Minnesota Attorney General's Report on Emerging Technology and Its Effects on Youth Well-Being

Vol. 2 • February 2025

The Office of
Minnesota Attorney General Keith Ellison
helping people afford their lives and live with dignity, safety, and respect • *www.ag.state.mn.us*

Table of Contents

Foreword From Attorney General Keith Ellison 4

Executive Summary 5

The Report 8

Section One: The effects of emerging technology on Minnesotans, especially youth 8

Many consumers, especially youth, are experiencing bullying and harassment. 9

Many consumers are having experiences with unwanted disturbing, graphic, and sexual content, often served to them by AI-powered algorithms 10

Many users experience envy and negative social comparison, which are encouraged by technology platform dynamics 11

Many cases of manipulation and fraud begin with unwanted contact, facilitated by loose privacy defaults and high rate limits, with especially serious consequences for young people 12

Platforms facilitate the misuse of user information and images, including that of younger users 13

Excessive and compulsive use of technology, facilitated by systems that are optimized for time and attention, displaces beneficial activities like sleep and in-person socialization 14

Algorithms often exhibit bias, and the integration of increasingly powerful AI into more algorithms is likely to accelerate this trend 15

Specific groups often experience more acute harms. 15

Girls and young women often have worse online experiences, including gender-based harassment and negative image comparisons 15

Boys and young men are often targeted for sextortion and misogyny 16

Minority and LGBTQ+ groups find community online but also report more negative experiences 17

Section Two: The legislative and legal landscape 18

Social media regulation 18

Content regulation in the U.S. 19

Social media age limits 20

Social media reform focusing on minors 20

Privacy and data protection 22

AI-specific legislation 22

Section Three: What can we learn from previous legislative efforts? 24

Vague statutory language can lead to legal challenges, implementation difficulty, and opposition from those who fear misuse of well-intentioned efforts 24

Being too prescriptive about solutions can have negative consequences 25

Broad reporting requirements have often not had a material impact 25

Identifying minors needs to be done in a way that respects privacy and free expression concerns 25

Potential constitutional challenges require the inclusion of alternative mechanisms to enforcement 26

Opt-out policies generally have not been effective 26
Age limits for social media platforms have both pros and cons 26
Policies relating to content have been ineffective and led to both opposition related to potential misuse and legal challenges 27
A design focus has been impactful both within companies and in legislation, but needs to focus on function, rather than expression 27

Section Four: The current and expanding impact of AI 28
Generative AI has been commonly used to make non-consensual sexual imagery 28
Chatbots do not have appropriate safeguards for young people, who use them widely 28
Protecting society against current threats from Generative AI 29

Section Five: Policy recommendations 29
I. Ban "deceptive patterns" within platform design 30
Ban design features that encourage greater usage for children beyond their explicit desires. offer all users accessible tools to limit their platform usage 31
Mandate aggressive privacy defaults to limit the unwanted sharing of data and images 31
Mandate responsible amplification through limits on engagement-based optimization 32
Mandate transparent, sensible rate limits that would limit the ability for small groups of users to manipulate others 33
II. Mandate transparency of product experimentation that can illuminate new harmful deceptive patterns 33
III. Mandate user and parent empowerment via consumer-friendly device-based defaults 34
IV. Track technology platform specific impact on user experience, including amongst sub-groups 34
V. Mandate interoperability to encourage consumer choice 35
VI. Mandate technology usage limits and education within schools 35
VII. Protect youth from the current harms of AI 36

Conclusion and next steps, including model bills 37

Endnotes 39

Appendices 55
Appendix A – Model Bill: Prohibiting Deceptive Patterns. 55
Appendix B – Model Bill: Device Based Age Settings 61
Appendix C – Model Bill: Preventing Identity Appropriation Act 63
Appendix D – Model Bill: State Version of ACCESS Act 66
Appendix E – Model Bill: Digital Advertising Tax for Public Health Monitoring 71
Appendix F – Model Bill: Act to Promote Safe, Effective, and Distraction Free Education for PreK-12 Students 73

Foreword
From Attorney General Keith Ellison

My desire to protect Minnesotans from technology related harms remains a crucial part of my role in helping Minnesotans afford their lives and live with dignity, safety, and respect. Following the release of the first report, the Legislature directed my Office to expand on our initial findings and recommendations in a second report. *See* 2023 Minn. Laws chapter 57, Art. 1, § 4, subd. 3.

As directed by the Legislature, this report:

- Expands on how social media related products affect youth mental health and overall wellbeing.
- Explores the increasingly harmful impacts of social media on marginalized communities.
- Further analyzes proposed and enacted technology regulation related laws in multiple jurisdictions.
- Proposes an updated set of policy recommendations, specifically related to AI.

My Office was able to expand on the first report with the continued help of the exceptional and highly experienced expert Dr. Ravi Iyer. Dr. Iyer is a technologist and academic psychologist who is currently managing director of USC Marshall School's Neely Center for Ethical Leadership and Decision Making. Prior to this, he worked for Meta (which owns Facebook and Instagram) and has published multiple scholarly articles on the impacts of technology related harms. His ongoing support through writing and research was essential in creating this report.

A law clerk with our Office, Alyssa Padmanabhan, also assisted with this project by researching proposed regulations and related case law. She assisted in drafting Section Two of this report while in her third year at the University of St. Thomas School of Law. My deepest thanks to both Dr. Iyer and Alyssa for their time, energy, and commitment to helping us complete this thorough and thoughtful report.

This report, an update on the Attorney General's 2024 report, further examines the impact of technology companies and their products on the mental health and well-being of Minnesotans, with a focus on children. Since the initial report was released, the focus on this issue has only increased, with numerous legislative bills introduced and legal cases argued. AI adoption has also increased, leading to new and novel harms and requiring new solutions. This updated report analyzes proposed and enacted consumer protection laws related to the regulation of technology companies from Minnesota and from other jurisdictions. Finally, it builds upon recent efforts to make updated policy recommendations that may be helpful for future legislation both in Minnesota and other states across the country.

My Office has continued working in a joint effort with other state attorneys general in our ongoing litigation against Meta for creating manipulative and harmful design features that adversely affect young people. My intent is that this report will provide Minnesotans and policymakers with additional guidance to create and navigate modern solutions that address the functions (and resulting harms) of new and emerging technology, especially AI. As explained in the Report, young people are extremely vulnerable to the manipulative and addictive functional design features of these technologies. I hope to assist in creating safer solutions that will protect and nurture the mental and physical wellbeing of all Minnesotans and, ideally, people everywhere.

Executive Summary

The core conclusions of our 2024 report remain the same. Technology remains an important tool for beneficial societal progress. Yet, like many new technologies, these advances create new societal harms.

A century ago, personal cars enabled fast access to family, employment, education, and medical care across previously far-flung locales, but at the same time they created an epidemic of deaths on the road. Regulations on vehicle design, road planning, and driver safety education were developed to ensure that their use led to as few deadly collisions as possible. Advances in agricultural technology reduced the labor and cost required to bring crops to harvest, but laws were soon needed to prevent producers from cutting costs in ways that endangered the health of consumers. Ultimately, these safety standards were beneficial for industries as consumers felt more comfortable using cars and eating food that met consensus standards of safety. These standards also enabled car and food manufacturers to compete on a level playing field without fear of competitors under-cutting them by selling cheaper—yet unsafe—products.

Most Americans want their government to ensure that technology companies design their products to protect the mental health of children.[1] Momentum toward this goal has accelerated over the past year, including the passage of numerous child focused online safety laws. Jonathan Haidt's book, *The Anxious Generation*, which focuses on technology's impact on children, has spent more than 35 weeks as a New York Times bestseller, and has galvanized communities around the world toward action. In our previous report, we noted that 80 percent of Americans believe that currently-evolving AI technologies will make these problems worse.[2] In 2024, we saw many of these fears come true as we saw increasing harms from AI, including from chatbots that deceive young people into believing they are human[3] and bullying using deepfaked, non-consensual sexual imagery.[4] This citizen concern has led to even more regulatory effort across jurisdictions to protect public health and safety from these emerging technologies. This updated report builds on those efforts and proposes a way forward for Minnesotans that is constitutional, feasible, and effective.

This report contains the same five sections as our original report but adds a few new areas of focus within each section. In the first section, it documents the existing evidence that technology products have had a material impact on Minnesotans, with a focus on the well-being and mental health of youth. It discusses the many highly prevalent negative effects of technology created by tech companies' specific product design choices.[5] In particular, technological design choices create the below negative effects on youth:

- Many consumers, especially youth, are experiencing online bullying and harassment.
- Many consumers are having experiences with unwanted disturbing, graphic, and sexual content, often served to them by AI-powered algorithms.
- Many users experience envy and negative social comparison, which are encouraged by technology platform dynamics.
- Many cases of manipulation and fraud begin with unwanted contact and are facilitated by loose privacy defaults and high rate limits (*i.e.*, how many actions a user can take in a given period), with especially serious consequences for young people.

- Platforms facilitate the misuse of user information and images, including that of young users.
- Excessive and compulsive usage of technology, facilitated by systems that are optimized for time and attention, displaces beneficial activities like sleep and in-person socialization.
- Algorithms often exhibit bias, and the integration of increasingly powerful AI into more algorithms is likely to accelerate this trend.

This report also adds a new section describing the wide variety of user experiences with technology, focusing on the particular experiences of young women, young men, racial minorities, and LGBTQ+ people. We note that people in these categories often experience specific acute benefits and harms, suggesting that platform safety design regulations may be even more important for these groups, to enable them to better control their experiences. In particular, we note that:

- Girls and young women often have worse online experiences, including gendered harassment and negative comparisons
- Boys and young men are often targeted for sextortion and misogyny
- Minority and LGBTQ+ groups find community online but also report more negative experiences

In the second section, we provide new details about the legal landscape and the many legislative efforts underway nationwide, including in Minnesota, with an eye toward what we can learn about what may be most effective, especially given recent court decisions that have curtailed laws governing online content while opening more clarity regarding laws regulating product design. In the third section, the report makes a set of recommendations for policymakers to address the above harms in ways that allows the benefits of tech to continue. There are successes within previous legislative efforts that can be replicated, but also many notable areas where improvement is needed to make maximal impact and learn from previous court decisions. The trends we identified in our previous report have continued, and this report identifies the following principles:

- Vague statutory language can lead to legal challenges, implementation difficulty, and opposition from those who fear misuse of well-intentioned efforts.
- Being too prescriptive about solutions can have negative consequences.
- Broad reporting requirements have often not had a material impact.
- Identifying minors needs to be done in a way that respects privacy and free expression concerns.
- Potential constitutional challenges require the inclusion of alternative mechanisms to enforcement.
- Opt-out policies generally have not been effective.
- Age limits for social media platforms have both pros and cons.
- Policies relating to content have been ineffective and led to both opposition related to potential misuse and legal challenges.
- A design focus has been impactful both within companies and in legislation, but needs to remain focused on function, rather than expression.

We previously ended our report with a section about the likely impact of AI. Given that AI has gained much wider adoption even within the last year, we no longer have to speculate about potential harms. Our fourth section now details the observed harms of AI, especially for young Minnesotans. We also include proposed mitigations and conclude:

- Chatbots do not have appropriate safeguards for young people, who use them widely.
- Generative AI has been commonly used to make non-consensual imagery, including sexual imagery.

Finally, in our fifth section, we synthesize the ways that technology products could be made more beneficial, incorporating lessons from previous legislative efforts to inform recommendations for new legislation. While the past year brought many more legislative and regulatory efforts that we can analyze, the lessons from those efforts remain similar. Accordingly, our recommendations remain similar, but we raise them with even more confidence and add new, finer-grained resolution. In order to directly address the concerns and challenges that have arisen in improving technology's impact on society, our recommendations are:

- Ban "Deceptive Patterns" within platform design:
  - Ban design features that encourage greater usage for children beyond their explicit desires (*e.g.* infinite scroll, auto-play, aggressive notifications). Offer all users accessible tools to limit their use if desired.
  - Mandate maximal privacy defaults to limit the unwanted sharing of data and images, especially for sexual content.
  - Mandate responsible content amplification by limiting engagement-based optimization (*e.g.* optimizing for time spent or video consumption).
  - Mandate transparent, sensible rate limits to limit the ability of small groups of users to intentionally deceive and manipulate large groups of people.
- Mandate transparency of product experimentation to illuminate new harmful "deceptive patterns" of platform design.
- Mandate user and parent empowerment via consumer-friendly device-based defaults.
- Track technology platform-specific impact on user experience.
- Mandate interoperability between platforms to prevent monopoly-like moats and empower consumer market choice.
- Mandate usage limits and education within schools.

