeping laws are unlikely to be effective. Third, it explains that the Parent Gatekeeper Model can raise privacy concerns that would create unnecessary pitfalls. The Article proposes, however, that hybrid

---

\* Technology Privacy and Policy Professor of Law, Co-Director of the Institute for Privacy Protection and the Gibbons Institute for Law Science and Technology at the Seton Hall University School of Law. For their thoughtful comments, I would like to thank Elettra Bietti, Brett Frischmann, Josh Golin, and Elana Zeide, as well as the participants of the *Villanova Law Review* Symposium, the AALS Section of Privacy and Defamation Annual Meeting Panel, the Seton Hall Law School Legal Responses to Addictive Technologies Conference, and the Fordham Law School Neuroscience of Social Media Conference. Most of all, I would like to thank my wonderful Seton Hall RAs Emma Burch, Sophia Dagostino, and Skyler Martinez.

laws combining both models could be successful if carefully executed. Specifically, it proposes that timing matters. Legislatures can effectively enact parent gatekeeping laws if they do so simultaneously with or after implementing laws under the Tech Liability Model.

CONTENTS

INTRODUCTION . . . . . 952

I. THE TECHNOLOGY ADDICTION CRISIS . . . . . 956

    A. *Time, Kids, and Public Health* . . . . . 956

    B. *Addiction by Design* . . . . . 957

    C. *Reaction to the Tech Addiction Crisis* . . . . . 959

II. LEGISLATIVE MODELS TO REGULATE ADDICTIVE TECHNOLOGIES . . . . . 959

    A. *The Tech Liability Model* . . . . . 960

    B. *The Parent Gatekeeper Model* . . . . . 961

    C. *Hybrid Laws* . . . . . 962

III. THE VULNERABILITIES OF THE PARENT GATEKEEPER MODEL . . . . . 963

    A. *Shifting the Blame—an Old Tactic* . . . . . 963

    B. *An Ineffective Gatekeeper* . . . . . 965

    C. *Creating an Illusionary Conflict Between Privacy and Containing Tech Addiction* . . . . . 968

        1. *The Age-Verification Privacy Hyperbole* . . . . . 969

        2. *Parents as Gatekeepers and Kids’ Privacy* . . . . . 971

        3. *Privacy and Containing Tech Addiction as Harmonious Goals* . . . . . 975

IV. ROLES FOR PARENTS AS GATEKEEPERS . . . . . 977

CONCLUSION . . . . . 979

## INTRODUCTION

ADULTS spend a lot of time online. But kids who are digital natives practically live there, spending many of their waking hours on screens.<sup>1</sup> Current research reveals the alarming impact of excessive screen time on a generation of kids. Researchers found evidence of wide-ranging harm, including deteriorating mental health, delayed cognitive development, and attention problems.<sup>2</sup> At the same time, information emerging from Silicon Valley uncovered that the long periods of time spent on screens are not accidental. As one whistleblower after another testified before Congress, they documented how tech platforms, including social media and online games, design their products to addict users. These Silicon Valley insiders explained that tech companies do so because their revenue model depends on keeping users online for as long as possible.<sup>3</sup>

From the start, parents stood on the front lines of the fight against technology addiction. Even before the COVID-19 pandemic, when they saw their kids disappearing into their screens, parents started looking for solutions. They tried different parent controls, such as apps to limit kids time on their devices, and digital well-being tools like setting time warnings on social media.<sup>4</sup> Yet nothing worked. Screen time just kept creeping up.<sup>5</sup>

Hopes quickly faded that tech companies would regulate themselves and change product designs to limit time online. In recent years, a growing movement emerged, battling Big Tech on different fronts to contain kids' tech addiction and related online harms. This movement focused on state and federal legislation as a major vehicle for change. Legisla-

---

1. See *Daily Time Spent on Social Networking by Internet Users Worldwide from 2012 to 2024*, STATISTA, <https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/> [<https://perma.cc/HC4E-DNPT>] (last visited Jan. 6, 2025) (reporting how much internet users time spend online); VICTORIA RIDEOUT, ALANNA PEEBLES, SUPREET MANN & MICHAEL B. ROBB, COMMON SENSE, *THE COMMON SENSE CENSUS: MEDIA USE BY TWEENS AND TEENS 1, 3* (2021), [https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web\\_0.pdf](https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf) [<https://perma.cc/P287-PMGW>] (applies to media screen time).

2. See JONATHAN HAIDT, *THE ANXIOUS GENERATION: HOW THE GREAT REWIRING OF CHILDHOOD IS CAUSING AN EPIDEMIC OF MENTAL ILLNESS* 19–44, 140–72 (2024) (describing the impact on mental health); GAIA BERNSTEIN, *UNWIRED: GAINING CONTROL OVER ADDICTIVE TECHNOLOGIES* 16–20, 22–24 (2023) (providing an overview of cognitive development studies); GLORIA MARK, *ATTENTION SPAN: THE SCIENCE OF FOCUS IN THE DIGITAL AGE* 222–41 (2023) (describing the impact on attention).

3. See, e.g., Victor Ordonez, *Key Takeaways from Facebook Whistleblower Frances Haugen's Senate Testimony*, ABC NEWS (Oct. 5, 2021, 4:47 PM), <https://abcnews.go.com/Politics/key-takeaways-facebook-whistleblower-frances-haugens-senate-testimony/story?id=80419357> [<https://perma.cc/HN7X-M2UV>].

4. See, e.g., Christine Elgersma, *So You Got a Parental Control . . . Now What?* COMMON SENSE MEDIA (Aug. 8, 2018), <https://www.commonsensemedia.org/articles/so-you-got-a-parental-control-now-what> [<https://perma.cc/4SCP-FSMP>].

5. See Fabio Duarte, *Average Screen Time for Teens (2024)*, EXPLODING TOPICS (Nov. 10, 2023), <https://explodingtopics.com/blog/screen-time-for-teens#average> [<https://perma.cc/4R3Z-8WHL>].

tures proposed hundreds of state bills and successfully enacted some into law.<sup>6</sup> Tech companies reacted by raising freedom of speech claims under the First Amendment to challenge these laws.<sup>7</sup> By doing so, they successfully hijacked the discourse and obstructed the real issue at stake—which legislative model would be most effective in regulating addictive technologies and containing excessive screen time? This Article analyzes the legislative landscape to assess the answer to this question.

The Article reveals that the seemingly diverse legislative landscape embodies two models of laws espousing different conceptions of who should be in charge.<sup>8</sup> In other words, who should be the gatekeeper to ensure that kids do not spend excessive time online? Under one model, laws require tech platforms—typically social networks, but often games and other platforms as well—to ensure that kids are not harmed (the Tech Liability Model).<sup>9</sup> For example, these laws may require technology platforms to avoid using certain design features that are known to keep users online for longer.<sup>10</sup> Under the second model, tech companies are required to empower parents by giving them the tools to monitor their kids (the Parent Gatekeeper Model). For example, these laws may provide that minors cannot use social media unless their parent consents.<sup>11</sup> Some legislatures choose one model over another, while some create a hybrid of both models, leaning more toward one or the other.<sup>12</sup>

This Article argues that the Tech Liability Model, which directly regulates tech platforms and places them as the gatekeepers, is essential to successfully regulate addictive technologies and reduce kids' screen time. Further, this Article advocates that hybrid laws could also be highly effective, as long as legislatures provide parents with gatekeeping powers simultaneously with or after implementing comprehensive protections under the Tech Liability Model.

The Article cautions, however, that while tech companies prefer to ward off regulation altogether, if forced to choose between the two models, they would opt for the Parent Gatekeeper Model. The tech industry prefers the Parent Gatekeeper Model because placing responsibility on parents shifts it away from them. By opting for the Parent Gatekeeper

---

6. See, e.g., Tim Bernard, *144 State Bills Aim to Secure Child Online Safety as Congress Flounders*, TECH POL'Y PRESS (May 22, 2023), <https://www.techpolicy.press/144-state-bills-aim-to-secure-child-online-safety-as-congress-flounders/> [https://perma.cc/VK67-6Y3K] (summarizing state laws and bills in mid-2023).

7. See *NetChoice, LLC v. Bonta*, 113 F.4th 1101 (9th Cir. 2024).

8. See Zephyr Teachout, *In Techno Parentis: Teens, Social Media, and the First Amendment 15–29* (July 2024) (unpublished manuscript) (on file with author) (providing a different classification of the laws).

9. See *infra* Part II.

10. See, e.g., Kids Online Safety and Privacy Act, S. 2073, 118th Cong. § 3 (2023); UTAH CODE ANN. § 13-71-202 (West 2024).

11. See, e.g., LA. STAT. ANN. § 51:1752(b) (2024); H.B. 3, 2024 Leg., §§ 2–3 (Fla. 2024).

12. See *infra* Part II.

Model, they resort to a familiar strategy of placing the responsibility on the consumer. Furthermore, the tech industry knows from experience that parents are ineffective gatekeepers and kids will remain online garnering profits for tech companies. The Parent Gatekeeper Model relies on parental consent as a main tool. Years of attempting to regulate privacy online through consent, coupled with extensive use of parental controls to contain kids' screen time, reveals that parent gatekeeping laws standing alone are likely to fail. Kids hooked on social media, games, and devices usually persist as parents fatigue from constant requests, arguments, and family discord, topped by complicated consent and control mechanisms, often give up.<sup>13</sup>

The Article also warns that legislatures should use the Parent Gatekeeping Model cautiously as a stand-alone model because it creates an unnecessary and illusory conflict between reducing kids' screen time and protecting their privacy interests. It explains that the conflict is illusory for the following reasons. First, the Parent Gatekeeper Model relies on granting parents' rights to consent, as well as supervisory powers over their kids' online activity. By tying age to the identity of a specific child, the Parent Gatekeeper Model enflamed the age verification debate. Opponents argued that age verification techniques inherently violate the privacy of both children and adults.<sup>14</sup> Yet, new advances in age verification techniques show age verification is not inherently privacy threatening. Furthermore, age gating is already implemented online and offline for different purposes. Finally, the Tech Liability Model does not impose the same stringent requirements of tying age to a specific identity and thereby alleviates any remaining concerns.<sup>15</sup>

Second, some laws under the Parent Gatekeeper Model, specifically those granting parents access to teens' communications and the identity of those they communicate with,<sup>16</sup> raise concerns regarding the privacy interests of these older minors. Kids always revered the privacy of their communications with peers growing up. Granting parents access to adolescent explorations destabilizes long-held expectations of privacy. Family law scholars are increasingly emphasizing the importance of older kids' privacy rights against their parents to autonomously develop their identities.<sup>17</sup>

The Article then proceeds to argue that the goals of containing tech addiction and the objective of protecting privacy are not at odds.

---

13. *See infra* Section III.B.

14. *See, e.g.*, Jason Kelley & Adam Schwartz, *Age Verification Mandates Would Undermine Anonymity Online*, ELEC. FRONTIER FOUND. (Mar. 10, 2023), <https://www.eff.org/deeplinks/2023/03/age-verification-mandates-would-undermine-anonymity-online> [<https://perma.cc/U4RD-UP27>].

15. *See infra* Section III.C.1.

16. *See, e.g.*, Utah Social Media Regulation Act, 2023 Utah Laws 498, *repealed by* Utah Minor Protection in Social Media Act, 2024 Utah Laws 224; Utah Minor Protection in Social Media Act, UTAH CODE ANN. § 13-71-203 (West 2024).

17. *See infra* Section III.C.2.