Given newly-observed harms that have arisen from AI, we also make the following new recommendations for AI technologies:

- Prohibit tech companies from experimenting on young people with high-risk AI systems.
- Design limitations on chatbots to ensure that vulnerable citizens do not perceive them to be actually human.
- Mandate that all parties take appropriate responsibility in reducing the creation and spread of non-consensual imagery.

Beyond making recommendations, we also are now in a position to offer in appendices to this report a variety of model bills, based on experiences across states, including Minnesota. We continue to be grateful for the broad research, advocacy, and legislative efforts by all stakeholders that have informed our report. Along with numerous interested parties,[6] we have synthesized the lessons learned from these efforts into a series of model bills that turn our recommendations into constitutional, effective, and feasible legislative language.

One understandable objection we encountered in the Minnesota Legislature last year was the desire not to be isolated within the wider technology landscape. But, as this report makes clear, Minnesotans need updated and modern protections from the known harms that flow from these ubiquitousness, and new technologies. Our hope in offering model legislation that addresses common risks across states and countries, and that borrows from efforts across jurisdictions, is that the recommendations and policies raised in this report can be used not only by Minnesota but also by other states, so that society can state, with a unified voice, what we expect from technology providers.[7]

The Report

Section One: The effects of emerging technology on Minnesotans, especially youth

Scientific consensus has been difficult to achieve as to whether emerging technology affects Americans (and Minnesotans) positively or negatively *on average*, with studies on both sides of this debate.[8] Over the past year, this debate has grown in the public consciousness, with the publication of the bestselling book, *The Anxious Generation*, and the resulting societal discussion.

Given the complex heterogeneous nature of both technologies and individuals, a focus on the average aggregate effect may be misplaced, and the societal consensus that action needs to be taken to fix specific issues has grown, even as the scientific community remains divided as to the overall effects.[9] There is clear evidence that the specific choices of many technology platforms have caused harmful experiences for a substantial number of individuals, especially youth. Here we summarize how certain specific design choices of some technology platforms have led to increased harm versus benefit, with an eye toward informing policy solutions to define minimum standards of safe platform design for Minnesotans.

Users report many specific categories of harmful and unwanted experiences. For each of the below categories of such experiences, there is clear evidence of unacceptable **prevalence**, with a large number of users, especially youth, reporting experiencing these harms. Since our previous report, more reports of the ubiquitousness of such experiences have been released including an updated survey from the University of Minnesota[10] showing the continued ubiquitousness of excessive internet use, internal platform research suggesting increased risk from those using traditional social media platforms[11] and new surveys looking at novel harms stemming from the use of generative AI.[12] Across numerous harms, increased social media use is associated with increased negative issues with depression, diet, sleep, anxiety, body image, physical activity, and sexual exploitation.[13]

For each of these categories of harm, we can also demonstrate **causality**, by pointing to evidence that these harms are often exacerbated by "deceptive patterns,"[14] which have been defined as the "design practices that trick or manipulate users into making choices they would not otherwise have made and that may cause harm."[15] These product decisions are made in order to get youth to use these products more, and over 70 percent of youth report feeling manipulated by them.[16] These deceptive patterns employed by technology companies exist in stark contrast to how the companies hold out and market their products to the public, including their emphasis on user choice and empowerment. Youth are particularly vulnerable to such manipulation as their brains crave social reward, and lack inhibition, per the American Psychological Association.[17] Greater integration of AI into society is further exacerbating these issues. This rising threat to Minnesota youth suggests that government action is necessary. However, not all technology products exhibit these same deceptive patterns,[18] which proves that a better technological future that still makes room for corporate innovation and profits is possible.

72%
of youth report feeling manipulated by deceptive patterns employed by technology companies[16]

A list of common unwanted harmful experiences reported by consumers is elaborated below. Notably, these are not experiences that any government agency has defined as harmful. Rather, these are experiences that Minnesotans themselves are reporting as unwanted and harmful, yet are experiencing nonetheless, due to rarely understood and often undisclosed aspects of product design. To emphasize this point, each section begins with a quote from a user, including many from Minnesotans who have filed complaints with the Attorney General's Office. In many cases, consumers have false beliefs about how their information is being used and how much control they have over their experience. As a result, many consumers experience harm to their well-being, even as companies experience financial benefit. Under such circumstances, there is clear precedent for the government to take action to prohibit design elements that lead to false beliefs and undisclosed costs.[19]

Many consumers, especially youth, are experiencing bullying and harassment.

> **"When I was 16/17, I faced harassment and bullying on Snapchat. I had blocked these individuals and still faced harassment by them. They found ways to add me to group chats and after blocking someone the chats were still available. This changed the way I approached social media. I thought it was safe and instead I had it used against me. I deleted the app and terminated my account, and encouraged others who had faced bullying on Snapchat to do the same. To this day I refuse to get on any platform, (especially Snapchat), because I know that the app will not protect those who face bullying. The tormentors will still have access to you."**
>
> - Quote from a complainant to the Minnesota Attorney General's Office

Online bullying is a primary societal concern, having been linked to numerous suicides[20] and with many parents reporting it as a top concern.[21] Bullying and harassment is often not readily perceptible by outsiders[22] as, unfortunately, there are many ways for people to harass each other online such as by reminding people of traumatizing events, revealing information that a target does not want to be known, or using coded language. As such, the best way to understand online bullying and harassment is to survey users as to whether they feel they have been targeted. Bullying is significantly more prevalent among youth, whose developing reward systems are hyper-sensitive to social stimuli[23] which magnify the impact on their well-being. In one study of 8th and 9th graders in Utah, 29 percent reported having been a target of bullying or harassment by friends or acquaintances.[24] A Pew Survey including US teens ages 13-17 found that 46 percent reported experiencing cyberbullying.[25] In a 2021 Meta survey, 28.3 percent of Instagram users reported witnessing bullying and harassment in a seven-day period, while 8.1 percent reported being a target. Among teens ages 13-15, 27.2 percent reported witnessing bullying and 10.8 percent reported being a target.[26] A recent World Health Organization report suggests similar prevalence across 44 countries with 15% of teens having experienced recent cyberbullying across platforms, which represents an increase from previous years.[27]

There are two identified product design aspects of technology platforms that facilitate cyberbullying. Online platforms provide the unique ability of anonymous strangers to contact others at scale, without the accountability or manual steps that offline contact requires. One study estimated that 40 and 50 percent of young victims of cyberbullying do not know

In a Pew Survey

46%

of US teems ages 13-17 reported witnessing bullying and harrassment in a seven-day period

In a 2021 Meta Survey

28.3%

of Instagram users reported witnessing bullying and harrassment in a seven-day period

8.1%

of Instagram users reported being a target of bullying and harrassment in a seven-day period

their perpetrator's identity and popular applications that permit anonymous messaging allow perpetrators to bully without revealing their identity to their victims.[28] Overseas groups have published some of their tactics for finding sextortion victims, which include 'bombing' prospective targets with invitations.[29] Platforms have developed policies to enforce on such harassment,[30] but those policies are often retroactive and require behaviors to conform to narrow definitions of harm. Importantly, any such enforcement is aimed at specific users and does not remedy any aspect of design leading or facilitating the harassment in the first place.

In addition to facilitating scaled frictionless anonymous contact, the algorithmic incentives of platforms also facilitate bullying. Bullying often happens within comment threads and the AI-powered incentivization of comment thread participation has been experimentally shown to increase experiences of bullying and harassment.[31] In contrast to simple engagement optimization[32] that rewards the most active users, who also tend to be more abusive,[33] platforms could amplify high reputation users, which would amplify sources that are less likely to be reported for bullying.[34]

Many consumers are having experiences with unwanted disturbing, graphic, and sexual content, often served to them by AI-Powered algorithms

> **"When she was 13, she started cutting herself. When asked why, she said that girls on Instagram talked about how it was exhilarating to cut yourself, so she did it."**
>
> - Quote from a complainant to the Minnesota Attorney General's Office

Seeing disturbing, graphic, or sexual content online is a relatively common experience with a majority of both adult[35] and youth[36] populations reporting having had negative experiences with recommended content. Many of these experiences are unintentional and occur as a result of AI-powered recommendation systems that optimize for engagement,[37] rather than explicit user preference. In a study of Australian 16-17 year olds,[38] 72 percent reported being recommended content that made them feel uncomfortable. In one study of 8th and 9th graders in Utah, 32 percent reported having seen images of violence and 31 percent reported having seen sexual content.[39]

72%
of Austrailian 16-17 year olds reported being recommended content that made them feel uncomfortable[38]

32%
of 8th and 9th graders in a Utah study reported having seen images of violence[39]

31%
of 8th and 9th graders in a Utah study reported having seen sexual content[39]

58%
of youth said they came accross pornography online by accident[42]

Internal platform studies confirm that unwanted experiences, across categories, are common. In one leaked report from Meta,[40] more than 70 percent of Facebook users reported seeing something they wanted to see less of on a regular basis, with 61 percent reporting that occurring multiple times per day and most reporting seeing such content within the first five minutes of scrolling.

Such content can be particularly harmful to youth when it is sexual in nature or concerns sensitive topics such as eating disorders or self-harm. Internal platform analyses of user complaints show that seeing too much sexually suggestive content is one of the top categories of user complaints, especially for increasingly popular, algorithmically driven short form video content.[41] According to a US study by Common Sense Media,[42] the average age of pornography exposure online is age 12, with 15 percent reporting seeing pornography at age 10 or younger. 58 percent of youth said they came across pornography online by accident. More than half of respondents said they viewed violent porn, which has been linked across dozens of studies to an increased risk of sexual exploitation.[43] Investigations by the Wall Street Journal have shown how algorithmic recommendations can lead users to be served content relating to eating disorders[44] and the sexualization of minors.[45] Meta's own BEEF survey showed that 6.7 percent of all Instagram users reported seeing self-harm content in the last seven days, but for users ages 13-15, that number rose to 8.4 percent.[46]

Internal and external studies show how the specific design choices of these platforms, whose algorithms are largely optimized for engagement rather than user preference, facilitate unwanted experiences. Controls tend to be hidden beneath layers of menus, such that they are rarely used,[47] and even when used, they often do not have the impact that users expect.[48] A Mozilla study on regretted YouTube experiences found that most unwanted content was surfaced by recommendations[49] rather than from user choice. Recommendation algorithms are largely optimized for engagement, which tends to be dominated by small groups of relatively abusive users.[50] Product changes that reduce engagement incentives have been shown to reduce exposure to unwanted content.[51] The Integrity Institute, which is a coalition of over 300 platform workers, has recommended limits on engagement-based algorithms due to their propensity to amplify harmful content.[52]

Many users experience envy and negative social comparison, which are encouraged by technology platform dynamics

> **"My daughter is 17 and has struggled with mental health issues since she was about 13, when she first started using Snapchat, Facebook and Instagram….She strives to be like the "girls on Instagram" and has resorted to body shaming herself and extreme sexual behaviors because that's what "the girls on Instagram do".**
>
> - Quote from a complainant to the Minnesota Attorney General's Office

Social comparison is a basic human process that has a long history of study in psychology.[53] Negative social comparison has been linked to increased feelings of threat and reduced psychological well-being.[54] Many technology platforms have been linked to experiences of negative upward social comparison, particularly among youth. In one study,[55] roughly half of teens expressed a desire to be "influencers." Yet, many "influencers" report unhealthy incentives to project more glamorous images than their lives really are.[56] A study by the Allianz Life Insurance Company of North America[57] found that 57 percent of millennials reported spending more money than they had originally planned due to the influence of social media. The same study found 61 percent of millennials reported feeling inadequate due to social media use and 55 percent reported experiencing a fear of missing out. A 2020 study by the Australian eCommisioner found that being deliberately excluded from groups was a top reported negative experience of teenagers.[58]

Internal studies by platforms indicate similar patterns. In one internal study from Meta,[59] over half of teens report struggling with FOMO ("fear-of-missing-out") and the study concluded that "young people are acutely aware that Instagram can be bad for their mental health yet are compelled to spend time on the app for fear of missing out on cultural and social trends." Comparisons can be made with regards to wealth, lifestyle, and also with regards to physical appearance. Approximately 70 percent of teen girls reported seeing "too much" content that leads to negative appearance comparisons. Other research has linked such comparisons to an increased risk of eating disorders.[60] Quantification of engagement within platform interfaces makes it easy to compare how popular any piece of content is and to clearly see what kinds of content get more or less social approval. In a 2024 study, 26% of youth reported that they "focus too much on numbers, followers, likes, comments, or shares on my social media".[61] 52% report feeling that they "always need to show the best version" of themselves on social media.

26%
of youth reported that they "focus too much on numbers, followers, likes, comments, or shares on my social media"[61]

52%
of youth report feeling that they "always need to show the best version" [61]

Platforms have done several tests that indicate that design choices of the platforms increase experiences of negative social comparison. For example, based on the results of Instagram's Project Daisy, where like counts were hidden for a random sample of the population, the decision to provide comparative like counts leads to a 2 percent increase in negative social comparisons.[62] Teens with reduced well-being are more likely to be affected by engagement metrics that allow

for comparison, with one study finding they were more than three times as likely to "feel bad about themselves if no one comments on or likes their posts" or to "have deleted social media posts because they got too few likes".[63] Researchers at a Canadian children's hospital found[64] that experimentally reducing social media use significantly improved body image for teens and young adults. As detailed in the civil enforcement action the State brought against Meta, Meta's internal and external research allegedly both stated that allowing visual effects that mimic plastic surgery were likely to have negative effects on well-being, especially for young women.[65] Broadly, engagement-based algorithms tend to reward content that depicts wealth, glamor, and beauty,[66] and several companies have acknowledged the risk of being continually exposed to such content.[67]

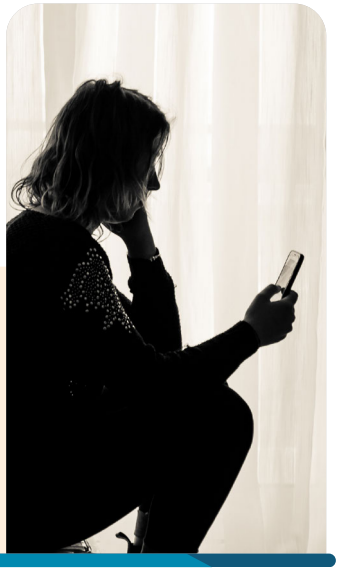
Many cases of manipulation and fraud begin with unwanted contact, facilitated by loose privacy defaults and high rate limits, with especially serious consequences for young people

> **"On more than one occasion, while I was a minor I had received sexually explicit photos from men who added my account. I did not need to add them back to see the image they had sent me. No minor should ever be subjected to this….until the company makes changes, more minors will unfortunately get sent these unwanted pictures."**
>
> - Quote from a complainant to the Minnesota Attorney General's Office

Both parents and teens report serious concerns about the ability of abusive users to find and contact youth. There are many documented cases[68] of foreign individuals targeting youth online, such that the FBI recently issued a public safety alert.[69] In one study of adolescents in Utah,[70] 26 percent reported getting involved in an unwanted conversation and 17 percent reported a stranger trying to meet them. A recent study by the UK's OfCom showed similar numbers with 30% of youth reporting having received "unwelcome friend or follow requests or messages" over a 4-week period.[71] Generally, per a Common Sense Media report,[72] youth report the ability of strangers to contact them as having a negative effect. Once contacted, youth are particularly vulnerable to being manipulated.[73]

These trends are corroborated by internal research by technology platforms. Per internal research detailed in the Wall Street Journal,[74] one in eight users under the age of 16 said they experienced unwanted sexual advances on Instagram. These unwanted messages are facilitated by relatively lax default privacy settings which benefit companies by facilitating more social interactions. Friend lists are made public to increase new connections, but also are used by harassers to threaten exposure of unwanted images to friends.

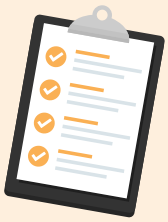
Unwanted contact is also facilitated by the capabilities that platforms provide new untrusted users to contact numerous strangers without the limits that exist in offline life,[75] where such behavior would have negative consequences. In contrast, having a history of trustworthiness plays an important part in reducing risk across domains,[76] including in internal social media research.[77] Platforms have intermittently acknowledged this risk by removing capabilities for untrusted users during times of stress, but such product changes are often ad-hoc. Criminal



In a Study of Adolescents in Utah

26%
reported getting involved in an unwanted conversation[70]

17%
reported a stranger trying to meet them[70]



Per the Wall Street Journal

12.5%
of users under the age of 16 said they experienced unwanted sexual advances on Instagram[74]

networks that target youth have published playbooks that specifically show how they take advantage of platform design features, such as the ability to mass contact others and to view targets' friend connections.[78] A safer platform ecosystem would reduce the risk of untrusted actors contacting large numbers of strangers, requiring a positive explicit feedback history (reputation) from a broad set of other users before allowing users to affect people they do not already know. In response, many platforms have functionality that limits unwanted contact by new users, but those limits are not robust across platforms.[79]

Platforms facilitate the misuse of user information and images, including that of younger users

> **"I started out following some family influencer pages. And I noticed that some parents are exploiting their daughters, having these young girls pose in leotards and bikinis, and using Instagram to get subscribers to pay for more 'exclusive content.'"**
>
> - Quote from a concerned parent in the New York Post[80]

Recent press articles[81] based on investigations from Stanford University[82] and the University of Massachusetts[83] have highlighted how technology platforms facilitate the unwanted sexualization of many users, including youth. Unfortunately, some of these cases even involve the parents of those users who seek to monetize attention. In one 2021 study in Utah,[84] conducted before generative AI tools were widely used, 6 percent of 8th/9th graders reported having their photos used in an inappropriate way. In a Pew study,[85] "others posting things about you or pictures of you without asking permission" was one of the top complaints about Facebook (36 percent strongly disliked). A 2023 Snapchat study found that 12% of youth were willing to report that they had shared intimate imagery of themselves and 33% of those youth reported losing control over those images, with younger teens and boys being at higher risk.[86] Numerous state attorneys general, including Minnesota's, have recently written about the increased urgency of these problems given the ubiquity of generative AI[87] and over the past year, these concerns have unfortunately become realized (see Section Four for more detail).[88]

In some cases, the sexualization of youth is a direct result of incentives that platforms encourage and foster through facilitating monetary rewards for popular content creators. Engagement-based algorithms reward sexually suggestive content with greater distribution, which translates to ad revenue for creators of such content.[89] Without that monetary incentive, such content would have less incentive to be created. The display of the number of likes and shares that a piece of content has received means that youth can easily see the high engagement that sexually suggestive content receives, which researchers have shown can trigger a desire for similar levels of attention.[90] Access to content that can be misused is also often facilitated by a lack of privacy defaults and high rate limits that allow untrusted actors to collect information from others, including youth, and misuse it, in order to create content that others will want to consume.

6%
of 8th/9th graders in a 2021 Utah study reported having their photos used inappropriately[84]

36%
of respondents to a Pew study strongly disliked "others posting things about you or pictures of you without asking permission"[85]

12%
of youth in a 2023 Snapchat study were willing to report that they had shared intimate imagery of themselves[86]

33%
of those youth reported losing control over those images[86]

Excessive and compulsive use of technology, facilitated by systems that are optimized for time and attention, displaces beneficial activities like sleep and in-person socialization

> **"I have two teenagers, one is diagnosed with ADHD, Depression and anxiety. We have Bark to help monitor our kids usage but we only use it to shut off their phones or give them approved more time. They constantly sneak passwords and figure out ways to bypass the system....I feel they give no attention to their schoolwork or even care about it. I see their attention spans have decreased. They cannot focus on a person talking to them."**
>
> - Quote from a complainant to the Minnesota Attorney General's Office

52%
of Minnesota college students reported having an issue with excessive computer/ internet use[91]

49%
of those reporting having this issue saying that it impacted their academic performance[91]

50%
of teens reporting at least one symptom of clinical dependency on social media[94]

50%
of Minnesota college students report getting adequate sleep on three or fewer days a week[95]

93%
of Gen Z admit to staying up past their bedtime due to social media[96]

59%
of teens use their phones between midnight and 5:00 a.m. on school nights[97]

Many users, especially youth, report using technology more than they would ideally like, leading to negative consequences in their life. For example, a 2024 study of Minnesota college students found that 52 percent reported having an issue with excessive computer/internet use with 49 percent of those reporting having this issue saying that it impacted their academic performance.[91] A 2022 Pew study found that 36 percent of teens say they use too much social media and that 54 percent say that it is hard to give up.[92] In a study of parents by Accountable Tech,[93] 23 percent reported that their kids were "addicted to the phone." Per the American Psychological Association, recent research shows over 50% of teens reporting at least one symptom of clinical dependency on social media.[94]

Sleep, in particular, is widely reported to be affected by technology use. For instance, 50 percent of Minnesota college students report getting adequate sleep on three or fewer days a week.[95] Youth who report reduced days of adequate sleep also report a reduced ability to manage stress. The American Academy of Sleep Medicine reports that 93 percent of Gen Z admit to staying up past their bedtime due to social media.[96] In a Common Sense Media study, 59 percent of teens use their phones between midnight and 5:00 a.m. on school nights, with a median usage of 20 minutes per night.[97] Tiktok was specifically reported as being overstimulating, leading to difficulties in falling asleep. Per internal Meta research detailed in the Attorney General's recent lawsuit,[98] "when social media use displaces sleep in adolescents, it is negatively correlated to indicators of mental health."

Design features of technology platforms, such as infinite scroll, excessive notifications and auto-play videos, facilitate increased usage, beyond the desires of users. Per a former company executive's statements,[99] these features were designed intentionally to increase time spent through features that "give you a little dopamine hit every once in awhile." Cognitive psychologists[100] have tied features of smartphones and social media to dopamine reward systems. In a Common Sense Media study, many youth report using tactics to increase the number of steps required to access content and reduce interruptions due to notifications.[101] In a typical day, participants in a Common Sense Media study received a median of 237 notifications, with 5 percent (over 10) arriving at night.[102] Instagram uses an array of push notifications that require users to navigate complex settings in order to disable.[103] Many algorithms within technology platforms are designed to maximize users' time spent on the platform.[104] Based on experiences with these systems, one study found that 72 percent of teens believe that tech companies manipulate users to spend more time on their devices.[105] Another found that 73 percent of youth report reaching for social media "unconsciously" when bored and 49% reporting that they "can't control their use or end up using social media for a longer period of time than they originally wanted to".[106]

Algorithms often exhibit bias, and the integration of increasingly powerful AI into more algorithms is likely to accelerate this trend

> **"Facial recognition systems are even more unreliable and racially biased than we feared"**
>
> - Rep. Bennie G. Thompson (D-Miss.), commenting on a federal study of facial recognition systems that are being used increasingly by law enforcement.[107]

Algorithmic systems reflect biases in training data, which is the data that is used to teach AI or machine learning algorithms how to make proper decisions. For example, hiring algorithms that use data from recruiters learn the biases of those recruiters.[108] Unfortunately, there is little visibility of training data being provided to those in society who are ultimately affected by these algorithms, though recent AI legislation in the EU and across states may eventually provide this visibility. As a result of concern about this bias, many reports and laws have been written to address potential discrimination from algorithmic systems in domains such as medicine,[109] workplace hiring,[110] government decision making,[111] insurance,[112] content moderation,[113] and criminal justice decision making.[114] Biases typically disproportionately affect minority and disadvantaged populations whose data is not adequately represented in training data. As AI systems become more powerful, the temptation to integrate these systems into more domains will increase, magnifying the risk of bias in an increasing number of settings. Technology companies cause these biases through the use of non-representative training datasets[115] or mis-specified objective functions[116] and so society has a role to play in overseeing such technological decision making.

Specific groups often experience more acute harms

The effects of Emerging Technology on Youth Well-Being are not homogeneous. Specific groups often experience distinct harms, which, due to their specificity, often are more impactful than the general experiences that all young people experience. Platform design shapes these experiences, such that addressing platform design is even more important for improving these specific group's experiences.

Girls and young women often have worse online experiences, including gender-based harassment and negative image comparisons

Broadly, women report having worse online experiences than men. A 2020 Australian study of teenagers' online experiences found that 47% of young women and girls reported a negative online experience over the past six months, compared to 41% of young men.[117] An internal Meta study of platform behavior among new users found that across countries, women and girls tended to engage in more platform behaviors (*e.g.* hiding, blocking, reporting) indicative of negative experiences.[118] American women engaged in these behaviors 30% more than men.