In fact, the Article argues these goals are harmonious and legislatures can promote them both through well-drafted laws. It explains that the collection of data and the extension of user time online are part of the same business model. Under this business model, tech companies give many products away for free. For example, they provide Gmail and Instagram accounts for free. Instead of relying on user fees, they rely on ads to generate revenues. But to accumulate revenues, tech companies seek to keep users online for as long as possible so they can collect more data on them. They use this data to create targeted ads that advertise the products they are most likely to purchase. Tech companies again need to keep users online for as long as possible so they will see the ads. Laws protecting privacy by restricting the collection of data or containing tech addiction by limiting time online would reduce the effectiveness of the business model. This would make it less profitable and hence less desirable. At that point, tech companies would reduce their reliance on both user data and time. Thus, since both laws that regulate user time online and laws that protect privacy weaken the same business model, they help accomplish their common objectives.<sup>18</sup>

Finally, while the Article offers that the Tech Liability Model is preferable over the Parent Gatekeeper Model, it supports hybrid models that incorporate parent gatekeeping laws. It proposes, however, that legislatures enact parent gatekeeping laws only simultaneously or after they adopt laws under the Tech Liability model. It particularly cautions that early adoption of broad parent gatekeeping laws could obstruct attempts to add on laws under the Tech Liability Model—in effect, halting progress to resolve the tech addiction problem. Furthermore, prioritizing the Tech Liability Model will likely reduce online harms and the need for parental monitoring will decrease. This will open the door for narrowly tailored parental gatekeeping laws that provide parents options for monitoring, while minimizing encroachment of privacy interests of older minors.<sup>19</sup>

This Article proceeds as follows. Part I describes the youth technology addiction crisis, its impact, its causes, and the legal movement, which is battling to contain it. Part II describes the two main regulatory models: the Tech Liability Model and the Parent Gatekeeping Model, the types of laws they incorporate, and provides examples of hybrid choices. Part III argues that the Tech Liability Model is superior in accomplishing the goal of regulating addictive technologies, describes potential privacy issues related to laws implemented under the Parent Gatekeeper Model, and underscores the ultimate synergies between privacy protection and limiting kids time online. Part IV describes how legislatures can effectively integrate parental gatekeeping laws with laws that directly regulate tech platforms under the Tech Liability Model.

---

18. *See infra* Section III.C.3.

19. *See infra* Part IV.

## I. THE TECHNOLOGY ADDICTION CRISIS

A. *Time, Kids, and Public Health*

Many, particularly kids, spend many of their waking hours on screens.<sup>20</sup> Teens spend an average of eight and a half hours on screens (not including time dedicated to school work).<sup>21</sup> Half of teens say they are nearly “constantly online.”<sup>22</sup> This phenomenon started around 2009 when the smartphone and social networks became popular.<sup>23</sup> Smartphones gave people the ability to take online communications anywhere, while social networks replaced many in-person interactions, especially for teens.

The science wars regarding the impact of screen time—particularly social media, games, and smartphone use—on kids have been ongoing for more than a decade.<sup>24</sup> While adults are affected as well, the strongest evidence points to the impact on kids, specifically addiction,<sup>25</sup> cognitive development problems,<sup>26</sup> mental health issues (including depression,

20. For example, one 2024 survey finds that the average screen time in the U.S. is around seven hours. *Revealing Average Screen Time Statistics*, BACKLINKO, <https://backlinko.com/screen-time-statistics> [<https://perma.cc/7VSJ-WRRM>] (Mar. 11, 2024).

21. RIDEOUT, PEEBLES, MANN & ROBB, *supra* note 1, at 1, 15.

22. *Teens and Internet Device Access Sheet*, PEW RSCH. CTR. (Jan. 5, 2024), <https://www.pewresearch.org/internet/fact-sheet/teens-and-internet-device-access-fact-sheet/> [<https://perma.cc/DLF4-MKR2>] (reporting that 46% of teens report being almost constantly online).

23. Josh Boyd, *The History of Facebook: From BASIC to Global Giant*, BRANDWATCH (Jan. 25, 2019), <https://www.brandwatch.com/blog/history-of-facebook/> [<https://perma.cc/NLM8-6HHP>]; Susannah Fox & Lee Rainie, *The Web at 25 in the U.S.*, PEW RSCH. CTR. (Feb. 27, 2014), <https://www.pewresearch.org/internet/2014/02/27/the-web-at-25-in-the-u-s/> [<https://perma.cc/8J8Q-WXNP>]; Chris Quick, *With Smartphone Adoption on the Rise, Opportunity for Marketers Is Calling*, NIELSEN (Sept. 2009), <https://www.nielsen.com/us/en/insights/article/2009/with-smartphone-adoption-on-the-rise-opportunity-for-marketers-is-calling/> [<https://perma.cc/RBW3-KMWT>].

24. See BERNSTEIN, *supra* note 2, at 26–28 (explaining that science wars erupt when scientific evidence suggests that corporate action causes consumer harm, and corporate entities fight this evidence with their own cadre of studies).

25. *Id.* at 16–20. The World Health Organization included “Gaming Disorder” as a disorder. *Inclusion of “Gaming Disorder” in ICD-11*, WORLD HEALTH ORG. (Sept. 14, 2018), <https://www.who.int/news/item/14-09-2018-inclusion-of-gaming-disorder-in-icd-11> [<https://perma.cc/MYD9-N79T>].

26. BERNSTEIN, *supra* note 2, at 6–20, 22–24. For examples of specific studies, see Sheri Madigan, Dillon Browne, Nicole Racine, Camille Mori & Suzanne Tough, *Association Between Screen Time and Children’s Performance on a Developmental Screening Test*, 173 JAMA PEDIATRICS 244 (2019); John S. Hutton, Jonathan Dudley, Tzipi Horowitz-Kraus, Tom DeWitt & Scott K. Holland, *Associations Between Screen-Based Media Use and Brain White Matter Integrity in Preschool-Aged Children*, 174 JAMA PEDIATRICS 1 (2020); Tzipi Horowitz-Kraus & John S. Hutton, *Brain Connectivity in Children Is Increased by the Time They Spend Reading Books and Decreased by the Length of Exposure to Screen-Based Media*, 107 ACTA PAEDIATRICA 685 (2018); Hongmei Wang, Chenwang Jin, Kai Yuan, Tahir Mehmood Shakir, Cuiping Mao, Xuan Niu, Chen Niu, Liping Guo & Ming Zhang, *The Alteration of Gray Matter Volume and Cognitive Control in Adolescents with Internet Gaming Disorder*, 9 FRONTIERS IN BEHAV. NEUROSCIENCE 1 (2015); Martin P. Paulus, Lindsay M. Squeglia, Kara Bagot, Joanna Jacobus,



anxiety and suicide),<sup>27</sup> difficulty focusing,<sup>28</sup> lack of sleep,<sup>29</sup> and social isolation.<sup>30</sup> While the tech industry is continuing to challenge the accumulating data,<sup>31</sup> prominent governmental bodies and associations that evaluate the data have become concerned about the connection between excessive screen time and kids' public health and have raised alerts.<sup>32</sup>

### B. *Addiction by Design*

The public learned that the excessive time spent online was not a coincidence. One by one, whistleblowers emerging from Silicon Valley's largest companies, such as Google and Meta (owner of Facebook and

---

Rayus Kuplicki, Florence J. Breslin, Jerzy Bodurka, Amanda Sheffield Morris, Wesley K. Thompson, Hauke Bartsch & Susan F. Tapert, *Screen Media Activity and Brain Structure in Youth: Evidence for Diverse Structural Correlation Networks from the ABCD Study*, 185 *NEUROIMAGE* 140 (2019).

27. See Haidt, *supra* note 2, at 19–44, 140–72, 173–97; Jean M. Twenge, *Generations: The Real Differences Between Gen Z, Millennials, Gen X, Boomers, and Silents—And What They Mean for America's Future* 392–416 (2023). In addition, studies show that heavy social media use is related to deteriorating mental health in kids. A longitudinal cohort study of U.S. adolescents aged 12–15 (n=6,595) that adjusted for baseline mental health status found that adolescents who spent more than three hours per day on social media faced double the risk of experiencing poor mental health outcomes, including symptoms of depression and anxiety. OFF. OF THE SURGEON GEN., *Social Media and Youth Mental Health* 6 (2023) (citing Kira E. Riehm, Kenneth A. Feder, Kayla N. Tormohlen, Rosa M. Crum, Andrea S. Young, Kerry M. Green, Lauren R. Pacek, Lareina N. La Flair & Ramin Mojtabai, *Associations Between Time Spent Using Social Media and Internalizing and Externalizing Problems Among US Youth*, 76 *JAMA PSYCHIATRY* 1266–73 (2019)), <https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf> [<https://perma.cc/F6AS-TAUP>]; see also Matthew B. Lawrence, *Public Health Law's Digital Frontier: Addictive Design, Section 230, and the Freedom of Speech*, 4 *J. FREE SPEECH L.* 299, 308–12 (2023) (discussing public health concerns).

28. See Mark, *supra* note 2, at 221–41.

29. See generally Kids Online Health and Safety Task Force, *Online Health and Safety for Children and Youth: Best Practices for Families and Guidance for Industry* 10–12 (2024), <https://www.ntia.gov/sites/default/files/reports/kids-online-health-safety/2024-kohs-report.pdf> [<https://perma.cc/ETS9-WTUP>].

30. Adolescents and young adults in 2019 (even before the pandemic) spent twenty-five minutes less a day socializing in person with others than those in 2012. Twenge, *supra* note 27, at 409–10 fig. 6.46. That translates to three hours a week, thirteen hours a month, and 152 hours a year less in the company of others. *Id.*

31. See, e.g., Kate Gibson, *Mark Zuckerberg Accused of Having "Blood on His Hands" in Fiery Senate Hearing on Internet Child Safety*, CBS NEWS, <https://www.cbsnews.com/news/mark-zuckerberg-meta-x-child-exploitation/> [<https://perma.cc/55NH-MKQB>] (Jan 31, 2024, 7:57 PM) (reporting that Meta's founder and CEO, Mark Zuckerberg, testified in congressional hearings and repeatedly refuted a link between Facebook and teen mental health).

32. See Kids Online Health and Safety Task Force, *supra* note 29, at 10–12; OFF. OF THE SURGEON GEN., *supra* note 27, at 6–12; AM. PSYCH. ASS'N, *Health Advisory on Social Media Use in Adolescence* (2023), <https://www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use.pdf> [<https://perma.cc/KMW5-GAYZ>]; AM. PSYCH. ASS'N, *Potential Risks of Content, Features, and Functions* (2024), <https://www.apa.org/topics/social-media-internet/psychological-science-behind-youth-social-media.pdf> [<https://perma.cc/3KMH-GUXH>].

Instagram), revealed that the tech industry manipulates users to spend as much time as possible on screens.<sup>33</sup> As the Article explains in detail in Section III.C, extending users' time online is part of the tech industry's business model and is closely tied to its revenues. To meet their revenue goals, and keep users online, tech companies harp on human psychological vulnerabilities through different strategies.<sup>34</sup> They apply these strategies to devices ranging from computers to tablets and smartphones. They use them on a wide array of internet platforms, including social media, games, dating apps, and entertainment websites.