Many researchers have highlighted the particular effects of social media on teenage girls[119] and teenage girls are more likely to use platforms such as TikTok, Instagram, and Snapchat,[120] which are more social in nature. Many meta-analyses show greater relationships between negative mental health outcomes for teenage girls compared to teenage boys.[121]

Austrailian teenagers reporting a negative online experience over the past six months[117]

47% females

41% males

13-15 year olds reporting feeling "worse about yourself because of other people's posts on Instagram"[122]

27.4% females

14.6% males

Social comparison processes may be responsible for these effects. In an internal Meta study,[122] younger and female users reported much greater rates of feeling "worse about yourself because of other peoples' posts on Instagram," with 27.4% of 13-15 year old females reporting this experience over a 7-day period, compared to only 14.6% of males in the same age group. Many studies have linked unrealistic, sexualized body images to negative mental health outcomes amongst young girls.[123] Such content also exists in traditional media, but personalized engagement-based feeds, which are unique to social media, have been found in both internal[124] and external[125] studies to increase young women and girls' exposure to this content.

Harassment is not necessarily experienced more by young women but can be more impactful when encountered. In an internal Instagram study, 13-15 year old boys report being a target of bullying more often than girls their age, but girls were more likely to know the bully offline, suggesting that it may be part of a pattern of bullying rather than an individual incident of harassment. Harassment of young women and girls also often weaponizes their gender, with harassment of women and girls often being sexualized and often restricting their free expression.[126] A 2020 study by The Economist Intelligence Unit[127] found that 85% of women globally reported witnessing online attacks against women, with 38% reporting a personal experience. Younger women were more likely to report experiencing online attacks against them, with 45% of Gen Z/Millennial women reporting a personal experience. As with all forms of bullying and harassment, design features like optimizing for engaging comments enables small groups of trolls or bullies to hyper-engage and amplify each other, facilitating these experiences.

85%
of women globally reported witnessing online attacks against women[127]

38%
of women reporting a personal experience with being attacked online[127]

45%
of Gen Z/Millennial women reporting a personal experience with being attacked online[127]

Boys and young men are often targeted for sextortion and misogyny

Two particular online harms often target young men and boys. Boys are often targeted by scammers pretending to be attractive women to solicit intimate photos and then use their photos to extort them for money. These "sextortion" schemes have increased in recent years, with primary targets being males between the ages of 14 to 17, and at least 20 documented cases ending in the boy taking his own life.[128] The playbook for sextortion has been widely discussed online[129] and includes taking advantage of several design features of social media platforms, like the ability of strangers from other countries to impersonate young women and befriend young people en masse, as well as the default visibility of contacts lists to allow strangers to make connections, which enables the discovery of new targets and provides a distribution list for exploitive materials. Instagram has acknowledged that the broad ability for anyone to contact minors is risky by setting stricter privacy settings for minors as part of efforts to counter sextortion.[130] Still, many of these efforts require the identification of accounts that are specifically suspicious, which historically has meant that many accounts go uncaught.[131] Default settings that prioritize user privacy instead of relying on active identification and reporting of every bad actor would provide more robust protection.

Young men and boys are also often targeted for extreme discussions of gender, which often have misogynistic components. In one 2023 study,[132] 40% of men reported trusting influencers who spread misogynistic messages, with influencers like Andrew Tate—who was banned from several platforms after repeatedly describing and encouraging violence towards women[133]—having particular appeal for the youngest age group surveyed (ages 18-23). These influencers often appeal to men and boys who may be having financial issues, be lonely or be unable to engage in dating as desired,[134] and personalized engagement-based algorithms often match these vulnerable young men and boys to these influencers,[135] who profit from the resulting attention.[136]

40%
of men reported trusting influencers who spread misogynistic messages[132]

These communities not only spread harmful ideas to these young people, limiting their ability to have healthy relationships with women in the future, but the young people within these communities also then go on to harass women both online and in real life.[137]

Minority and LGBTQ+ groups find community online but also report more negative experiences

Social media is seen as a double-edged sword by diverse communities, per a 2024 Common Sense Media report,[138] with important and unique benefits that come from finding support and community, but also unique challenges. Latino and Black young people report that social media is more critical for connection, expression, and learning compared to White youth. They are also much more likely than White young people to report taking a break or stopping using social media due to harassment concerns. In Minnesota, an effort to Reimagine Black Youth Mental Health engaged over 200 young people who identified safety as a key component of mental health, and safety on social media from bullying as a key area for improvement.[139]

A similar double-edged sword pattern can be found for LGBTQ+ youth.[140] LGBTQ+ youth report more likelihood to see comments that affirm their identities and/or that are body positive. They also report more likelihood to see homophobic, body-shaming, or transphobic comments, as compared to non-LGBTQ+ youth. A survey of NYC youth found that LGBTQ+ youth were particularly likely to report being bullied online.[141] A national survey found that LGBTQ+ youth were three times as likely to experience unwanted and risky online interactions.[142] In a recent national poll, LGBTQ+ respondents were more likely to say that social media had a negative impact on their emotional health (47% vs. 35%).[143]

Latino (16%) and Black (185) teens also report being more likely to use chatbots[144] and text generators on a daily basis, as compared with White teens (8%). This usage may enable them to supplement their educational needs, but also leaves them susceptible to new harms that may result from the use of chatbots. Generative AI may prove to be the same double-edged sword in these communities.

Across groups, youth report a desire to control their social media experiences, with 76% in one study reporting taking steps to control content they do not want to see over the past year.[145] LGBTQ+ youth report greater efforts to control and curate their feeds. Still, even with those efforts, LGBTQ+ youth are more likely to report "reaching for social media without thinking about it" (78% vs. 73%), that social media "gets in the way of my sleep" (56% vs. 42%), and a lack of control such they "end up using (social media) for a longer period of time than I originally wanted to" (63% vs. 47%). Given that LGBTQ+ youth report greater attempts at control as well as a self-reported lack of control, improving the ability to more explicitly control social media would likely particularly improve the LGBTQ+ experience. Unfortunately, controls are generally lacking on social media platforms, with recommendation systems optimizing on behavior as opposed to explicit preference.[146] Where existing controls do exist, several external studies have found them to be ineffective and inadequate.[147]

LGBTQ+ Youth

78% vs. 73%
report "reaching for social media without thinking about it"

56% vs. 42%
report that social media "gets in the way of my sleep"

63% vs. 47%
report a lack of control such they "end up using (social media) for a longer period of time than I originally wanted to"

Section Two: The legislative and legal landscape

In this section, we provide more detail as to the many specific legislative efforts that are occurring across jurisdictions. In 2024, several legal cases were decided with regards to legislation. We review those efforts and decisions to inform what we can learn and how those learnings ladder up collectively to our recommendations in the next section.

Social media regulation

The United States is far from the only nation now grappling with how to protect its citizens from the harms of social media, with jurisdictions including the United Kingdom, the European Union, and Australia passing legislation imposing new obligations on social media platforms. In the United Kingdom, the Online Safety Act imposed multiple new duties of care, including required risk assessments and reporting, onto online services to further the goal of identifying and removing illegal or legal but harmful content.[148] There are further requirements for services that are "likely to be accessed by children" and for the largest platforms. Critics of the Act maintain that "lawful but harmful" speech is too broad a category, one that will effectively allow the government to censor legal speech, and are concerned that some requirements will undermine users' privacy.[149] In 2024, OfCom, the regulatory body tasked with implementing the Online Safety Act, introduced its draft Children's Code of Practice[150] which aims to address harmful content and harmful contact. It aspires to ensure that regulated services are "safe by design", including several recommendations that overlap with this report. In particular, it addresses the design of recommendation systems that may recommend harmful content, and among the draft standards is the recommendation that platforms allow for negative feedback for unwanted forms of content.

In the European Union, the Digital Services Act ("DSA") has similar goals and uses similar methods to regulate illegal content and disinformation. The Act requires technology platforms to disclose to regulators how their algorithms operate and provide transparent standards for targeted advertising and content moderation.[151] Critics of the Act have expressed concerns about users' privacy protections and about the Act's lack of clarity, though many have heralded the Act's focus on increasing transparency of platforms' decision-making.[152] The enforcement body responsible for this Act is now in the process of consultation on their specific code of practice for Article 28, which calls for the online protection of minors.[153] This report has been submitted to regulators at several steps within their consultation process and we are hopeful that the code of practice that is finalized reflects similar observations about harmful design patterns. To date, little has changed with regard to the operation of platforms, though DSA enforcers have prevented potential new risks, such as a plan by TikTok to reward users for engagement that likely would have led to more unwanted usage.[154] Several investigations have also been launched that may lead to required changes within platforms.[155]

In Australia, the Online Safety Act 2021 introduced Basic Online Safety Expectations for technology platforms to minimize bullying and other harmful content online and strove to make it easier for users to submit and receive answers about harmful content they see online.[156] The Act further required technology platforms to develop new codes to scan for illegal and harmful content, such as graphic sexual or violent imagery. Much of the impact of the act has been through individual complaints fielded by the Australian regulator, with the implementation of more robust "Safety by Design" principles largely being voluntary.[157] Pressure from parents and civil society has led to renewed efforts to mitigate harmful technological effects and so Australia is now considering fully banning social media for children under a certain age,[158] which some

International Legislation

European Union
- Digital Services Act
- General Data Protection Regulation
- Artificial Intelligence Act

United Kingdom
- Online Safety Act 2023
- Age Appropriate Design Code 2020
- Children's Code of Practice 2024

Australia
- Open Safety Act 2021

have opposed due to possible unintended negative effects.[159] Our recommendations to enable voluntary device-based age settings would provide a privacy safe mechanism for enacting some of these proposed reforms.

In the absence of a global standard, some countries have responded to online harm by imposing restrictions and penalties on users who facilitate online harm. These laws have been challenged by civil society groups who do not trust the government's judgment in restricting speech, and who point to many specific instances where governments have engaged in authoritarian restrictions. Civil society groups in diverse countries, including India,[160] Sri Lanka, Kenya, Israel,[161] and Brazil, have all highlighted the potential for abuse by governments who are likely to define misinformation and violence incitement in terms of their own political views.

Broadly, we have yet to see a major impact as a result of these laws and regulators have expressed disappointment with companies' compliance to date.[162] These laws generally defer specific implementation of improved technology design, following more detailed rule making or risk reporting by companies. Given the uncertain impact of requiring companies to self-report risks[163] and the required administrative effort to process such reports, we suggest that the State of Minnesota plainly direct the design requirements of companies within legislation. Such clear guidance would also address constitutional issues identified by courts regarding the non-specific reporting requirements in California's Age Appropriate Design Code.[164]

Content regulation in the U.S.

Within the United States, some states have adopted international precedents' focus on moderation of harmful content. However, these have thus far faced opposition and largely been unsuccessful in the face of First Amendment concerns.

In 2021, Florida passed State Bill 7072, which would prohibit platforms from banning any "journalistic enterprises" operating in the state or candidates running for public office.[165] The law was challenged shortly after it was passed, and a federal judge for the District Court of the Northern District of Florida granted a preliminary injunction halting the law from going into effect.[166] The Eleventh Circuit Court of Appeals upheld the injunction in May 2022.[167]

Texas passed a similar bill, Texas House Bill 20, in 2021, which prohibited social media platforms from censoring content based on viewpoint and required platforms to provide transparency reports about their content moderation policies.[168] As in Florida, the law was promptly challenged in court, and the federal district court judge granted a preliminary injunction enjoining the law.[169] The Fifth Circuit Court of Appeals granted a stay of the injunction, allowing the law to take effect, and the petitioners sought certiorari from the United States Supreme Court to reinstate the injunction.[170] The Supreme Court vacated the appellate court's stay, allowing the injunction to remain in place.[171] In response, the Fifth Circuit Court of Appeals ruled that the regulated content did not constitute speech under the First Amendment, thus creating a circuit split.[172]

In response to this circuit split, the United States Supreme Court agreed to jointly hear the cases relating to Florida and Texas' laws. *Moody v. NetChoice* and *NetChoice v. Paxton* were heard together in oral argument on February 26, 2024.[173] While the decision in this case did not fully clarify what specific aspects of a social media platform

United States Legislation

Within the United States, some states have adopted international precedents' focus on moderation of harmful content. However, these have thus far faced opposition and largely been unsuccessful in the face of First Amendment concerns.

Federal Legislation
- Protecting Americans from Foreign Adversary Controlled Applications Act
- The Kids Online Safety Act

Content Regulation
- Florida
- Texas

Social Media Age Limits
- Montana
- Ohio
- Arkansas

Social Media Reform Focusing on Minors
- California
- Deleware
- New York
- Utah

Privacy and Data Protection
- California
- Minnesota

AI Specific Legislation
- lawmakers in at least 45 states and the District of Columbia introduced bills related to AI
- at least 31 states adopted resolutions or enacted legislation in 2024

could be regulated, it did discuss the importance of distinguishing between a platform's function and its expression.[174] The Court addressed this distinction between function and expression by emphasizing that "curating a feed and transmitting direct messages. . . involve different levels of editorial choice, so that one creates an expressive product, and the other does not." Thus, future legislation that regulates the function of social media platforms should withstand constitutional scrutiny.

The Supreme Court refrained from determining what components of social media are function vs. content based. They did, however, cite case law[175] that concluded that the act of curating or compiling a third party's speech is an expressive activity and therefore protected by the First Amendment. They reasoned that this is because expressive conduct necessarily includes exercising editorial discretion. They also cited case law that concluded that editorial choices may not be regulated to require inclusion of messaging that they choose to exclude. The Court heavily relied on Hurley v. Irish American Gay, Lesbian, and Bisexual Group of Boston, Inc. to illustrate that it is unconstitutional to force an entity to include messages it chooses to exclude.

Several justices also discussed what aspects of a platform would be considered functional and therefore not protected. Justices Barrett and Jackson both noted that each social media platform is complex, distinct, and may require individualized analysis. They also argued that for a function to qualify as a protected form of speech it must be inherently expressive and suggested that functions that are not inherently expressive can be regulated in the future. Building on this decision, US District courts have concluded that many aspects of platform design, including engagement-based algorithms, are indeed not expressive, given that no message is intended to be conveyed, and therefore such design elements are subject to regulation.[176] Broadly, the decision pointed to the need for more information to help understand the functionality of platforms, including new AI enabled platforms. In so far as this report describes the discrete functionality of platforms and how they interact with the state's interest in protecting minors, it is hoped that this report can help fill that gap.

Social media age limits

Strict age limits for social media have been controversial, even amongst those who acknowledge the scope of online harm, and several states have passed or considered an age limit on social media. Montana passed a law that set strict age limits on TikTok,[177] though a federal judge granted a preliminary injunction enjoining the law in November 2023.[178] Ohio and Arkansas also passed laws restricting access to social media based on age limits, and both laws were also enjoined on first amendment grounds.[179]

A US federal law that mandates the sale of TikTok was challenged unsuccessfully in court, with the United States Supreme Court holding that the law was content neutral and did not violate the First Amendment.[180] Internationally, calls for age limits for social media have drawn concerns about restricting the benefits for individuals who use social media for social support or essential information as well as concerns from child's rights advocates who fundamentally do not believe in restricting children's access to information.[181]

It is likely that any law that strictly limits access to social media platforms, in part or in whole, will continue to face political opposition, legal challenges and First Amendment concerns.[182] As such, our recommendations do not advocate for any new state-wide restrictions on social media. Policies like requiring device-based age settings would enable existing regulations, such as the Children's Online Privacy Protection Act, to be more robustly enforced. Design-based mandates would enable youth—who often acknowledge and want to control their own excess usage—would likely face fewer challenges. And school-based mandates would likely provide a needed break from social media for youth as well at least during the school day.

Social media reform focusing on minors

Congress has considered the unique harms to children online in recent years. The Kids Online Safety Act ("KOSA")[183] is a bill introduced first in 2022, which passed the Senate in 2024, with bipartisan and presidential support, but ultimately stalled in the House.[184] KOSA would apply to online platforms that are likely to be used by minors, and would require platforms

to restrict access to minors' personal data and provide parents with access to supervision and control of minors' privacy settings.[185] Social media platforms would also be required to provide information about targeting advertising practices and prohibit advertising of age-restricted products (such as tobacco and gambling) to minors. Critics of the bill have expressed concerns about censorship, and there has already been disagreement about the type of content that would constitute harm to children.[186] For example, a co-author of the bill Senator Marsha Blackburn (R-TN) has suggested that the bill would be used to censor content about the LGBTQ+ community and critical race theory.[187]

The United Kingdom enacted the Age Appropriate Design Code in 2020, which requires online services likely to be accessed by minors to make design choices in the "best interests" of children's safety and privacy.[188] Online platforms are required to set minors' accounts with the strongest privacy setting options by default (and must not use deceptive patterns to nudge minors towards lower-privacy settings), and to only collect data that is strictly necessary to deliver their product from minors. Furthermore, online services cannot engage in location tracking of minors, present minors with targeted advertising or curated algorithms, or disclose minors' data to third parties absent compelling reasons to do so.[189] Online platforms have adapted to these new requirements. For example, on Instagram, adults may not send private messages to any minors unless they are followers, and minors' accounts are marked private by default. TikTok has stated that it will comply by not sending push notifications to minors during evening and nighttime hours. YouTube now treats all videos designated as "made for kids" with child-friendly features, such as disabling autoplay and targeted advertising.[190]

Building on the UK Age Appropriate Design Code, California passed a similar law in 2022. The California Age Appropriate Design Code would put additional requirements on businesses that provide online services, products, or features likely to be accessed by children, including configuring higher level default privacy settings as well as completing data impact assessments.[191] Before the law could take effect, NetChoice—a technology company trade association with members that include Meta and TikTok—filed suit against the state alleging First Amendment violations and asking the court for a preliminary injunction.[192] The court granted the preliminary injunction, finding that the Age Appropriate Design Code does regulate expression and speech in violation of the First Amendment.[193] The court also expressed concern that the Act might cause greater harm by mandating increased collection of private data.[194] The State of California appealed to the Ninth Circuit Court of Appeals in October 2023.[195] In 2024, the Appeals court ruled that the primary mechanism of enforcement—Data Privacy Impact Assessments—were "compelled speech" in part because those impact assessments required judgments of content. The court did not rule on the specific design prohibitions in the law.

Other states have enacted bills to protect minors' data privacy. In 2023, Connecticut passed a law that, among broader data privacy provisions, limited targeted advertising and geolocation data collection of minors' data, and also required data protection assessments of the heightened risks of minors' data.[196] Delaware's general data privacy act also prohibits sites from marketing specific products, including alcohol and tobacco, firearms, and body modifications, to children.[197] New York passed a similar bill that prohibits sites from collecting, using, sharing, or selling minors' personal data for purposes of targeted advertising without consent.[198]

States are also enacting legislation regulating children's social media use and access. Utah passed the Social Media Regulation Act in 2023, which would require parental consent from users under the age of 18 to create social media accounts and compel social media companies to restrict minor access to accounts from 10:30 p.m. to 6:30 a.m.[199] Utah repealed and replaced the law in response to constitutional concerns, but the law was nonetheless again enjoined by the court as violative of the First Amendment because it found it regulated "social" speech.[200]

Other jurisdictions have also passed laws to protect minors. New York and California have passed bills that would specifically regulate algorithmic feeds for minor users and allow parents some control over minors' social media accounts. The Stop Addictive Feeds Exploitation ("SAFE") for Kids Act restricts "addictive feeds" for minor users of social media platforms, with addictive feeds being defined as feeds which use the personal data of a user to prioritize content.[201] The Act also prohibits sending notifications to minors during nighttime hours without parental consent. This statute attempts to address the addictive quality of algorithmic feeds, particularly on minors' still developing brains.[202] Since this act targets the functionality of these feeds, based on what data is ingested, rather than the expressive output, the authors of these bills are hopeful that they will continue to pass constitutional review.[203]

In general, there are successes to be built on from these bills, in particular the UK Age Appropriate Design Code, which led to notable broad protections for children. However, more remains to be done and the broad "duty of care," which KOSA and the California Age Appropriate Design Code share, has proven controversial and been subjected to legal challenge. A more specific elaboration of the functional design changes that companies should undertake could lead to reduced opposition and legal challenges. Such elaboration needs to be done with care to navigate the constitutional challenges laid out by previous laws, but notably, the Supreme Court has laid out a path for the regulation of functional design. Even if deemed constitutional, some laws recommend specific changes that may not be effective[204] and so we suggest a level of specificity that constrains misuse and charges of vagueness, while also making room for the evolution of technological contexts and solutions. By specifying principles around issues of privacy, engagement optimization, user empowerment, minor identification, and including non-mandated opportunities, we aimed to strike the right level of balance between specificity and flexibility within our recommendations.

Privacy and data protection

Many jurisdictions have passed laws intended to protect consumers' data online. The General Data Protection Regulation,[205] passed by the European Union in 2016, has served as a model both internationally and within the United States.[206] Several states, beginning with California in 2018, have passed comprehensive data privacy bills that outline specific consumer rights about their data, including the right to know what personal information a business collects about them, to whom their personal information is sold, and the right to opt-out of these sales.[207] Other states have passed similar legislation, including Minnesota, which passed the Minnesota Consumer Data Privacy Act in 2024.[208] It is one of many state privacy laws that have passed or gone into effect in 2024.[209] The Minnesota act provides the option for consumers to opt-out of or delete their data from numerous data broker practices. It also sets default protections for children ages 13-16 and generally concerns harms that occur when businesses exploit consumer data. Our recommendation to mandate default settings with greater privacy protection complements the consumer rights protected by these bills, by adding protections for when other online users exploit user data.

AI-specific legislation[210]

United States AI legislation

As Generative AI gains adoption, the United States has largely attempted to regulate AI through executive action and state legislation. President Biden issued Executive Order 14110, on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, on October 30, 2023.[211] This Executive Order directs 50 federal agencies to help "guide responsible AI development and deployment" over eight policy goals, including safety and security, worker support, consumer protection, and privacy. The National Institute of Standards and Technology ("NIST") has released several reports on AI risks, in collaboration with industry and academia, but the standards they release are not binding. Biden's Executive order was subsequently revoked by the next administration.[212]

As AI has become more widely integrated into society, lawmakers in at least 45 states and the District of Columbia introduced bills related to AI, and at least 31 states adopted resolutions or enacted legislation in 2024.[213] Among the most prominent themes across state regulation are the regulation of deep fakes, the mitigation of algorithmic bias, the use of AI within government and schools, the specific protection of children from exploitation, and the further study of emerging AI harms.

45 states introduced bills related to AI[213]

31 states adopted resolutions or enacted legislation related to AI[213]

20 states enacted laws related to the use of deepfakes in elections

31 states enacted laws addressing sexual deepfakes

Several states and municipalities in the U.S. have passed or introduced legislation about potential bias in the use of AI, citing civil rights concerns about its use. New York City Local Law 144, enacted in 2023, restricts employers with a physical office in the city from using automated employment decision tools in hiring and promotion decisions unless an independent third party has audited it, and further requires employers to publish a public report of their annual audit and to notify candidates about their use of automated decision tools.[214] In 2024, Illinois passed a similar law.[215] California considered similar legislation to prohibit automated decision tools that result in algorithmic discrimination on the basis of race, sex, disability, or other protected classifications, but that bill did not pass in part due to opposition from business groups.[216] In May of 2024, Colorado passed SB 205 with a goal of preventing algorithmic discrimination from high risk systems.[217]

Other states have also discussed legislation relating specifically to the use of deepfakes, often with a focus on high harm cases—including within elections and for the production of sexual content.[218] Per a tracker maintained by MultiState.ai, 20 states had enacted laws related to elections and 31 states had enacted laws addressing sexual deepfakes as of October of 2024. For example, Michigan enacted a bill in 2023 requiring disclaimers of AI in political advertising. Pennsylvania introduced a bill that would criminalize some categories of AI-generated sexual imagery, including content involving minors.[219] Most laws regarding the regulation of AI-generated deceptive media in political communications require disclosure, with only 2 states (Minnesota and Texas) prohibiting the dissemination of deceptive deepfakes immediately before an election.[220] Regarding sexually explicit deepfakes, states have generally either criminalized the dissemination of non-consensual sexual imagery,[221] provided a private right of action,[222] or in Minnesota's case, done both. Some states have also clarified their existing CSAM laws to specifically include deepfakes of minors.[223]

Minnesota's laws combine aspects of laws that exist across states, including addressing deepfakes in both election and sexual contexts. These laws provide important protections from harms that have been recognized as societal concerns across jurisdictions, but there remain opportunities to further extend protections. The current law mixes provisions on sexual content, which extend protections that have been upheld by courts,[224] with provisions that relate specifically to political speech, which have led to court challenges.[225] Harm from non-consensual deepfakes does not need to be sexual, election related, or even visual in nature to be perceived as harmful. For example, one recent case of harm involves a family whose murdered daughter is being impersonated by a chatbot.[226]

A Tennessee law[227] that prohibits all unauthorized use of deepfakes entitled the "Ensuring Likeness, Voice, and Image Security Act of 2024" ("ELVIS"), may provide inspiration in that it builds on established statutes to protect against the unauthorized use of an individual's image, likeness, and also voice. It also adds liability for tools whose "primary purpose or function" is to replicate an individual's persona without authorization as well as for providers that distribute, transmit, or otherwise make available" such content. It contains specific exclusions for fair use and speech that may be protected by the First amendment. Legal analysts[228] have suggested that more clarity could be added to the law and there exist opportunities to clarify the responsibilities of distributors, in a way that is consistent with Section 230, as well as to clarify that the law specifically applies to any usage that is sexual in nature.