Examples are plentiful. Social media companies use algorithms that prolong kids time online by exposing them to harmful and hate-invoking content.<sup>35</sup> Many tech platforms and devices use designs based on the intermittent reward model. Psychologists found that when people receive rewards, whether money, food, or social approval, on an unpredictable schedule, their brains release dopamine—a pleasure-enhancing neurotransmitter.<sup>36</sup> Tech companies apply insights from this model to different online designs to entice users to stay on for longer. For example, notifications are an intermittent reward. Users hearing their phones beep or seeing the notification across their screen, repeatedly pick up their phones to find out what happened—hoping for a socially enhancing reward. The “pull to refresh” design also implements this model. Users pull to refresh Facebook or Instagram to check if they got new reactions to their post or to check if someone they are interested in has posted something new. They repeatedly pull to refresh, hoping for a

---

33. See Gaia Bernstein, *A Window of Opportunity to Regulate Addictive Technologies*, 2022 WIS. L. REV. FORWARD 64, 68–69; Dara Kerr, *Meta Failed to Address Harm to Teens, Whistleblower Testifies as Senators Vow Action*, NPR (Nov. 7, 2023, 6:53 PM), <https://www.npr.org/2023/11/07/1211339737/meta-failed-to-address-harm-to-teens-whistleblower-testifies-as-senators-vow-act> [<https://perma.cc/68KV-TPJR>]; Bianca Bosker, *The Binge Breaker*, THE ATLANTIC (Nov. 2016), <https://www.theatlantic.com/magazine/archive/2016/11/the-binge-breaker/501122/> [<https://perma.cc/884Z-LK7J>]; THE SOCIAL DILEMMA (Netflix 2020); Victor Ordonez, *Key Takeaways from Facebook Whistleblower Frances Haugen's Senate Testimony*, ABC NEWS (Oct. 5, 2021, 4:47 PM), <https://abcnews.go.com/Politics/key-takeaways-facebook-whistleblower-frances-haugens-senate-testimony/story?id=80419357> [<https://perma.cc/B2D2-MBLS>]; *Former Meta Executive Testifies on Social Media and Youth Mental Health*, C-SPAN (Nov. 7, 2023), <https://www.c-span.org/video/?531650-1/meta-executive-testifies-social-media-youth-mental-health#> [<https://perma.cc/S6C9-H4GU>]; Justin Hendrix, *Transcript: Senate Hearing on Social Media and Teen Mental Health with Former Facebook Engineer Arturo Bejar*, TECH POL'Y PRESS (Nov. 8, 2023), <https://www.tech-policy.press/transcript-senate-hearing-on-social-media-and-teen-mental-health-with-former-facebook-engineer-arturo-bejar/> [<https://perma.cc/9BQL-Q6WV>].

34. Daniel Susser, Beate Roessler & Helen Nissenbaum, *Technology, Autonomy, and Manipulation*, 8 INTERNET POL'Y REV. (SPECIAL ISSUE) 1 (2019).

35. See, e.g., *Protecting Kids Online: Testimony from a Facebook Whistleblower Before the Sub-Comm. on Consumer Prot., Prod. Safety, and Data Sec.*, 117th Cong. (2021) (statement of Frances Haugen, former employee of Facebook).

36. NATASHA DOW SCHUL, *ADDICTION BY DESIGN: MACHINE GAMBLING IN LAS VEGAS* (2014); Michael D. Zeiler, *Fixed-Interval Behavior: Effects of Percentage Reinforcement*, 17 J. EXPERIMENTAL ANALYSIS BEHAV. 177 (1972).

reward. Tinder uses swipes in a similar way. Users keep swiping, and sometimes they get a dating match—a reward.<sup>37</sup>

### C. *Reaction to the Tech Addiction Crisis*

Awareness of the problem of tech addiction and some attempts to address it emerged before the pandemic. But during the pandemic, particularly during lockdown, when life happened mostly on screens, the timing was unsuitable for a movement against technology addiction to emerge. Technology was the crutch of life then.<sup>38</sup> When the pandemic ended and scientific data accumulated on the harms of excessive screen time, especially for kids,<sup>39</sup> legal action took off through different avenues. Parents brought class action cases against social media companies and game manufacturers for addicting their kids.<sup>40</sup> A large group of attorneys general sued Meta for addicting kids.<sup>41</sup> Many school districts sued social networks for the costs of treating kids' mental health caused by excessive time online.<sup>42</sup> But action was not contained to litigation. A boom of legislation aimed at protecting kids from online harms generally, and technology addiction specifically, swept many states as well as Congress.<sup>43</sup>

## II. LEGISLATIVE MODELS TO REGULATE ADDICTIVE TECHNOLOGIES

The movement to contain kids' excessive screen time invests substantially in legislation. In recent years, many states and Congress (as well as jurisdictions outside the United States) proposed bills and enacted laws to protect kids from excessive screen time and other online harms.<sup>44</sup> The legislative landscape to contain kids' exposure to addictive technologies<sup>45</sup>

---

37. See ADAM ALTER, *IRRESISTIBLE: THE RISE OF ADDICTIVE TECHNOLOGY AND THE BUSINESS OF KEEPING US HOOKED* 76–77 (2017); Tristan Harris, *How Technology Is Hijacking Your Mind—from a Magician and Google Design Ethicist*, MEDIUM (May 18, 2016), <https://medium.com/thrive-global/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3> [<https://perma.cc/NLB6-LTFZ>].

38. BERNSTEIN, *supra* note 2, at 13–14.

39. See *supra* Section I.A.

40. See, e.g., Complaint for Personal Injuries, *Alexis v. Meta Platforms, Inc.*, No. 22-cv-03294 (N.D. Cal. June 6, 2022), 2022 WL 2101825.

41. Complaint for Injunctive and Other Relief, *California v. Meta Platforms, Inc.*, No. 23-cv-05448 (N.D. Cal. Oct. 24, 2023).

42. See, e.g., Complaint, *Seattle Sch. Dist. No. 1 v. Meta Platforms, Inc.*, No. 23-cv-00032 (W.D. Wash. Jan. 6, 2023), 2023 WL 1794885; Complaint, *Sch. Dist. of the Chathams v. Meta Platforms, Inc.*, No. 23-cv-00910 (D.N.J. Feb. 16, 2023), 2023 WL 2117905.

43. See, e.g., Bernard, *supra* note 6 (summarizing state laws and bills in mid-2023); Kids Online Safety and Privacy Act, S. 2073, 118th Cong. (2023).

44. Bernard, *supra* note 6 (summarizing state laws and bills in mid-2023); S. 2073.

45. Although the focus of this Article is on technologies that extend user time online, I include laws that target other harms because companies use algorithms that expose kids to harms, like suicide or eating disorder information, to prolong

is in flux.<sup>46</sup> Some approaches focus on social media, and some focus on online providers more broadly, including games, the metaverse, and educational programs.<sup>47</sup> While laws rely on a broad array of mechanisms to accomplish their goal, this Article identifies two overarching models. The first model makes tech companies directly responsible to ensure their products are not designed to keep kids online and are safe for kids (the Tech Liability Model). The second model makes parents responsible, giving them rights to monitor and protect their kids (the Parent Gatekeeper Model). To shift the responsibility to parents, these laws require tech companies to provide parents with tools that will allow them to restrict their kids' time and activities online. This Part will describe which laws fall under each model and under a hybrid model.

#### A. *The Tech Liability Model*

Under the Tech Liability Model, laws require tech companies to undertake measures and/or incur liability that would limit kids' time online and prevent related harms. These laws use one or more of the following mechanisms:

- Imposing a duty of care on technology platforms by requiring them to exercise reasonable care when creating or implementing design features to prevent harms to minors. Listed harms include compulsive use, anxiety, depression, eating disorders, substance use disorders, and suicidal behaviors.<sup>48</sup>
- Imposing a fiduciary duty of loyalty on technology platforms to act in the best interest of children, even when these interests conflict with their commercial interests.<sup>49</sup>

---

their time online. Therefore, these laws, indirectly, alleviate the technology addiction problem. *See, e.g.,* C-SPAN, *Facebook Whistleblower Frances Haugen Testifies Before Senate Commerce Committee*, YouTube (Oct. 5, 2021), [https://www.youtube.com/live/GOnpVQnv5Cw?si=Sf-7hnJh19EI\\_Y3V](https://www.youtube.com/live/GOnpVQnv5Cw?si=Sf-7hnJh19EI_Y3V) (Frances Haugen's testimony tying time spent online to other harms).

46. Utah Social Media Regulation Act, 2023 Utah Laws 477, *repealed by* Utah Minor Protection in Social Media Act, 2024 Utah Laws 224; California Age-Appropriate Design Code Act, CAL. CIV. CODE § 1798.99.28 (West 2022), *invalidated by* Netchoice, LLC v. Bonta, 692 F. Supp. 3d 924 (N.D. Cal. 2023), *aff'd in part and vacated in part* 113 F.4th 1101 (9th Cir. 2024).

47. For laws regulating online providers beyond social networks, see CAL. CIV. CODE § 1798.99.29 (applying to any online service, product, or feature likely to be accessed by children); Securing Children Online Through Parental Empowerment (SCOPE) Act, TEX. BUS. & COM. CODE ANN. § 509.002 (2024) (expanding beyond social networks to the metaverse, games, and some educational programs).

48. *See, e.g.,* S. 2073 § 3. Another variation, though more specific than the duty of care, requires technology platforms to create a "strategy" that is designed to prevent exposure to content, which promotes harms including suicide, self-harm, eating disorders, substance abuse, and bullying. *See, e.g.,* TEX. BUS. & COM. CODE ANN. § 509.053.

49. *See, e.g.,* INFO. COMM'R'S OFF., AGE APPROPRIATE DESIGN: A CODE OF PRACTICE FOR ONLINE SERVICES (2022), <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and>

- Requiring technology platforms to undertake internal risk assessment reports<sup>50</sup> or independent, third-party audits, and issue transparency reports detailing foreseeable risks to minors, as well as specifying their attempts to mitigate these risks.<sup>51</sup>
- Requiring technology platforms to limit use of design features that increase the amount of time that minors spend on their platforms. These include the infinite scrolling, autoplay, rewarding time spent on the platform, push notifications, algorithmic personalized recommendations, and in-game purchases.<sup>52</sup>
- Requiring social media companies to ban minors from holding an account.<sup>53</sup>
- Requiring technology platforms to provide their algorithms (that may be used to prolong time online) to independent security researchers.<sup>54</sup>
- Requiring tech companies to turn on the highest privacy and safety settings by default for minors, and to permit minors to limit or opt out of features like personalized algorithmic recommendations.<sup>55</sup>

#### B. *The Parent Gatekeeper Model*

Under the Parent Gatekeeper Model, laws give parents rights to monitor their kids' online activity to limit their time and protect them from harm. To implement these rights, the laws require tech companies to give parents the tools to do so. These laws use the following mechanisms to ultimately place the responsibility on parents:<sup>56</sup>

- Requiring parental consent for minors to use social network platforms and/or other online platforms, such as online games. Laws require parental consent for minors ranging from fourteen to eighteen years old.<sup>57</sup>

---

resources/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf [https://perma.cc/2WA9-BNEH]; CAL. CIV. CODE § 1798; *see also* Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. 11, 14–15 (2000) (discussing the different duties).

50. *See, e.g.*, INFO. COMM'R'S OFF, *supra* note 49, at 86; CAL. CIV. CODE § 1798.99.28.

51. *See, e.g.*, S. 2073.

52. *See, e.g.*, S. 2073 § 3; UTAH CODE ANN. § 13-71-202 (West 2024).

53. *See, e.g.*, H.B. 3, 2024 Leg., §§ 2–3 (Fla. 2024); FLA. STAT. ANN. §§ 501.1737–501.1738 (2025).

54. TEX. BUS. & COM. CODE ANN. § 509.053 (2024).

55. S. 2073 § 7.

56. This Article focuses on laws that give parents tools to monitor and protect their kids online. It does not cover laws that give private rights of action to parents to sue technology platforms. *See, e.g.*, H.B. 464, 65th Gen. Assemb., Reg. Sess. (Utah 2024).