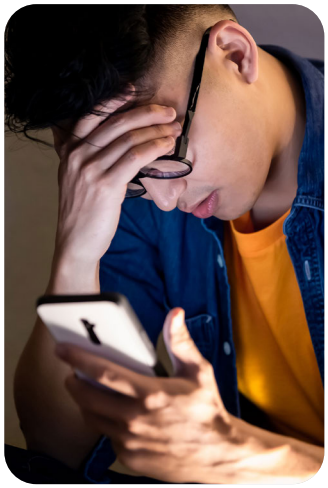
Given AI's rapidly evolving nature, many states, including Texas, Hawaii, Connecticut, and Rhode Island, have passed legislation creating task forces and councils to further study AI and make recommendations for state agency use.[229] This report is made possible by legislation passed in Minnesota that similarly mandates the study of emerging technology, including AI.

States have been grappling with legislation around AI in a number of ways, and we expect to see a greater variety of legislation in the coming years. Our recommendations build upon the harms identified across laws by addressing the most harmful current issues, such as the use of AI within engagement-based algorithms, the increasing use of chatbots by teens, and the use of generative AI for non-consensual sexual imagery. Many laws also attempt to anticipate future risk. By mandating product experiment transparency and measuring user experiences with AI, we are hopeful that our recommendations can help inform future laws while respecting that we may not be in a place to fully anticipate future uses of AI technology nor its intended or unintended consequences and harms.

International AI legislation

The most significant AI regulation was passed in the European Union, which passed the Artificial Intelligence Act to regulate AI across a broad range of sectors. The Act was proposed in 2021, passed by the Council and Parliament in December 2023, and implementation is currently underway, though most obligations are voluntary before full implementation occurs in 2026.[230] The EU AI Act features a risk-based approach with four defined risk categories, banning those applications deemed to be an "unacceptable risk" (including facial recognition and other biometric identification and social scoring), enforcing government evaluations for those deemed "high-risk" (including AI used in health, education, and law enforcement), and instilling transparency requirements for "general purpose" and "limited risk" applications of AI.[231] Among the transparency requirements are disclosures for when human beings are interacting with chatbots or content that has been generated by AI, which mirror laws that have been passed in the United States. The EU's regulatory model is being watched and considered by other countries, such as Brazil, where a similar risk-based approach is being considered.[232]

Section Three: What can we learn from previous legislative efforts?



Given the widespread negative experiences reported above, numerous jurisdictions have attempted to address the impact of technology on society, with a focus on youth well-being. Below we enumerate specific lessons that can be learned from those efforts with an eye toward crafting improved legislation.

Vague statutory language can lead to legal challenges, implementation difficulty, and opposition from those who fear misuse of well-intentioned efforts

Laws need to be clear that they cannot be legislating expressive content due to constitutionality and section 230 concerns. California's Age Appropriate Design Code ("AADC") was enjoined due, in part, to the fact that parts of the law could be read to apply to expressive content.[233] Vagueness in the California AADC's "duty of care" language, which is also part of KOSA, has made it less clear whether the principle would apply to experiences with content or solely to the design of platforms. This has enabled opponents of the law to more successfully challenge its constitutionality.[234]

The "duty of care" was intentionally designed to be flexible enough to encompass new technological developments. However, this has also created space for politicians to potentially leverage the principle for unintended ends—such as suggesting that LGBTQ+ content is "harmful" sexual content that a duty of care would mandate limiting exposure to.[235] This threat has led to a loss of support among some who have historically worked toward advocating for a healthier online environment.[236]

Charges of "vagueness" regularly come up in response to any proposed law, including in Minnesota. In response to a Minnesota bill introduced to prohibit algorithms targeting teens, Jeff Tollefson, the president of the Minnesota Technology Association warned about the law being overly vague.[237] He suggested it could be applied to retailers, not just social media companies, stating "we do not believe that this overly broad and vague bill, coupled with the private right of action, is the answer. We support the bill's intent to keep children safe online, but House File 1503 in its current form creates more questions than answers." A recent Ohio law was also restrained by a judge who referred to aspects of it as "troublingly vague."[238] Indeed, in responses to this report, industry lobbyists have already submitted concerns to the Minnesota Attorney General's Office about laws that they perceive to be overly vague.

Being too prescriptive about solutions can have negative consequences

Some laws use broader language in order to be able to adapt to future technologies,[239] as overly prescriptive laws may become obsolete quickly as technology advances. Overly prescriptive laws can also have negative consequences. For example, with algorithmic incentives for engagement having been identified as a problem, both advocates[240] and legislators have proposed the idea of imposing a chronological feed.[241] However, experimental data[242] suggests that chronological feeds may not be beneficial, as it incentivizes hyper-posting, which is often done by problematic actors.[243] New laws have specifically referenced the removal of algorithms,[244] which may have similar effects. Algorithms may be beneficial or even essential in some settings, even as they create harm in others, such that the consequences of removal may be unpredictable. Future laws should take care to be evidence-based and avoid prescribing overly narrow solutions that may have negative externalities and that may not work well in various online settings.

Broad reporting requirements have often not had a material impact

Many legislative efforts, domestically and internationally, require platforms to write reports designed to bring transparency to the risk inherent in their product design decisions. Since transparency requirements are often not specific, platforms have generally been able to meet these requests readily without meaningfully changing their product design practices. Asking if a product is harmful can always be met with a "no" if a platform does not look for harm in sensitive ways or if a platform defines harm in a narrow way that conforms to their unduly narrow policy-based definition of harm. Platforms also have not been neutral arbiters as to the risks and harms inherent in their product design choices.[245] For example, Europe's Digital Services Act mandates risk assessments without clear guidance as to how they should be conducted. Early results suggest that these risk assessment reports are not meaningfully pushing companies to identify and mitigate risk, but rather to describe existing efforts in ways that benefit the company narrative.[246] Since regulatory bodies are often under-staffed with regards to the research needed to turn general principles into specific rules, it may take time before future iterations of these reports make a material impact on improving technology's impact on society. Expecting companies to identify risks themselves may predictably continue to lead to disappointing results without more specific guidance from society. Work is ongoing to help provide this needed specific guidance.[247]

Identifying minors needs to be done in a way that respects privacy and free expression concerns

Legislators have been focused on a bipartisan desire to protect children, and research has shown that existing laws may be difficult to enforce due to ineffective age verification. In one study, 68% of 11 and 12 year olds, for whom existing laws would generally exclude from technology platforms,[248] reported using social media apps.[249] However, the specific methods to identify who is or is not in need of protection have led to concerns and opposition. Legislative language like "estimate the age of child users with a reasonable level of certainty" in combination with vague definitions of harm, have led some to suggest that sites will begin to check identification for news stories that contain any PG-13 level material (*e.g.* mentions of sexuality or violence), even from sites like NPR or local news.[250] Advocates for freedom of information dislike this because children can be restricted from relatively benign content that may relate to important societal or personal issues. They also suggest that asking for identification will have a chilling effect on adults accessing information, as adults may not want to provide their identity in connection with controversial material (*e.g.* pornography or information about a mental health condition they don't want to reveal that they have). The prospect of collecting more data from users, regardless of age, and storing it has also led to opposition from many groups concerned about privacy,[251] especially given that the average teenager uses approximately 40 different applications which may each need age information.[252] Device-based age settings have been proposed as a potential solution to these issues.[253]

Potential constitutional challenges require the inclusion of alternative mechanisms to enforcement

Recently, the California Age Appropriate Design Code ("AADC") was enjoined.[254] Courts have disagreed about which aspects of the law are or are not constitutional, demonstrating that the law is still unsettled and it is currently unclear how broadly the Supreme Court will interpret the First Amendment rights of technology companies. Some legal scholars have argued that product design is specifically covered by the First Amendment as a form of expression,[255] even as others disagree with that interpretation.[256] Several Supreme Court justices have suggested that "functional" design could be regulated, but it is unclear exactly what design provisions would be considered expressive or functional. Court decisions regarding the AADC[257] suggest that a less expansive reporting provision would not have been ruled unconstitutional, but it has yet to be determined what such a reporting provision would look like.

Other legal decisions[258] do suggest that some aspects of design governance are enforceable, while others are not.[259] For example, in one recent decision,[260] design mandates that require defendants to publish or recommend less third-party content were deemed violative of Section 230, as such recommendations are "indistinguishable from publishing." In contrast, numerous other design mandates were deemed subject to legislation without the same Section 230 and First Amendment concerns.[261]

Still, the law is unsettled and a robust legislative strategy would include non-coercive ways to improve technology's impact on society.[262] Mandates are not the only way that regulators can encourage safer product design. Governments can create best practices that they publicize and encourage private actors to adopt, similar to nutrition standards, which may inform consumer and advertiser choice.[263] Government run organizations can adopt these practices within settings they control, such as within the school environment, where the impact of technology has led to widespread concern by educators.[264] Governments can make consumers aware of the choices they can make in relation to best practices. Governments can fund and incentivize research to improve and add to current best practices. Finally, governments can measure outcomes in society, to help provide clear metrics reflecting the impacts from emerging technologies, which private actors such as advertisers, investors and consumers can use to hold technology companies accountable.

Opt-out policies generally have not been effective

Several privacy laws have been passed that allow for users to opt-out of data collection practices of companies. Very few people use many of these opt-out provisions,[265] which mirrors the experience of platforms who have found similarly low levels of usage of opt-out functionality. For example, when hiding like counts (Project Daisy) was implemented as an opt-out, only 0.72 percent of users chose to hide like counts.[266] It is established knowledge at companies that very few people use any user control,[267] such that the default settings are very important for driving behavior, whether the goal is profit or preventing harm. Notably, a lack of usage does not mean that users do not want these protections, and simpler, more accessible privacy options, such as Facebook's Locked Profile feature, have proven popular where offered.[268]

Age limits for social media platforms have both pros and cons

Several jurisdictions[269] have responded to the challenges imposed by social media companies by imposing or proposing age limits. A social media age limit would almost certainly reduce usage and therefore harm from emerging technologies to youth. Per a University of Chicago study,[270] many people use these products solely because their friends do as well and they would actually prefer a world where nobody used such products, lending support to the idea of an age limit.

However, experiences with technology platforms and social media are not homogenous.[271] Any enforcement of a hard age-gated limit is going to require collecting data on age, which will lead to privacy concerns and may have a chilling effect for adults who do not want to identify themselves when accessing certain apps or information. Several age limit laws have been overturned by courts in the US, suggesting that legislation in this area may face legal challenges. It may be more effective to limit usage by enabling the enforcement of existing laws, such as COPPA, via device-based age settings.

Policies relating to content have been ineffective and led to both opposition related to potential misuse and legal challenges

Companies have spent billions of dollars on systems to moderate content that their policies deem inappropriate, hiring many thousands of moderators, yet users continue to report negative experiences with platforms that negatively impact their well-being, whether measured externally[272] or internally.[273] Even in cases where platforms have concentrated their moderation efforts, such as in wars or elections,[274] issues have remained rampant.[275] Meta whistleblower Arturo Bejar's recent testimony to Congress illustrated the limits of policies to address content, as certain negative experiences are unlikely to ever be addressable by policies.[276] Platforms may never be able to detect, for example, the subtle ways that partisans create hate and animosity. Efforts to make platforms less hateful by increasing enforcement of policies have led to backlashes from both the right[277] and the left.[278]

Efforts to moderate content externally have led to similar issues. Opponents of the California Age Appropriate Design Code have successfully argued that it should be enjoined partially because it could be seen as regulating speech.[279] Consequently, it must be made clear that any proposed law is content neutral, as this is important for surviving potential constitutional challenges. Recent laws concerning ideological bias in content moderation[280] have been enjoined by the Supreme Court on similar First Amendment grounds and have earned widespread opposition. Even in other countries without First Amendment protections, content-based governance proposals have led to opposition. For example, UNESCO guidelines regarding content moderation have been regarded by some as "endorsing a state-led online content moderation framework that could have a substantial and adverse impact on global democracy and civil liberties."[281] Similarly, a Sri Lankan law designed to protect against gender-based violence, has been opposed by civil society organizations that agree with the goal of the bill, but worry deeply about potential misuse by the government in deciding what kinds of content are or are not allowed.[282]

A design focus has been impactful both within companies and in legislation, but needs to focus on function, rather than expression

In contrast to content-based policies, focusing on design has been more impactful, both within companies and in legislation. The "Break the Glass" measures that companies have often launched in response to outbreaks of violence, health crises, or elections have often taken the form of changes to fundamental platform functionality, including things like limiting group invitations[283] or changing algorithmic incentives away from certain kinds of engagement such as reshares.[284] Notably, the UK's version of the Age Appropriate Design Code, which shares a framework with the California Age Appropriate Design Code, had its most successful impact in the realm of design.[285] YouTube turned off default Autoplay for users under the age of 18.[286] Tiktok[287] and Instagram[288] removed the ability of strangers to contact teens by default. Legislative pressure in the US has been credited with inspiring further design changes from Instagram that have improved teen safety.[289] Critics of the Kids Online Safety Act have been more amenable to design changes,[290] suggesting that a legislative focus on design could lead to reduced opposition. Such legislation needs to take into account guidance from court decisions as to what kinds of design decisions would be considered expressive.