57. *See, e.g.*, S.B. 396, 94th Gen. Assemb., Reg. Sess. (Ark. 2023); NetChoice, LLC v. Griffin, No. 23-CV-05105, 2023 WL 5660155 (W.D. Ark. Aug. 31, 2023)

- Requiring technology platforms to allow parents to supervise minors accounts, including placing time limits and scheduling breaks on their kids' accounts.<sup>58</sup>
- Requiring tech companies to implement technology that will notify parents if their kids are at risk of suicide, eating disorders, substance abuse, sexual abuse, child pornography, anxiety, academic dishonesty, or fraud.<sup>59</sup>

### C. *Hybrid Laws*

Some laws incorporate both the Direct Liability Model and the Parent Gatekeeper Model by imposing responsibility directly on the technology platforms and on parents. The following are examples of these hybrid laws:

- Requiring online platforms to prevent younger minors from becoming account holders, while requiring parental consent for older minors.<sup>60</sup>
- Requiring parental consent and/or parental supervisory options as well as imposing direct prohibitions on technology platforms on using targeted advertising and designs that extend time or lead to harmful content, and imposing requirements that platforms disclose their algorithms.<sup>61</sup>
- Requiring parental consent for a minor to change enhanced default privacy settings or other features like algorithmic feed.<sup>62</sup>

---

(issuing a preliminary injunction against S.B. 396); LA. STAT. ANN. § 51:1752(b) (2024); Fla. H.B. 3 §§ 2–3.

58. *See, e.g.*, LA. STAT. ANN. § 51:1754 (requiring a social media company to permit a parent to supervise the minor's account, including to view privacy settings, set daily time limits, schedule breaks, and offer the minor the option to set up parental notifications when the minor reports a person or issue); TEX. BUS. & COM. CODE ANN. § 509.054 (requiring the digital service to install controls that allow a parent to "supervise" the minor's account through tools that enable the verified parent to control "privacy and account settings," limit access time, and restrict the known minor's purchases or other financial transactions through the digital service).

59. *See* Sammy's Law, H.R. 5778, 118th Cong. § 4(f) (2024); Parental Digital Choice Act (Sammy's Law), H.B. 5380, 103rd Assemb. (Ill. 2024); Let Parents Choose Protection Act (Sammy's Law of 2024), S.B. 1444, 2023-2024 Reg. Sess. (Cal. 2024); Let Parents Choose Act (Sammy's Law of 2024), H.B. 773, 2023-2024 Reg. Sess. (N.C. 2023).

60. Fla. H.B. 3 § 1 (prohibiting minors under 14 from having a social media account while requiring parental consent for older minors).

61. *See, e.g.*, LA. STAT. ANN. § 51:1752(b) (requiring parental consent); LA. STAT. ANN. § 51:1753 (prohibiting advertising to minor accounts); TEX. BUS. & COM. CODE ANN. §§ 509.053–509.054 (restricting design that leads to harmful content, requiring disclosure of algorithms, and requiring providing parents with supervisory options).

62. *See, e.g.*, N.Y GEN. BUS. LAW §§ 1500–1508 (McKinney 2024).

### III. THE VULNERABILITIES OF THE PARENT GATEKEEPER MODEL

The tech industry has launched a campaign to invalidate laws seeking to protect kids from tech addiction and other online harms, primarily on First Amendment grounds.<sup>63</sup> I address the First Amendment issue elsewhere and argue that these laws do not, in fact, violate the First Amendment.<sup>64</sup> This Article goes beyond the First Amendment debate to highlight the important choice legislatures make when selecting between the Tech Liability Model and the Parent Gatekeeper Model.

This Part underscores the vulnerabilities of the Parent Gatekeeper Model. It argues that tech companies prefer the Parent Gatekeeper Model for two reasons. First, it allows them to use an old playbook strategy, adopted from the tobacco industry, of shifting responsibility from them to the users—in this case, from the tech industry to the parents. Second, parents are ineffective gatekeepers. Years of experimentation with parental controls and consent models online demonstrate this. Parental fatigue resulting from kids' persistence to gain screen access and ensuing family discord, combined with tech complexity, usually defeat parents' best intentions. Consequently, kids' time online continues to escalate. This Part then argues that parent gatekeeping laws instigated reactions that created an illusory conflict between the goals of protecting kids' privacy and containing tech addiction, while the opposite is in fact true. Protecting privacy and limiting kids' time online are harmonious goals—accomplishing one helps achieve the other by weakening the tech industry's business model that relies on time and data as its resource.

#### A. *Shifting the Blame—an Old Tactic*

Placing the parent as a gatekeeper shifts responsibility to the user. In this case, since the user is a minor, to its proxy—the parent. The strategy of shifting responsibility from industry to consumer is not new. Historically, industries reacted to accusations that their product is harmful by resorting to the tactic of blaming consumers for the harm. They used the dogmas of personal choice and personal responsibility.<sup>65</sup> For example, when smokers sued the tobacco industry, cigarette companies argued that smokers chose to smoke and, therefore, they were responsible for the health consequences. For decades, the tobacco industry prevailed in court.<sup>66</sup> Similarly, when a group of teenagers who ate at McDonald's

63. See, e.g., *NetChoice, LLC v. Bonta*, 113 F.4th 1101 (9th Cir. 2024).

64. Gaia Bernstein, Opinion, *California Is Right: Addictive Tech Design Is Not Free Speech*, THE HILL (Oct. 24, 2023, 12:00 PM), <https://thehill.com/opinion/technology/4270910-california-is-right-addictive-tech-design-is-not-free-speech/> [<https://perma.cc/A9RP-CTFM>]; Brief for Amici Curiae Design Scholars as Amici Curiae Supporting Defendant-Appellant, *NetChoice v. Bonta*, 113 F.4th 1101 (9th Cir. 2024) (No. 23-2969).

65. BERNSTEIN, *supra* note 2, at 47–49, 97–99.

66. *Lartigue v. R.J. Reynolds Tobacco Co.*, 317 F.2d 19, 22 (5th Cir. 1963); *Horton v. Am. Tobacco Co.*, 667 So. 2d 1289, 1289–91 (Miss. 1995); *Cipollone v. Liggett*

daily sued McDonald's for their health problems, including obesity and diabetes, McDonald's argued that the kids chose to eat at McDonald's and, therefore, they are responsible for their health problems. The New York court accepted the argument.<sup>67</sup>

The tech industry has already followed suit. Online game makers fighting against the World Health Organization's move to classify internet gaming as a disorder used the same argument. Game makers also utilized it when defending against lawsuits involving loot boxes (a common addictive game feature). In both cases, they argued that the gamers chose to play, and they or their parents are responsible for their addiction.<sup>68</sup> The tech industry then proceeded to take the strategy a step further. It created digital well-being tools for its users.

They promoted tools for users of all ages. For example, Apple provided iPhone users with Screen Time reports that let them know how much time they spend on their device. Instagram gave its users the option to set alerts to remind themselves how much they spent on the social network. By creating these tools, the tech industry indirectly made the same argument. They basically claimed that since they gave their users tools that let them control how much time they spend online, the users are responsible if they spend excessive time on their screens.<sup>69</sup> Tech companies also made a special category of well-being tools for parents. These tools are known as parental controls. Parental controls come in two main forms: device controls and platform controls. Device controls often limit time and access on phones or computers while platform controls allow parents to set notifications or time limits on specific platforms, such as social media accounts.<sup>70</sup>

Tech companies used their digital well-being tools, particularly parental controls, to ward off regulation. They attempted to show the world that they can self-regulate by solving the problem themselves through technological measures.<sup>71</sup> Once again, this move was not innovative. The tobacco industry also provided their users with tools to ward off blame and regulation. When studies found that cigarettes are addictive, the tobacco industry came out with the perfect solution: the filtered

---

Grp., Inc., 693 F. Supp. 208 (D.N.J. 1988) (assigning 20% of cause to the tobacco company, but New Jersey law did not allow for damages without 50% liability), *aff'd in part, rev'd in part*, Cipollone v. Liggett Grp., Inc., 893 F.2d 541 (3d Cir. 1990).

67. *Pelman v. McDonald's Corp.*, 237 F. Supp. 2d 512, 512–33 (S.D.N.Y. 2003).

68. BERNSTEIN, *supra* note 2, at 97.

69. *Id.* at 41–43.

70. *Use Parental Controls on Your Child's iPhone and iPad*, APPLE INC. (Dec. 11, 2024), <https://support.apple.com/en-us/105121> [<https://perma.cc/6G68-5DVD>]; *Family Privacy Disclosure for Children*, APPLE INC., <https://www.apple.com/legal/privacy/en-ww/parent-disclosure/> [<https://perma.cc/4DTY-UL3V>] (last visited Jan. 5, 2025); *For Parents: Helping Your Teen Navigate Instagram Safely*, META PLATFORMS INC., <https://about.instagram.com/community/parents> [<https://perma.cc/LPJ4-BEK4>] (last visited Jan. 5, 2025).

71. BERNSTEIN, *supra* note 2, at 102–04.



cigarette. They advertised the filtered cigarette, which was as harmful as the unfiltered cigarette, as “just what the doctor prescribed.”<sup>72</sup>

For the tech industry, promoting parental controls could only delay the inevitable. As discussed in Part II, federal and state lawmakers eventually advanced multiple laws to protect kids from addictive technologies. While the tech industry hoped to ward off regulation altogether, it preferred the Parent Gatekeeper Model over the Direct Liability Model.<sup>73</sup> For the tech industry, parental gatekeeping laws serve a similar role as parental controls. By giving parents consent or supervisory options, they shift responsibility from the tech companies to parents. True, under these laws, tech companies need to provide parents with the tools, but parental controls already provided many of these options. Parental gatekeeping laws are the lesser evil for tech companies. Not only do they shift responsibility from companies to parents, but once they are in place, the tech industry can argue that laws imposing direct liability on tech companies are unnecessary. They can insist there is no need for direct liability laws because parents can provide protection from online harms. Furthermore, and importantly, as discussed in the next section, tech companies know that parental gatekeeping laws are unlikely to be effective.

#### B. *An Ineffective Gatekeeper*

Why are parents unlikely to be effective gatekeepers? The Parent Gatekeeper Model relies primarily on parental consent. But user consent carries its own set of problems. Privacy law for years implemented user consent as a protective measure. Many scholars wrote about the ineffectiveness of online consent.<sup>74</sup> They showed that consent online

---

72. RICHARD KLUGER, *ASHES TO ASHES: AMERICA'S HUNDRED-YEAR CIGARETTE WAR, THE PUBLIC HEALTH AND THE UNABASHED TRIUMPH OF PHILIP MORRIS* 153, 188 (2010).

73. Meta's post on its blog is an example. See e.g., Antigone Davis, *Parenting in a Digital World Is Hard. Congress Can Make It Easier*, META PLATFORMS INC. (NOV. 15, 2023), <https://about.fb.com/news/2023/11/online-teen-safety-legislation-is-needed/> [<https://perma.cc/P3QK-VYP9>] (“Parents should approve their teen's app downloads, and we support federal legislation that requires app stores to get parents' approval whenever their teens under 16 download apps.”).

74. See generally Daniel J. Solove, *Murky Consent: An Approach to the Fiction of Consent in Privacy Law*, 104 B.U. L. REV. 593 (2024) (arguing that both the United States' notice and choice approach and the European Union's active consent approach under the General Data Protection Regulation (GDPR) do not work); Stacy-Ann Elvy, Response, *Privacy Law's Consent Conundrum*, 104 B.U. L. REV. 641 (2024) (responding to Solove's *Murky Consent* article); Zahra Takhshid, *Children's Digital Privacy and the Case Against Parental Consent*, 101 TEX. L. REV. 1417, 1420–22, 1426 (2021) (arguing that parental consent is ineffective in the online education market (EdTech), which highlights the unsuitability of the Children's Online Privacy and Protection Act (COPAA) solutions to today's internet); see also Jon M. Garon, *To Be Seen but Not Heard: How the Internet's Negative Impact on Minor's Constitutional Right to Privacy, Speech, and Autonomy Creates a Need for Empathy-By-Design*, 73 MERCER L. REV. 463 (2022) (discussing the problem of parental consent and kids rights online). But see Katharine B. Silbaugh & Adi Caplan-Bricker, *Regulating Social Media Through Family Law* (Bos. Univ. Sch. of L. Rsch. Paper Series, Working Paper No. 24-6, 2024), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4753061](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4753061) [<https://perma.cc/P3QK-VYP9>].

does not work because few people read the terms they consent to.<sup>75</sup> They also underscored that users' decisions to consent are often manipulated.<sup>76</sup> Finally, privacy scholars report that users experience consent fatigue from multiple requests to consent and end up granting consent to make these requests go away.<sup>77</sup>

Parents are likely to experience the usual online consent problems. They are less likely to read the details of what they consent to when the set of options becomes more complex. In these instances, tech companies could manipulate them more easily. Specifically, a parent who needs to decide whether to consent to complicated privacy default options is more likely to fall prey to manipulation than a parent asked to consent to opening a social media account for their kid.<sup>78</sup>

Parents' experience with parental controls underscores the difficulty. Parents find it hard to keep up with complicated and ever-changing parental controls.<sup>79</sup> As Section III.C.3 will discuss, tech companies need to generate revenues by keeping kids online for as long as possible. Providing parents with effective and easy to use tools contradicts the technology industry's business model.<sup>80</sup> They have no incentive to provide parents with a simple and stable option of parental controls. And while parents often lack the requisite technological know-how, tech-savvy kids find ways to get around the controls.<sup>81</sup>

---

cc/4TYN-V797] (emphasizing that relying on parental control to regulate kids on social media is in line with other parental rights and is less susceptible to First Amendment challenges).

75. Eric Goldman, *The Crisis of Online Contracts (As Told in 10 Memes)*, 2 NOTRE DAME J. ON EMERGING TECH. 1, 5 (2021) (noting "few consumers actually read online contract terms"); Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEGAL STUD. 1, 1 (2014) ("[O]nly one or two of every 1,000 retail software shoppers access the license agreement and . . . most of those who do access it read no more than a small portion.").

76. See Solove, *supra* note 74, at 610–12; see also Ido Kilovaty, *Legally Cognizable Manipulation*, 34 BERKELEY TECH. L. J. 449, 469 (2019) (arguing that manipulation "deprives individuals of their agency by distorting and perverting the way in which individuals typically make decisions" (footnote omitted)); Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQUIRIES L. 157, 174 (2019) ("Manipulative practices impair the process of choosing, subjecting it to the preferences and influences of a third party, as opposed to those of the individuals themselves.").

77. Solove, *supra* note 74, at 623–27. See generally Ella Corren, *The Consent Burden in Consumer and Digital Markets*, 36 HARV. J.L. & TECH. 551 (2023).

78. If parental consent is required only to change privacy default options, it is less likely to erupt into a conflict in which the parent will eventually give up. See Takhshid, *supra* note 74, at 1420–22 (arguing against relying on parental consent).

79. BERNSTEIN, *supra* note 2, at 103–04; Monica Anderson, Michelle Faverio & Eugenie Park, *How Teens and Parents Approach Screen Time*, PEW RSCH. CTR. (Mar. 11, 2024), <https://www.pewresearch.org/internet/2024/03/11/how-teens-and-parents-approach-screen-time/> [<https://perma.cc/4AD3-KURU>] (noting that about four-in-ten parents say it's hard to manage how much time their teen spends on their phone).

80. See *infra* Section III.C.3.

81. BERNSTEIN, *supra* note 2, at 103–04; Anderson, Faverio & Park, *supra* note 79.

Complexity is a significant challenge to the Parent Gatekeeper Model. But so is parental fatigue and fear of socially isolating one's kids. Professor Matthew Lawrence emphasizes that laws that deputize family members carry costs. He describes the impact on family relationships, the invisibility of the burden, and the gender inequality of its distribution—mainly affecting women.<sup>82</sup> Parents attempted for years to implement parental controls, engaging in endless fights with their kids, and ending up feeling exhausted and powerless. Mothers particularly carried the brunt of the burden.<sup>83</sup> Parents find the fight exhausting and untenable because the problem cannot be solved individually. As long as most kids communicate digitally particularly through social media, parents face an uphill battle. As they struggle, parents also fear that prohibiting their kids' access to phones or social media will result in their isolation. Until norms change collectively for kids, many parents often give up the battle.

Parental gatekeeping laws are likely to exacerbate these problems. Parents lack the time to constantly monitor their kids' screen use, and the added burden of adjusting to unexpectedly long homework assignments and keeping up with constant updates to parental controls often makes effective monitoring infeasible. These laws are unlikely to lead to comprehensive collective change of social norms.<sup>84</sup>

Specifically, some laws under the Parent Gatekeeper Model give parents the right to determine a decision that is of vital importance to kids—whether they can have a social media account. In a world in which most kids are on social networks,<sup>85</sup> kids are unlikely to accept “no” as a long-term answer. The experience of parental controls shows that parents are likely to give up due to fatigue or fear of isolating their child.<sup>86</sup>

---

82. Matthew B. Lawrence, *Deputizing Family: Loved Ones as a Regulatory Tool in the “Drug War” and Beyond*, 11 *NEW ENG. L. REV.* 195, 216–17 (2019).

83. See 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/short-reads/2019/03/22/how-parents-feel-about-and-manage-their-teens-online-behavior-and-screen-time/> [https://perma.cc/JU6B-JHTT] (“[M]others are somewhat more likely than fathers to regularly track what their teen does online . . . .”); Anderson, Faverio & Park, *supra* note 79 (reporting that 38% of teens and parents fight over how much time teens spend online).

84. While grassroot groups like Smartphone Free Childhood are attempting to collectively change social norms, a top down approach that does not rely solely on parents is needed. See SMARTPHONE FREE CHILDHOOD, <https://smartphonefreechildhood.co.uk/> [https://perma.cc/LP4L-MF4H] (last visited Jan. 6, 2025) (a grassroot movement in the United Kingdom); SMARTPHONE FREE CHILDHOOD, <https://www.smartphonefreechildhoodus.com/> [https://perma.cc/TCC7-3YS4] (last visited Jan. 6, 2025) (a grassroot movement in the United States).

85. A 2023 survey found that among thirteen to seventeen-year-old teens, 93% use YouTube, 63% use TikTok, 60% use Snapchat, 59% use Instagram, and 33% use Facebook. Monica Anderson, Michelle Faverio & Jeffrey Gottfried, *Teens, Social Media and Technology 2023*, PEW RSCH. CTR. (Dec. 11, 2023), <https://www.pewresearch.org/internet/2023/12/11/teens-social-media-and-technology-2023/> [https://perma.cc/HMP4-5FZE].

86. See Naomi Nix, *Meta Says Its Parental Controls Protect Kids. But Hardly Anyone Uses Them*, WASH. POST. (Jan. 30, 2024, 8:25 AM), <https://www.washingtonpost.com/technology/2024/01/30/parental-controls-tiktok-instagram-use/> [https://perma.cc/].

Some laws make it a one-time consent decision, and at that point, once the child has joined, the parent can no longer limit their time online.<sup>87</sup> Other laws provide parents with supervisory powers, including limiting time and creating breaks,<sup>88</sup> which could create a fatigue problem on steroids. Kids, addicted to their games, social media networks, and phones, would proceed to request parents to extend their time daily under different pretexts. Parents would eventually extend or eliminate limits to avoid family discord and burnout.<sup>89</sup>

All considered, parental gatekeeping laws are unlikely to fare better than parental monitoring tools. And the data reveals that despite widespread use of parental controls for years,<sup>90</sup> kids' screen time did not go down. Instead, it just kept creeping up.<sup>91</sup> Based on their experience with parental controls, tech companies prefer the Parent Gatekeeper Model, trusting that complexity and fatigue will render them ineffective.

### C. *Creating an Illusionary Conflict Between Privacy and Containing Tech Addiction*

An unexpected mix of privacy advocates, children advocates, as well as the tech industry, reacted to laws incorporating the Parent Gatekeeper Model. Their objections created the appearance of a conflict between regulation to protect kids from tech addiction and their privacy rights. This Part argues that the conflict is illusory for three reasons. First, laws placing parents as gatekeepers of minors under specific ages create hyperbolic concerns about age verification and privacy. It shows that these concerns are largely unfounded in the long-term, that the use of age verification systems is already in place, and furthermore, is needed for

---

cc/G9FP-6U3L]; Anderson, Faverio & Park, *supra* note 79 (38% of teens and parents say they argue about time spent on phone); JoJo Marshall, *When Should You Come Between a Teenager and Their Phone?*, CHILD MIND INST. (Nov. 6, 2023), <https://childmind.org/article/when-should-you-come-between-a-teenager-and-her-phone/#what-happens-when-you-confiscate-that-phone> [<https://perma.cc/UB3Q-TCVY>]; Parul Oh, *I Took Away My Teen's Phone and Here's What Happened*, MOMS OF TWEENS AND TEENS BLOG, <https://momsoftweensandteens.com/i-took-away-my-teens-phone/> [<https://perma.cc/PXX9-Z3W4>] (last visited Jan. 6, 2025).

87. See, e.g., H.B. 3, 2024 Leg., §§ 2–3 (Fla. 2024).

88. See, e.g., SCOPE Act, TEX. BUS. & COM. CODE ANN. § 509.054 (2024).

89. A survey found that teens are more supportive of needing parental consent to create an account (46% support v. 25% oppose) or verifying their age (56% support v. 16% oppose), but less supportive of limiting their time online (34% support v. 36% oppose). Monica Anderson & Michelle Faverio, *81% of U.S. Adults—Versus 46% of Teens—Favor Parental Consent for Minors to Use Social Media*, PEW RSCH. CTR. (Oct. 31, 2023), <https://www.pewresearch.org/short-reads/2023/10/31/81-of-us-adults-versus-46-of-teens-favor-parental-consent-for-minors-to-use-social-media/> [<https://perma.cc/76GZ-9MBG>]. Teens may be less concerned about their ability to convince a parent to grant a one-time consent to open an account but more concerned about the impact of ongoing time limitations.

90. For an example of a 2018 article prescribing parental controls, see Elgersma, *supra* note 4.

91. Duarte, *supra* note 5 (reporting that American teens' screen time has increased by around two hours since 2015).

online gate-fencing beyond regulating addictive technologies. Second, it argues that placing parents as gatekeepers is not only less effective, but also creates privacy concerns threatening kids' privacy vis-à-vis their parents, through both access to information and erosion of autonomy. At the same time, laws that place the responsibility on tech platforms under the Tech Liability Model do not raise such heightened privacy concerns. Third, the Article posits that laws making tech platforms, not parents responsible for preventing kids' tech addiction are, in fact, very much aligned with protecting minors' online privacy. Time online and data collection are part of the same business model. Laws limiting tech platforms' ability to extend kids time online make the whole business model, including data collection, less lucrative and less profitable.