Section Four: The current and expanding impact of AI

Over the past year, we have seen an increase in adoption of AI products. A Common Sense Media study fielded in the fall of 2023 found that roughly half of young people ages 14-22 reported using generative AI at some point in their lives, with 15% reporting using it on a weekly basis.[291] A 2023 University of Southern California study found a similarly low level of use of AI products, with only 16% of US adults having used these products.[292] A subsequent 2024 Common Sense study of youth ages 13-18 found that 70% of teens reported using generative AI.[293] The increasing ubiquity of search engines with AI-generated results may drive some of this increase, but for chatbots alone, 24% reported using them at least "several times per week". Accompanying wider adoption of AI has been an increase in specific AI driven harms, including those detailed below.

Generative AI has been commonly used to make non-consensual sexual imagery

The Minnesota Attorney General's Office, along with other state attorneys general, has been seriously concerned about the impact of AI on children,[294] specifically identifying the risks of revealing private information and enabling "deepfakes" of children's voices and images, including in sexualized contexts. Unfortunately, recent reports suggest that these concerns were well founded. Common Sense Media reports[295] that teens are using generative AI to bully each other, leveraging the ability to create harmful and fake images and audio. There have been numerous stories[296] of students making sexualized images of other students. In a Center for Democracy and Technology study,[297] 40% of students reported awareness of deepfakes being shared at school, with 15% depicting an individual in a sexually explicit or intimate manner. In over 60% of these cases, students report sexualized deepfakes being distributed via social media—whether by a post or direct messages.

Chatbots do not have appropriate safeguards for young people, who use them widely

Roughly half of teens report using AI powered chatbots, with 24% using them at least weekly and 11% using them daily.[298] Integration into widely used social media platforms[299] and the marketing of chatbots that mimic characters that are popular with teens[300] have helped drive this rapid adoption. Many teens report using generative AI to "keep me company".

This adoption has not been accompanied by corresponding safeguards. Executives from AI companies have warned that these products can become "extremely addictive"[301] and researchers have documented that over-usage and addiction are primary risks of personalized chatbots.[302] Several studies have shown that aggregate positive benefits of chatbots are possible,[303] but investigations by journalists and clinicians suggest that these products are not robust in terms of the quality and safety of their responses.[304] Serious consequences from chatbots have already occurred. A Florida teen committed suicide after engaging in a deep sexualized relationship with a Character.ai chatbot that mimicked a popular Game of Thrones character.[305] A Belgian man ended his life after interacting with an AI Chatbot that reportedly encouraged his suicide.[306]

Generative AI

70%
of 13-18 year olds reported using generative AI[293]

15%
of 14-22 year olds reported using generative AI on a weekly basis[291]

Chatbots

24%
of teens reported using AI powered chatbots **weekly**[298]

11%
of teens reported using AI powered chatbots **daily**[298]

Despite in-product reminders that chatbots are not real, the design features of these products are intended to convey a misleading sense of "humanness"[307] such that even trained engineers confuse them with actual humans,[308] especially when these products are trained to state unequivocally that they are indeed people.[309] Given the epidemic of loneliness in society,[310] care needs to be taken in introducing vulnerable youth and adults to products that may appear to fulfill an immediate social need, but where acute harms have already begun to surface and where long-term negative impacts, such as social deskilling[311] and demotivation[312] resulting from substitution for in-person socialization, may arise.

Protecting society against current threats from Generative AI

Many harms from generative AI are propagated on social media systems which distribute deepfakes[313] or host chatbots.[314] As such, the proposed recommendations elaborated in this report to regulate social media are even more important to make systems robust against scaled AI-enabled harms. By explicitly limiting the kinds of information that AI models ingest, the ability of malicious actors to access the information of minors via both rate limits and default privacy settings, and the ability to distribute and monetize this content through proactive limits on the distribution of non-consensual content, we are hopeful that the proposed recommendations would limit the systemic risk posed by AI generated content distributed on current technology platforms. By increasing the practical ability of parents and families to limit time spent on social media and on phones generally, youth will encounter fewer experimental AI systems that have unknown risk. Still, we do believe that some specific legislation concerning generative AI should be passed to reduce risk outside of the social media context. Such proactive risk limitation would complement laws that make such deepfake content illegal, including a recent law passed in Minnesota.[315]

The harms that concern society about AI often mirror the concerns we have had for other technologies, including social media. We worry that malicious actors will misuse the power of these technologies to harm others and setting reasonable limits should mitigate some of these risks. We worry that we will not understand the decisions that companies make and that algorithms will make indecipherable and unfairly discriminatory choices. Hopefully by mandating transparency of how AI training decisions experimentally affect outputs, we will gain the understanding necessary to mitigate such risk. By tracking user experiences with these novel technologies, we will have the tools to develop new legislation as new experiences—positive and negative—facilitated by these technologies arise. And in the interim, we should pass targeted legislation that allows for innovation, but reduces the risk of acute AI-enabled harm, especially with respect to our children.

Section Five: Policy recommendations

The above sections suggest that design focused legislation that provides the right level of specificity could lead to legislation that is effective, constitutional, and that engenders reduced opposition. It suggests that future legislation should mandate defaults, rather than requiring "opt-in" choices. Rather than restricting youth from online platforms, ideal legislation would empower families to protect their children from manipulative design in ways that respect privacy and do not chill expression.

Our hope is that the below recommendations provide design mandates that fit these criteria with enough generality to apply to new, emerging technologies, where we anticipate similar risks relating to privacy, engagement optimization, and manipulation by small groups of motivated users to arise, but also with enough specificity to reduce the risk of misuse and legal challenges. Since even functional design focused mandates could lead to legal challenges, we further recommend a modular, fully severable law that also includes non-coercive avenues toward improving technology impact.

Given our increasing knowledge of the harms experienced by users, the design choices that facilitate those harms, and the legislative precedent that attempts to address those harms, we feel confident in making the below recommendations.

These recommendations leverage the University of Southern California Neely Center's Design Code for Social Media, which is based upon internal platform best practices as well as external research, and has the explicit support of numerous academics, technology critics and former platform employees.[316] While we cannot say these steps will solve all issues, since none of them have been done to their fullest extent, we can be confident that each step will make a material difference in identified harms, especially with respect to youth. Some of these changes have already been adopted to some degree by some platforms[317] showing that such changes are technically and commercially feasible by responsible technology platforms.

Proposed legislation would be specific to the state of Minnesota such that IP addresses that are known to generally resolve to Minnesota residents or people who reside in Minnesota would receive such protections. Such systems are accurate enough such that large companies already use these systems to enforce location-based restrictions.[318] However, it is possible to get around these systems through VPN technologies. We recommend specifically excluding anyone who does not want to get the default Minnesota protections or who decides to use a VPN, as our goal is to protect those who want protection, which surveys indicate includes the majority of Americans and parents, but not to require these protections for those who do not want them. This would also help insulate proposed legislation from charges of impracticality, given that IP-based location predictions are already used to drive functionality changes in online products.

Our policy recommendations follow.

I. Ban "deceptive patterns" within platform design
   a. Ban design features that encourage greater usage for children beyond their explicit desires. Offer all users accessible tools to limit their platform usage
   b. Mandate aggressive privacy defaults to limit the unwanted sharing of data and images
   c. Mandate responsible amplification through limits on engagement-based optimization
   d. Mandate transparent, sensible rate limits that would limit the ability for small groups of users to manipulate others
II. Mandate transparency of product experimentation that can illuminate new harmful deceptive patterns
III. Mandate user and parent empowerment via consumer-friendly device-based defaults
IV. Track technology platform specific impact on user experience, including amongst sub-groups
V. Mandate interoperability to encourage consumer choice
VI. Mandate technology usage limits and education within schools
VII. Protect youth from the current harms of AI

I. Ban "deceptive patterns" within platform design

Existing legal precedent requires platforms to design reasonably safe products and inform users of risks. Platforms also have a duty to prevent third party harm via their products in cases where an entity itself creates the risk of harm and demonstrates malfeasance, defined as being responsible for making a user's position worse, which is distinct from a "failure to act." Deceptive patterns refer to the designs of user interfaces and algorithms in ways that benefit companies at the expense of users, often in ways that are imperceptible to those users and manipulative, given that consumers would make different choices with full information.[319] They often affirmatively increase or create risk, which can be measured by experimental data from platforms themselves.[320] While the Minnesota Attorney General's Office has the authority to address deceptive patterns already under existing authority to protect consumers from deceptive and unfair practices, whether the below design choices would qualify is likely to be subject to litigation. Providing clarity on what is or is not permissible within specific legislation would enable more certainty for technology businesses and regulators, as well as streamline the Office's enforcement efforts. Already, reports such as this one have been part of a societal movement to define minimum design standards for

companies.[321] Such certainty would also remove any incentive for companies to compete for market share using manipulative design choices, putting all companies on a level playing field.

Focusing on functional design and anchoring on users' definitions of harm removes the ability of politicians to define what is harmful for political reasons and mitigates constitutional conflicts. Previous research has shown that users have wider definitions of harm for most policies than companies have,[322] such that anchoring on user experience should lead to more robust changes.

The Federal Trade Commission has been able to create meaningful change for children's experiences of products by focusing on design.[323] It has broadly been able to address deceptive patterns relating to false beliefs, lack of disclosure of material information, unauthorized costs, and design elements that obscure privacy choices.[324] While a focus on design still could lead to First Amendment challenges, at least some scholars believe that design-based approaches are indeed constitutional[325] and several Supreme Court justices have specifically suggested that regulating functional design would be considered constitutional.[326] It will also provide a relatively broad level of user protection, given that similar design changes have proven among the most effective changes that platforms can make.[327] The specific design features to address are further enumerated below.

a. Ban design features that encourage greater usage for children beyond their explicit desires. Offer all users accessible tools to limit their platform usage.

There are many functional design choices and default functionality that relate to revenue and usage maximization (*e.g*. time spent optimization, infinite scroll, auto-play, aggressive notifications, automated resubscription, engagement counts) rather than to the explicit choices or preferences of users. Legislation should allow users to control their usage and limit platforms ability to design features that manipulate users. Examples of such features include optimizing for time spent watching or consuming content, scrolling interfaces that auto-load more content, notifications that are meant to drive users back to the product rather than inform them of important time sensitive information, displaying counts that gamify engagement and automatically playing content rather than waiting for users to indicate that they want to consume more.[328] Aside from the examples provided above, legislation can lean on the extensive literature on revealed versus stated preference[329] to adjudicate which new features really are honoring users' explicit, stated desires to use these products more. Governments have already restricted design patterns that make revenue from subscriptions automatic and frictionless,[330] accepting that users often want to be asked explicitly before choices are made that benefit companies at the expense of consumers. Legislation should make clear that these same protections, requiring affirmative choice, should apply to design decisions that lead to ad revenue at the expense of consumers' time and attention.