### 1. *The Age-Verification Privacy Hyperbole*

The Parent Gatekeeper Model brought age verification mechanisms to the center of the stage because it ties identity and age together by providing parents with a right to consent or supervise their child.<sup>92</sup> While the tech industry and others raised First Amendment claims against age verification techniques,<sup>93</sup> an unlikely coalition of privacy advocates and the tech industry also raised objections on privacy grounds. Some privacy advocates argued that the tech platforms or bad-intentioned third parties could abuse information gathered for age verification purposes.<sup>94</sup> They also raised concerns that age verification does not affect just kids, but everyone, since all would need to verify their age to prove they are not minors.<sup>95</sup> Tech companies joined in citing privacy concerns,<sup>96</sup> although as commentators noted, "Big tech's concern for 'protecting user privacy' is just a mirage. No one knows more about us—where we spend our time,

---

92. For an example of a law requiring age verification, see Fla. Stat. § 501.1737 (2025). This is different from age estimation, which relies on companies already having estimated knowledge of a user's age. Sarah Forland, Nat Meysenburg & Erika Solis, *Age Verification: The Complicated Effort to Protect Youth Online*, NEW AM. (Apr. 23, 2024), <https://www.newamerica.org/oti/reports/age-verification-the-complicated-effort-to-protect-youth-online/> [https://perma.cc/KVK2-3Z2G].

93. See, e.g., *NetChoice v Fitch*, No. 24-cv-170, 2024 WL 4068777 (S.D. Miss. July 15, 2024).

94. See, e.g., Kelley & Schwartz, *supra* note 14; Teachout, *supra* note 8 (describing privacy advocates arguments against age fencing).

95. See, e.g., Kelley & Schwartz, *supra* note 14.

96. Adam Candeub, Clare Morell & Michael Toscano, Opinion, *Big Tech Knows that Age Verification Is Necessary*, THE HILL (Sept. 7, 2023, 3:00 PM), <https://thehill.com/opinion/congress-blog/4192462-big-tech-knows-that-age-verification-is-necessary/> [https://perma.cc/B946-ZXT7] ("[T]he Big Tech lobbyists are now shifting from a legal defense to a policy argument: that age verification will destroy user privacy."); Jeff Horwitz & Aaron Tilley, *Apple Helped Nix Part of a Child Safety Bill. More Fights Are Expected*, WALL ST. J. (Sept. 2, 2024, 5:30 AM), <https://www.wsj.com/tech/apple-helped-nix-part-of-a-child-safety-bill-more-fights-are-expected-23905d4d> [https://perma.cc/FZ6R-YQQD].

what we like, who our friends are, even our financial information—than the Big Tech companies.”<sup>97</sup>

Methods of age verification include using a credit card, providing a government issued ID, or verifying a photo ID with a real time photo using biometric facial recognition.<sup>98</sup> Objectors claimed that no age verification method is foolproof.<sup>99</sup> However, this Article posits that those opposing age verification are caught up in a technology determinism fallacy.

Technology determinism means that technology is an autonomous entity that can develop in only one direction according to its internal logic. In other words, technology has a fixed track of evolution dictated by technological constraints and, therefore, its impact on society is predestined and unchangeable.<sup>100</sup> Still, we have seen that technology’s progress is not predetermined. We can choose and mold technology in our values. We can design technologies to be more private.<sup>101</sup> This means that age verification systems are not inherently non-private. And experts are already pointing to significant improvements in age verification systems, especially those involving third parties.<sup>102</sup> Further, leaving kids online with no protections exposes them to significantly higher privacy risks than age verification methods.<sup>103</sup>

While parental gatekeeping laws instigated a storm around age verification, age gating online started spreading well beyond laws to limit kids’ screen time. For example, states increasingly require age verification to prevent kids from entering pornography sites. Basically, states are

---

97. Candeub, Morrell & Toscano, *supra* note 96.

98. Forland, Meysenburg & Solis, *supra* note 92; *see also* Noah Aphrope, Brett M. Frischmann & Yan Shvartzshnaider, *Online Age Gating: An Interdisciplinary Evaluation*, 27 YALE J.L. & TECH. (forthcoming 2025) (manuscript at 19–25) (discussing different age gating technologies).

99. *See, e.g.*, Kelley & Schwartz, *supra* note 14.

100. *See generally* HERBERT MARCUSE, ONE-DIMENSIONAL MAN: STUDIES IN THE IDEOLOGY OF ADVANCED INDUSTRIAL SOCIETY (1964); Jacques Ellul, *The Technological Order*, 3 TECH. & CULTURE 394 (John Wilkinson trans., 1962); Gaia Bernstein, *When New Technologies Are Still New: Windows of Opportunity for Privacy Protection*, 51 VILL. L. REV. 921, 929 (2006).

101. This is called social shaping, a term coined by the social constructivist movement in science and technology studies. It conceives the social shaping of a technology as an interactive process between the technology and its users and not a predetermined outcome. *See* Robert L. Heilbroner, *Do Machines Make History?*, 8 TECH. & CULTURE 335 (1967); John Law & Michel Callon, *The Life and Death of an Aircraft: A Network Analysis of Technical Change*, in SHAPING TECHNOLOGY/BUILDING SOCIETY: STUDIES IN SOCIOTECHNICAL CHANGE 21 (Wiebe E. Bijker & John Law eds., 1992).

102. For example, France began requiring age verification to prevent minors from accessing pornography sites. It analyzed the different approaches and pointed to ways to improve privacy protections particularly by using an independent third party. *See generally* *Online Age Verification: Balancing Privacy and the Protection of Minors*, NAT’L COMM’N ON INFORMATICS AND LIBERTY (Sept. 22, 2022), <https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors> [<https://perma.cc/BQ4Z-KV8Q>].

103. *See infra* Section III.C.3 (discussing the privacy risks to kids under the existing business model).

progressively implementing online age verification where it is mandated in the physical world.<sup>104</sup> Furthermore, tech companies are already using age gatekeeping methods. They ask directly for identification and also estimate their users' ages for different purposes.<sup>105</sup>

## 2. *Parents as Gatekeepers and Kids' Privacy*

The Parent Gatekeeper Model, which empowers parents to control and sometimes supervise their kids' online communications, raised concerns regarding the privacy interests, particularly of older minors.<sup>106</sup> Children and privacy advocates argued that granting parents authority hinders kids' autonomy and their ability to access private spaces. They highlighted concerns related to sensitive issues involving sexual health, gender, and sexual identity.<sup>107</sup>

104. See, e.g., H.B. 1181, 2023 Leg., 88th Sess. (Tex. 2023); H.B. 142, 2022 Leg., Reg. Sess. (La. 2022); see also Teachout, *supra* note 8; Noah Aphthrope, Boen Beavers, Yan Shvartzshnaider & Brett Frischmann, The Authentication Gap: Higher Education's Widespread Noncompliance with NIST Digital Identity Guidelines 4–6 (Aug. 31, 2024) (unpublished manuscript), <https://arxiv.org/pdf/2409.00546> [<https://perma.cc/PCQ3-34L9>] (describing age gating in the physical world).

105. *Introducing Age Group Self-Certification & Get Age Category API for All Developers*, META (July 20, 2023), <https://developer.oculus.com/blog/age-group-self-certification-apis-meta-quest-developers/> [<https://perma.cc/T3CF-7E3V>]; Pavni Diwanji, *How Do We Know Someone Is Old Enough to Use Our Apps?*, META (July 27, 2021), <https://about.fb.com/news/2021/07/age-verification> [<https://perma.cc/3FY8-J8SW>] (explaining how Meta uses AI to estimate if a user is under eighteen); *Age Requirements for TikTok LIVE*, TIKTOK, <https://support.tiktok.com/en/safety-hc/account-and-user-safety/age-requirements-for-tiktok-live> [<https://perma.cc/7S6C-7FKT>] (last visited Jan. 6, 2025) (describing how TikTok uses selfies with photo identifications, credit card authorization, and facial age estimation to confirm users are over eighteen and can go live); *Introducing New Ways to Verify Age on Instagram*, INSTAGRAM (June 23, 2022), <https://about.instagram.com/blog/announcements/new-ways-to-verify-age-on-instagram> [<https://perma.cc/WD4H-EZ8V>] (explaining how Instagram uses selfies to estimate ages).

106. Laws that allowed parents to read kids' messages drew the harshest criticism. See, e.g., Social Media Regulation Amendments, 2023 Utah Laws 498 § 13-63-102, *repealed by* Utah Social Media Regulation Act, 2024 Utah Laws 224. For examples of organizations criticizing these laws for privacy violations, see Jason Kelley & Aaron Mackey, *States Attack Young People's Constitutional Right to Use Social Media: 2023 in Review*, ELEC. FRONTIER FOUND. (Dec. 30, 2023), <https://www.eff.org/deeplinks/2023/12/states-attack-young-peoples-constitutional-right-use-social-media-2023-year-review> [<https://perma.cc/D8ZE-4Z2Z>]; see also Michal Luria & Aliya Bhatia, Opinion, *Restricting and Monitoring Social Media Won't Protect Kids — Here's What Will*, CNN (May 16, 2024, 3:13 PM), <https://www.cnn.com/2024/05/15/opinions/social-media-monitoring-restriction-legislation-mediation-luria-bhatia> [<https://perma.cc/7KED-6LSD>] (“The problem with restriction and monitoring is that they undermine trust.”). Luria and Bhatia also argue that these laws pose a First Amendment violation because they limit kids' ability to express themselves and access information. *Id.*; see also Jason Kelley, *The Law Should Not Require Parental Consent for All Minors to Access to Social Media*, ELEC. FRONTIER FOUND. (May 12, 2023), <https://www.eff.org/deeplinks/2023/05/law-should-not-require-parental-consent-all-minors-access-social-media> [<https://perma.cc/3BMR-T2EF>].

107. See, e.g., Jason Kelley, *Utah's Governor Should Veto “Social Media Regulations” Bill S.B. 152*, ELEC. FRONTIER FOUND. (Mar. 9, 2023), <https://www.eff.org/deeplinks/2023/03/utahs-governor-should-veto-social-media-regulations-bill-sb-152>

Today, kids interact mostly in digital spaces. This happened gradually over the last two decades. Currently, much of their communications are recorded digitally online, often on social networks.<sup>108</sup> Still, one thing has not changed. Kids, particularly teens growing up and searching for their identities, tend to want to keep their peer interactions private. When teens used to interact mostly in person, they could easily do so.<sup>109</sup> But kids today live in a world in which over-parenting norms prevail. Parents engaged in intensive parenting often use technology monitoring, which exposes different aspects of their kids' lives. For example, by tracking their location via smartphone, parents can find out where their kids are and who they may be hanging out with.<sup>110</sup>

Some laws under the Parent Gatekeeper Model pose potential privacy threats to kids. These are primarily laws that expressly allow parents access to their kids' online communications or to the identity of connected or even deleted social media accounts they interact with.<sup>111</sup> However, legislatures granting parents supervisory powers, such as the ability to limit time online or to receive alerts for certain contents, need to also carefully draft these powers. Otherwise, they may, whether intentionally or unintentionally, grant parents access to their kids' online communications.<sup>112</sup>

Even laws that require parental consent for opening an online account may affect kids' autonomy in a way that an identical restriction under the Tech Liability Model would not. For example, a Tech Liability

---

[<https://perma.cc/7DWT-FLZQ>] (arguing that granting parents access to their kids' online activity violates their privacy); ALICE MARWICK, JACOB SMITH, ROBYN CAPLAN & MEHER WADHAWAN, CHILD ONLINE SAFETY LEGIS. (COSL), BULLETIN OF TECHNOLOGY & PUBLIC LIFE 26–28 (2024), <https://assets.pubpub.org/bujb2qf1/COSL-06.04-11717506843758.pdf> [<https://perma.cc/TY5G-GUHW>] (arguing that state laws allowing parental control give access to kids' communications, undermining their privacy and exposing kids to potential abuse and conflict, particularly affecting LGBTQ youth and those with political views divergent from their parents).

108. See generally SHERRY TURKLE, RECLAIMING CONVERSATION: THE POWER OF TALK IN A DIGITAL AGE (2015).

109. See Thomas J. Cottle, *The Connections of Adolescence*, 100 DAEDALUS 1177, 1202 (1971) (noting that adolescents hide their “subversive thoughts” at secret meeting locations); Michael Robb, *Think You Know What Your Kids Are Doing Online? Think Again*, COMMON SENSE MEDIA (Dec. 11, 2017), <https://www.commonsensemedia.org/kids-action/articles/think-you-know-what-your-kids-are-doing-online-think-again> [<https://perma.cc/Q4CX-6RAY>] (describing kids quest for privacy online).

110. See Gaia Bernstein & Zvi Triger, *Over-Parenting*, 44 UC DAVIS L. REV. 1221, 1238–39 (2011); see also *Use Find My to Locate People, Devices, and Items*, APPLE, <https://support.apple.com/guide/icloud/intro-to-find-my-mm11a95f979f/icloud> [<https://perma.cc/UZ65-925G>] (last visited Jan. 6, 2025); *You Want to Do What's Best for Your Family. So Do We.*, APPLE, <https://www.apple.com/families/> [<https://perma.cc/AP3L-65GC>] (last visited Jan. 6, 2025).

111. See, e.g. Utah Minor Protection in Social Media Act, UTAH CODE ANN. § 13-71-203 (West 2024) (granting parents a right to view connected or deleted accounts); Utah Social Media Regulation Act, 2023 Utah Laws 477, *repealed by* Utah Social Media Regulation Act, 2024 Utah Laws 224 (granting parents access to kids communications).

112. See, e.g., *Sammy's Law*, 2023 H.R. 5778, 118th Cong. § 4(f) (2024).



Model law prohibiting all kids under sixteen from holding social media accounts, treats all kids of the same age alike, irrespective of their familial interactions. But a parent gatekeeping law placing consent at sixteen may implicate family disagreements about gender identity, sexual development, or political views in the decision-making. Parents' restrictions on kids, particularly older teens, that impact their ability to make certain life choices and develop their identities in a certain way threatens teens' privacy interests.<sup>113</sup>

Currently, the law provides minimal privacy rights for kids against their parents. It views threats to kids' privacy as stemming from outside the family. It creates an illusion that parents' interests are always harmonious with those of their kids. Put simply, the law assumes that parents always know what is best for their kids. Consequently, it grants parents broad rights to raise their kids as they see fit.<sup>114</sup> For example, parents determine what school to send their kids to or whether they are homeschooled.<sup>115</sup> While the law grants children some limited rights in areas such as custody and health, with regards to other decisions, courts continue to view kids as dependent beings in need of adult supervision and control.<sup>116</sup>

Still, internationally, the United Nations Convention for the Rights of the Child (UNCRC) explicitly grants children a right to privacy.<sup>117</sup> Further, scholars increasingly call for a shift from focusing on privacy threats to kids from outside the family to protecting their privacy interests within (i.e., against their parents).<sup>118</sup> They argue that children's interests may

113. For articles connecting privacy, autonomy, and identity interests, see Benjamin Shmueli & Ayelet Blecher-Prigat, *Privacy for Children*, 42 COLUM. HUM. RTS. L. REV. 759, 778 (2011); Anita L. Allen, *Taking Liberties: Privacy, Private Choice, and Social Contract Theory*, 56 U. CIN. L. REV. 461, 466–69 (1987). See generally Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000).

114. See Anne C. Dailey & Laura A. Rosenbury, *The New Parental Rights*, 71 DUKE L.J. 75, 76–77 (2021) [hereinafter *The New Parental Rights*]; Emily Buss, "Parental" Rights, 88 VA. L. REV. 635, 647 (2002); Anne C. Dailey & Laura A. Rosenbury, *The New Law of the Child*, 127 YALE. L.J. 1148, 1461 (2018) [hereinafter *The New Law of the Child*]; Stacey B. Steinberg, *Sharenting: Children's Privacy in the Age of Social Media*, 66 EMORY. L.J. 839, 861 (2017); Clare Huntington & Elizabeth S. Scott, *Conceptualizing Legal Childhood in the Twenty-First Century*, 118 MICH. L. REV. 1371, 1377 (2020).

115. See *Wisconsin v. Yoder*, 406 U.S. 205, 213 (1972) (noting that while the state has the responsibility to educate its citizens, that right yields "to the right of parents to provide an equivalent education in a privately operated system"); *Pierce v. Soc'y of Sisters*, 268 U.S. 510, 534 (1925) ("[P]arents and guardians, as a part of their liberty, might direct the education of children by selecting reputable teachers and places.").

116. *The New Law of the Child*, *supra* note 114, at 1461 (mentioning custody and health care rights); *Tinker v. Des Moines Indep. Cmty. Sch. Dist.*, 393 U.S. 503, 514 (1969) (granting children constitutional rights for purposes of school speech).

117. Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3. The Treaty's scope is unclear and the United States has refused to ratify it. See Shmueli & Blecher-Prigat, *supra* note 113, at 785; *The New Law of the Child*, *supra* note 114, at 1472.

118. See, e.g., Shmueli & Blecher-Prigat, *supra* note 113, at 777. See generally Clare Ryan, *Are Children's Rights Enough?*, 72 AM. U. L. REV. 2075 (2023) (discussing the barriers to the development of children's rights)

diverge from those of their parents and call for courts and legislatures to support these interests.<sup>119</sup> They explain that parental rights should only further children's broader interests, not trump them.<sup>120</sup> To implement this shift, scholars suggest accounting for children's right to privacy from their parents, but qualifying it according to the child's age and evolving capacities.<sup>121</sup> While these scholars did not specifically address parental online gatekeeping laws, they emphasized the need kids have for some private spaces where they can socialize away from their parents' monitoring.<sup>122</sup> They also underscored the interests that children have in controlling the flow of information to their parents, especially when the information conflicts with their parents' wishes.<sup>123</sup>

As Section III.B discussed, the Parent Gatekeeper Model is unlikely to resolve the problem of kids' tech addiction. Threats to kids' privacy rights add another layer of concern about the Parent Gatekeeper Model and further support the Tech Liability Model. At first blush, opting for state direct regulation instead of holding the parent as an intermediary seems to go against the narrative of family privacy. The narrative under which parents have broad powers over their children and the state plays a non-intervention role. But this narrative of state nonintervention is false. The law, in fact, regulates children's lives on a daily basis.<sup>124</sup> It dictates safety measures, such as use of car seats.<sup>125</sup> It prohibits kids from gambling, smoking, or drinking.<sup>126</sup> It dictates when children may work for wages, when they may enter into enforceable contracts, and what they must waive to participate in sports and other activities.<sup>127</sup> While some view any law that restricts a person's activity as paternalistic, traditionally laws to restrict kids do not encounter these objections.<sup>128</sup> The Parent Gatekeeper Model's potential for privacy threats and the government's regular imposition of restrictions to protect kids provide further support for legislatures to opt for the Tech Liability Model.

---

119. See *The New Parental Rights*, *supra* note 114, at 77.

120. *The New Law of the Child*, *supra* note 114, at 1451.

121. Shmueli & Blecher-Prigat, *supra* note 113, at 762–63, 793.

122. *Id.* at 793.

123. *The New Law of the Child*, *supra* note 114, at 1502–03.

124. *Id.* at 109; *The New Parental Rights*, *supra* note 114, at 1473–74. See generally Clare Ryan, *Children as Bargaining Chips*, 68 UCLA L. Rev. 410 (2021) (discussing the state's custodial power).

125. See, e.g., CAL. VEH. CODE § 27360(a) (West 2024) (requiring children under eight to be secured in a car seat).

126. OHIO REV. CODE ANN. § 3775.99(A) (West 2024) (prohibiting people under twenty-one from sports betting); 720 ILL. COMP. STAT. 675/1 (2019) (prohibiting people under twenty-one from purchasing tobacco); 3 R.I. GEN. LAWS § 3-8-11.1(b) (2024) (prohibiting people under twenty-one from purchasing alcohol).

127. *The New Law of the Child*, *supra* note 114, at 1473–74.

128. BERNSTEIN, *supra* note 2, at 98; David L. Shapiro, *Courts, Legislatures and Paternalism*, 74 VA. L. REV. 519 (1988); Gerald Dworkin, *Paternalism*, 56 THE MONIST 64, 65 (1972).

### 3. *Privacy and Containing Tech Addiction as Harmonious Goals*

While some parent gatekeeping laws could create privacy issues, protecting kids' privacy and containing tech addiction are not inherently at odds. To the contrary, laws targeting tech addiction under the Direct Liability Model enhance efforts to protect privacy. These laws bolster privacy because the collection of data and the extension of user time online are part of the same business model. Laws restricting either of these activities make the entire business model less profitable and reduce the desirability of the other activity.

Let us turn to examining the business model, which governs large parts of the internet as we have known it for decades. Traditional industries rely on tangible assets. For example, the car industry uses iron, aluminum, and glass, and electrical companies use oil, coal, and natural gas. But the information economy relies on intangible assets.<sup>129</sup> Specifically, the internet economy relies on people as its intangible assets.<sup>130</sup> Its first resource is time—our attention; and the second is our data. One feeds another to create the internet economy's main business model.<sup>131</sup>

How does the business model operate? Companies like Meta or Google give users their products for free. They provide Facebook for free. They give Gmail for free. But these products are not actually free. Users pay for them with their time and their data. Many tech platforms make money by selling ads. They collect user data and use it to target ads of products and services they predict users would like to purchase. Tech platforms' ad revenues increase when users spend more time online and are more likely to see the ads and buy the advertised products. More time online also means collecting more user data, which increases the effectiveness of the ads.<sup>132</sup>

Data and time are closely integrated in the same business model. As Professor Elettra Bietti succinctly put it: "Data and attention, their

---

129. See generally YOCHAI BENKLER, *THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM* (2006).

130. As Shoshana Zuboff frames it, the internet economy "uses human experience as raw material." SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER* 8 (2018).

131. BERNSTEIN, *supra* note 2, at 80–81. For a historical discussion of the use of consumer attention, see TIM WU, *THE ATTENTION MERCHANTS: THE EPIC SCRAMBLE TO GET INSIDE OUR HEADS* (2017).

132. BERNSTEIN, *supra* note 2, at 80–81. Elettra Bietti described the operation of this business model as the "data-attention imperative." Elettra Bietti, *The Data-Attention Imperative*, 1, 6, 21, 27 (N.E. Univ. Sch. of Law Rsch. Paper No. 473, 2024); ZUBOFF, *supra* note 130, at 70 (explaining that the business model is based on predicting how we behave). For other discussions of the business model involving data, time, and ads, see Neil Richards & Woodrow Hartzog, *Against Engagement*, 104 B.U. L. REV. 1151, 1157–61 (2024); JULIE E. COHEN, *BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM* 83–89 (2019) (describing the manipulative power of engagement-optimized platforms); Tim Wu, *Blind Spot: The Attention Economy and the Law*, 82 ANTITRUST L.J. 771, 772, 778 (2019) (describing "attention brokerage" as attracting attention by offering entertainment, news, or free services and reselling that attention to advertisers).

capture, and the harms they cause must be considered jointly, not in isolation.<sup>133</sup> To illustrate the interwoven connection between data and user time, investors focus on monetizing users rather than personal data. This means that users are valued through the time spent on the platform. A study analyzing earning calls held by investors revealed that investors do not look at personal data as the asset, but at its monetization, i.e., the users (and the time they spend). In other words, investors view the users that data gives access to as the asset.<sup>134</sup>

As long as this business model exists, tech companies will continue to use addictive designs to capture more user time and attention.<sup>135</sup> But laws that restrict the collection of kids' data make advertising less targeted and, therefore, less lucrative for advertisers.<sup>136</sup> For example, an Instant Pot ad is less likely to lure a teen to click and purchase it than a forty-year old parent looking for effective ways to feed their family. When fewer users click on ads and purchase products, advertisers pay less for the lower yields.<sup>137</sup> At that point, the whole business model starts to destabilize and the reliance on user time decreases. User time loses its value because it no longer yields superior data or effectively results in ad clicks and product purchases.

Similarly, laws that restrict the use of addictive designs or user time online impact the business model and the reliance on the twin resource—data.<sup>138</sup> Once users spend less time online, tech platforms can collect less data. When tech companies have less data to rely on, the ads become less targeted and less effective. Moreover, without addictive designs, time online decreases. This means that fewer users are online at any given time.

---

133. Bietti, *supra* note 132, at 27; *see also* Richards & Hartzog, *supra* note 132, at 1175–76 (tying together data collection and user engagement).

134. Kean Birch, DT Cochrane & Callum Ward, *Data as Asset? The Measurement Governance, and Valuation of Digital Personal Data by Big Tech*, *BIG DATA & SOC'Y*, Jan.–June 2021, at 1, 4, 9, 10.

135. *See* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 *B.C. L. REV.* 1687, 1696 (2020) (tying privacy theory to constraining corporate power).

136. For examples of these laws, see *INFO. COMM'R'S OFF.*, *supra* note 49, at 54–55 (requiring social media companies to minimize data collection by only collecting necessary data and keeping the data for no longer than necessary); *CAL. CIV. CODE* § 1798.99.31(b)(3) (West 2024) (prohibiting social media companies from “[c]ollect[ing], sell[ing], shar[ing], or retain[ing] any personal information that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged”).

137. Xinran He, Junfeng Pan, Ou Jin, Tianbing Xu, Bo Liu, Tao Xu, Yanxin Shi, Antoine Atallah, Ralf Herbrich, Stuart Bowers & Joaquin Quiñero Candela, *Practical Lessons from Predicting Clicks on Ads at Facebook*, *ASS'N FOR COMPUTING MACH.* 1 (2014) (“Online advertising allows advertisers to only bid and pay for measurable user responses, such as clicks on ads. As a consequence, click prediction systems are central to most online advertising systems.”); *see also* Kelly Main, *PPC Advertising: The Ultimate Guide*, *FORBES*, <https://www.forbes.com/advisor/business/ppc-marketing-guide/> [<https://perma.cc/6NNF-KGEF>] (July 25, 2024, 10:31 AM).

138. For laws restricting time online, see *TENN. CODE ANN.* § 47-18-5703 (2024) (requiring parental consent for minors to use social media); *Stop Addictive Feeds Exploitation (SAFE) for Kids Act*, 2024 *N.Y. LAWS* 120 § 1502 (restricting social media from sending notifications between the hours of 12 AM and 5 AM).

This reduces the number of ad clicks and purchased products. And finally, laws restricting targeted advertising to kids similarly destabilize the business model. Prohibiting targeted advertising once again reduces the reliance on both the collection of data and user time online because revenue from advertising is reduced.<sup>139</sup>

The close synergy between data and time illustrates that regulation of either resource accomplishes the goal of reducing the need for the other. In other words, the prevalent business model depends on both. Laws that regulate time online promote privacy protection, while laws that restrict data collection help alleviate tech addiction by reducing user time online. Laws targeting time and laws targeting data collection can and should act in harmony to dismantle the business model that fails to serve its consumers but instead uses them as its resources.

#### IV. ROLES FOR PARENTS AS GATEKEEPERS

This Article cautioned that if the tech industry fails to avert regulation altogether, it would prefer to endorse the Parent Gatekeeper Model.<sup>140</sup> It underscored that adoption of the Parent Gatekeeper Model in lieu of the Direct Liability Model will likely fail to resolve the tech addiction problem and could raise privacy concerns. At the same time, this Article does not argue that legislatures should refrain from granting parents the rights to monitor their kids to contain online harms. Some kids are more vulnerable or less mature than others and may benefit from additional monitoring. To address parental concerns, legislatures could incorporate parent gatekeeping laws if they take care to minimize the risks of obstructing the enactment of laws under the Direct Liability Model and the risks to kids' privacy interests.

A reimagined internet, where kids can enjoy the benefits of information, communication, and innovation, without the harms of tech addiction, could consist of two levels of protection. Legislatures should prioritize enacting laws, which can effectively regulate tech platforms under the Direct Liability model. But they can simultaneously or afterwards add an optional second layer of parental gatekeeping options that are designed to limit threats to teens' privacy interests.

Prioritizing the adoption of laws under the Direct Liability Model is crucial for two reasons. First, initial adoption of the Parent Gatekeeper Model could obstruct later enactment of the vital Direct Liability Model protection layer. It could bolster an argument that there is no need for further legislation. Second, prioritizing Direct Liability Model

---

139. For examples of laws limiting targeted advertising, see INFO. COMM'R'S OFF., *supra* note 49, at 35 (restricting social media from collecting data to “profile” children and send them targeted advertisements without consent); Children and Teens' Online Safety Act (COPPA 2.0), S. 1418, 118th Cong. §6(a)(1) (2023) (prohibiting social media companies from “compil[ing] personal information of a user for purposes of targeted marketing . . . if such use . . . is reasonably likely to involve collection of personal information from a child or teen”).

140. See *supra* Section III.A.

laws would decrease the need for parental supervision because the initial layer of protection would reduce time online and the related online harms. Reducing the scope and urgency of the problem would provide more room for careful designing of parental gatekeeping roles in a way that protects kids' privacy.<sup>141</sup>

While this Article advocates that legislatures should prioritize the Direct Liability Model protection layer, it acknowledges that political realities may affect available choices. Nevertheless, this Article cautions that legislatures adopting laws under the Parent Gatekeeper Model, at any point, should carefully tailor them to leave room for subsequent direct regulation of the tech industry and to account for kids' privacy interests.

This Article proposes that legislatures promulgating laws under the Parent Gatekeeper Model should apply the following guidelines. First, laws should consider the age of the child. While kids have different levels of maturity, younger kids do not only require more supervision, but also have lesser privacy interests.<sup>142</sup> Second, laws that give parents access to the content of their kids' online interactions carry the greatest privacy risks. This includes laws providing access to kids' messages, accounts they are associated with, or to sites they visit.<sup>143</sup> Legislatures should carefully assess any supervisory roles that are content related and expose the nature of kids' interactions—especially teens. They should narrowly draft such roles and target only particularly risky situations. For example, exposure to materials like the TikTok choking challenge, which lead many kids to their untimely death.<sup>144</sup> Third, legislatures should prefer granting gatekeeping roles that do not expose the content of kids' interactions. For example, a parent

---

141. Parents whose kids suffered the worst that the internet can deliver, such as death of their child caused by drugs bought on Snapchat, advocate for laws requiring tech companies to implement technology that will notify parents if their kids are at risk of suicide, eating disorder, substance abuse, sexual abuse, child pornography, and other harms including anxiety, academic dishonesty, and fraud. *See Sammy's Law*, ORG. FOR SOCIAL MEDIA SAFETY, <https://www.socialmediasafety.org/sammys-law/> [<https://perma.cc/695N-PBFS>] (last visited Jan. 6, 2025); *Sammy's Law*, H.R. 5778, 118th Cong. § 4(f) (2024); *see also* H.B. 5380, 103rd Assemb. (Ill. 2024); S.B. 1444, 2023-2024 Reg. Sess. (Cal. 2023); H.B. 773, 2023-2024 Reg. Sess. (N.C. 2023). In a world in which tech platforms, and particularly social media platforms are unregulated, parents rightfully fear for their kids and seek tools to protect them. But in a world in which Direct Liability Model laws regulate tech platforms, the risk of harm will significantly reduce. Consequently, the need for parents to receive warnings would diminish. Parental protections could then focus on alerts for the most dangerous risks and alerts that could be designed to prevent harm while preserving teens' privacy. Sarah Felbin, Sabrina Talbert & Addison Aloian, *The 'Blackout Challenge' Has Resurfaced on Tiktok, and It's Still as Dangerous as It Was 17 Years Ago*, WOMEN'S HEALTH, <https://www.womenshealthmag.com/health/a38603617/blackout-challenge-tiktok-2021/> [<https://perma.cc/YW3T-NABP>] (Apr. 17, 2024, 5:35 PM).

142. *The New Law of the Child*, *supra* note 114, at 1476.

143. *See, e.g.*, Utah Social Media Regulation Act, 2023 Utah Laws 498, *repealed by* Utah Minor Protection in Social Media Act, 2024 Utah Laws 224; Utah Minor Protection in Social Media Act, UTAH CODE ANN. § 13-71-203 (West 2024).

144. Felbin, Talbert & Aloian *supra* note 141; *see also* Complaint for Wrongful Death and Survival Action (Strict Liability; Negligence; and Violation of the California Consumer Legal Remedies Act, Cal. Civ. § 1750, et seq.), *Smith v. Tiktok, Inc.*, No. 22STCV21355 (Cal. Super. Ct. June 30, 2022), 2022 WL 22835501.

can be given an option to stop notifications at different hours or keep an addictive algorithmic feed off.<sup>145</sup> These supervisory powers would provide parents with opportunities to structure protections for their individual child while minimizing the impact on kids' privacy.

#### CONCLUSION

This Article examined the legislative landscape of laws seeking to contain addictive technologies and kids' excessive screen time. It identified two models of laws espousing different conceptions of who should be the gatekeeper of kids' screen time. The Tech Liability Model imposes direct responsibility on tech platforms, while the Parent Gatekeeper Model directs tech platforms to provide parents with monitoring tools and powers.

Currently, tech companies seeking to avoid regulation dominate the discourse through casting it as a First Amendment debate. By doing so, they successfully obstruct the real issue: whether the Tech Liability Model or the Parent Gatekeeper Model would be more effective and suitable to regulate kids' screen time. The Article argued that the Tech Liability Model is superior in accomplishing this objective. It explained that while the two models can co-exist, legislatures should enact parents gatekeeping laws only simultaneously or after the adoption of a Tech Liability Model regime.

The Article explained that while the tech industry desires to ward off any regulation, if forced to choose, it would opt for the Parent Gatekeeper Model. Tech companies prefer the Parent Gatekeeper Model because it allows them to shift responsibility for kids' excessive screen time from themselves to the parents. Furthermore, experience with parental controls shows that parental gatekeeping laws would be ineffective in reducing kids screen time. The Article also highlighted that laws to protect kids' privacy and laws to regulate tech addiction generally bolster each other. Yet, it underscored that some laws enacted under the Parent Gatekeeper Model, unless carefully drafted, could threaten kids' privacy interests.

The Article concludes that while the Tech Liability Model is superior to the Parent Gatekeeper Model, hybrid models that incorporate parent gatekeeping laws can be effective as long as the timing of their adoption, their breadth, and the powers granted to parents are carefully drafted. It cautions that legislatures should enact parental gatekeeping laws only in a way that avoids obstructing the enactment of laws under the Direct Liability Model and protects kids' privacy interests.

---

145. *See, e.g.*, S.B. 7694.