This is especially important for children who are still developing their inhibition systems[331] and so are more vulnerable to design features that target reward systems, so defaults should be especially conservative, turning off these usage maximization features by default, when users are identified as minors (via device-based settings as outlined later in our recommendations). Indeed, some teens report feeling that platforms are manipulative[332] and therefore create extra barriers for themselves[333] to manage their usage. Many of the important changes resulting from the UK's Age Appropriate Design Code relate to user empowerment with regards to managing usage. Given the volume of notifications that teens experience,[334] it is important to set standards so that app developers don't engage in a "race to the bottom" by saturating youth, in particular, with notifications that are not actually timely.

b. Mandate aggressive privacy defaults to limit the unwanted sharing of data and images

Businesses have an incentive to make information publicly accessible as content to other users, even when users may have chosen otherwise, in order to facilitate the content and connections that bring users back to platforms which rely on user generated content. Users and their content should be presumed to

be private, unless users explicitly desire their content to be public. In situations where the expectation is ambiguous, platforms should default visibility to private. Previous bills with "opt-out" privacy measures have had limited or unclear consumer adoption.[335] Few users are willing to change their defaults. Users care about privacy[336] but often do not understand enough about their choices to provide consent,[337] which is why it is important to anchor on what users would expect, rather than what users are willing to change via settings. Since most users have been onboarded without meaningfully adjusting their privacy settings, these defaults should be set retroactively for all users who have not explicitly changed their privacy settings, not just for new users. As examples, features that share location should always be off by default. Content that is posted should be presumed to be shared only with contacts and friends, unless users have explicitly chosen otherwise. One-on-one activities (*e.g.* messaging a friend) should be only accessible to those participating in the activity. Users should not be publicly discoverable unless they specifically choose to be.

The increasing ubiquity of AI requires specific consideration about how to address private images that are sexual in nature. In particular, we are already seeing non-consensual sexual imagery as a pervasive online issue that affects the online participation of women[338] and that exploits children.[339] Platform-specific legislation can further protect against the misuse of images of minors or non-consenting adults, by creating liability for the distribution of images of private individuals without affirmative consent. AI makes it easy to manufacture such imagery and as such, strong legislation that prohibits the public distribution of content depicting individuals who do not explicitly provide permission is needed given that anyone can now generate misleading or sexual imagery of anyone else. This will provide an order of magnitude more protection as compared to the current system that requires the discovery and reporting of such content, given the difficulty of that process and the harm that will have already occurred when such content is distributed.

In addition, AI systems are likely to exacerbate privacy risk by making previously undiscoverable data about individuals more readily accessible. Given that risk, legislation should reduce the risk of AI models that "leak" consumer data[340] by specifying specific kinds of data (facial data, biometric data, social media data) that AI systems should not have access to, given the risk of leakage.

c. Mandate responsible amplification through limits on engagement-based optimization

Many harms to consumers occur when engagement-based algorithms provide content that is engaging, but that users do not explicitly want. Given the harms that are known in optimizing content for engagement, we recommend limiting optimizing important/sensitive content for engagement that is not explicitly related to users' stated preference, by restricting the use of personal data, following the precedent set by other states.[341] For example, leaving a comment or spending time watching a video are not examples of explicit stated user preference, since it is not uncommon for users to watch or comment on things they dislike. Comments or time spent have no inherent preference valence. In contrast, a like, a love, or an explicitly positive comment all indicate an explicit preference for that content, such that those signals would be allowed in optimization algorithms for sensitive content. We would expect companies to develop user interfaces to elicit explicit preference in response to this requirement (*e.g.* an "informative" reaction). Outside of the signals discussed here, the extensive literature on revealed versus stated preference[342] can help adjudicate when algorithms are indeed optimizing for explicit stated preference.

To avoid constitutional issues with the government regulating "expressive" design, future legislation could follow the model of New York and California's enacted SAFE acts, which restrict the functional use of personalization in algorithms with a few exceptions. Exceptions could be made for explicit user preference[343] or to reduce negative experiences for users - with allowances for users to consider when they want to allow their personal data to be used, rather than encouraging chronological feeds. This would follow industry data suggesting that the replacement of engagement signals with preference data improves

user experiences.[344] These changes have also been found to reduce bullying and harassment, given that highly engaging discussions often lead to such exchanges, and also reduce the risk of harmful, yet engaging content being recommended to users, often against their wishes. It will also improve the incentives in the ecosystem given that influencers, publishers and politicians have reported that their incentives are toward lower quality content due to engagement-based amplification.[345]

d. Mandate transparent, sensible rate limits that would limit the ability for small groups of users to manipulate others

Rate limits are used to control the number of actions that a user may take in a specific period and are an important tool used across domains to prevent abuse.[346] Limits can be made "hard", preventing actions above some limit, or "soft", reducing the impact of actions taken beyond a particular limit. Platforms often set these limits to relatively high numbers in order to inflate business metrics, allowing small groups of users that are more likely to be abusive to take a disproportionate share of actions.[347] Contrary to marketing that suggests that social media democratizes voice,[348] a lack of reasonable rate limits often allows a small group of motivated partisans to dominate a conversation.[349] To ensure that platforms live up to their marketing and reduce the harms caused by these groups, we recommend mandating transparent, sensible rate limits for new, untrusted users who access functionality that can be used to target or influence others. To remove ambiguity, legislation should specifically include (but not limit itself to) functionality that allows people to view the accounts of strangers, contact strangers, comment publicly, post publicly, share publicly, or invite others to participate in groups or discussions. This would make sure that small groups of actors cannot manipulate engagement signals nor use platforms to research or contact large numbers of strangers in order to affect vulnerable individuals, who often are youth. Rate limits should be set in relation to what median users need (*e.g.* what limit includes 90 percent of user behavior), rather than based on business goals, and should only be lifted for trusted users with demonstrated need. Platforms should be required to disclose their rate limits and how those limits are sensible in relation to metrics of existing user behavior, as well as under what circumstances they lift those limits for demonstrated need. They should also be required to show how views of content created are distributed across percentiles of users, to illustrate whether their systems are or are not democratic in terms of the voice provided to users. It is uncertain whether rate limits would be considered "functional" or "expressive" by future courts. However, even if deemed expressive, such regulation should be considered a reasonable time, place and manner restriction,[350] akin to laws that regulate spam,[351] which is a type of rate limit that has ample precedent.

II. Mandate transparency of product experimentation that can illuminate new harmful deceptive patterns

Product experimentation results can allow society to get at causality, since experimentation is the scientific community's basis of adjudicating what a given product decision is causing to occur. Platforms have a legitimate need to protect trade secrets, but legislation that specifies the indications of harm that are of interest (*e.g.* user-defined experiences of harm, specific kinds of algorithmic bias, content that promotes widely accepted harms like eating disorders) as well as the types of product decisions to be examined (*e.g.* recommendation optimization function changes, AI training data inclusion, visible UI changes) should bring enough specificity such that companies can meet these requirements without revealing trade secrets. Such specificity can also ensure that they will be unable to meet these requirements without meaningfully informing the public.[352] Platforms already run numerous internal product experiments and have data and systems to understand experimental results, such that these requirements should not be particularly onerous. To ensure that platforms do not stop collecting data on important experiences, legislation should mandate the inclusion of specific metrics (*e.g.* reports of negative experiences, user behavior that indicates that they want to avoid certain content, or views of content later deemed to be policy violating) that would be required to be included. Notably, Minnesota passed legislation to mandate product

experimentation transparency which goes into effect in July 2025.[353] Given expected industry pushback, we would hope that other jurisdictions[354] also pass similar legislation in order to make access to such data more robust.

Product experimentation is used widely in AI system development. Consequently, allowing society to understand how different decisions about what data is or is not used in training AI models may or may not lead to algorithmic bias will help society play a meaningful role in AI model development. Product experimentation is so ingrained in technology development that it will also likely be used for any future emerging technology. As such, mandating access to product experimentation data has the potential to mitigate a great deal of future emergent risk with technology, beyond its effect on social media systems.

III. Mandate user and parent empowerment via consumer-friendly device-based defaults

Identifying youth who require more protections can be done in a privacy safe way, by designating specific devices as belonging to minors, building on device OS provider functionality that identifies minors whose permissions are adjustable via Google,[355] Microsoft,[356] and Apple[357] family accounts. Together, these providers account for the vast majority of devices, whether mobile or desktop. These providers can be mandated to provide a "toggle" that is accessible to applications that wish to know if the user of that device self-identifies as a minor. No identifying information about a user needs to be provided nor does the user experience for non-designated devices need to change. This solution would entail less privacy risk and be more robust as compared to the current practice where every individual app has a separate process for minor identification or opting in to privacy protections[358] and many kids lie about their age to access services while still under the age of 13.[359] Providing the ability for families to voluntarily identify devices as belonging to minors would likely lead companies that operate clearly inappropriate services (*e.g.* porn, alcohol, or gambling) to voluntarily restrict their products for children - without any government mandate.

Consumer-friendly defaults means setting the default settings for these devices according to parental preference, rather than business preference. Defaults should cover any design choice that has been identified in legislation as needing a more protective option for children. Design-based controls are likely to be less controversial than any content level filter. Alternatively, if this proves unfeasible, it would be reasonable to set more restrictive design defaults for all users, to enable maximal user empowerment. If legislation does solely focus on protecting identified youth, options should also be provided to allow adults to opt-in to more restrictive design defaults. Older youth, elderly or disabled citizens may wish to voluntarily receive more restrictive design defaults, and should be afforded that opportunity.

IV. Track technology platform specific impact on user experience, including amongst sub-groups

Mandates are not the only way that the government can facilitate a better technology ecosystem. User experience measurement for specific platforms can facilitate cross-platform accountability by advertisers and consumers in a way that is not reliant on top-down definitions of good or bad content. Unlike measures of content prevalence or on platform behavior, such measurement can be done independently across platforms.

Several regulators have taken this approach. OfCom, the UK regulator, has been running their Online Experiences Tracker for several years[360] where they have noted that "unwelcome friend or follow request, or messages" and "content showing dangerous stunts or challenges" are amongst the top 5 reported potential harms amongst minors.[361] USC's Neely Center has been replicating internal platform research[362] on user experience, by surveying a representative sample of users as to their positive and negative experiences across platforms.[363] The results have been used by the press[364] to hold technology companies accountable for negative experiences and are being consumed internally by companies seeking to improve the user experience of their products.

Work on improving the user experience has been influential within tech companies for tracking a much broader set of harms for youth.[365] Recent Senate testimony[366] has highlighted how the harmful experiences of users often do not conform to the metrics that companies report, which generally focus on policy violating content. As such, we recommend that local governments also begin tracking the experiences of users, especially youth, as to what positive and negative experiences they report in using specific emergent technology platforms. Such tracking could be funded through taxes on platforms and legislation in this area should consider previous precedent in determining revenue generating options that do not trigger first amendment and commerce clause concerns.[367]

Given the differential effects that emerging technology has on diverse groups, including racial minorities, the LGBTQ+ community, as well as specific differing effects on young men vs. young women, it is important to track user experiences amongst these specific sub-populations. Privacy concerns and related regulation mean that companies will often be reluctant to conduct research on subgroup effects. Mandating such studies could lead to increased data collection and still may not lead to the tracking of the specific groups that society has an interest in. External user experience measurement can fill this essential gap, where the government can track differential effects on populations of interest - much as it does in other domains.[368]

Such tracking can be especially helpful for mitigating harm due to the increasingly ubiquitous use of AI outside of social media recommendation algorithms. As the public's familiarity and access to generative AI systems grows, we should understand both positive and negative experiences across platforms for these new technologies, to mitigate risks before they become widespread. User experience measurement has already enabled the tracking of novel AI enabled risk, showing the alarming rates of experiences with non-consensual, deepfake sexually explicit imagery.[369] Consistent user experience measurement would enable the detection of similarly problematic emerging risk.

V. Mandate interoperability to encourage consumer choice

Many consumers would prefer to leave platforms that engage in deceptive product design decisions, but are locked in by network effects,[370] which refer to the need to use a service to access information from a user's contacts, even if a user may not want to use that service otherwise.[371] Interoperability would remove that barrier and allow platforms to compete on providing more value to consumers, rather than on locking in network effects. Laws could mandate open APIs, as exemplified by a recent New York law,[372] that would allow users to continue to access data from others in their network, even when they are not using a specific service. A federal law, the ACCESS act, has similarly been proposed to require large communications platforms to maintain and support the ability of users to transport their data and delegate their access to trusted third party software. Such interoperability would enable a more diverse ecosystem of online platforms. This approach has the support of numerous stakeholders, including industry players like Block Party, academic groups such as Ethan Zuckerman's lab at UMass-Amherst,[373] and civil society groups like New_Public, which curates a directory[374] of smaller technology platforms seeking to create prosocial spaces. Recently, the new platform BlueSky, has gained a great deal of popularity through innovating novel user friendly features, such as Starter Packs and Moderation Lists. These platforms will be more successful if the network effects of larger players, that lock people into their services in order to access friend content, are able to be mitigated. The success of these platforms can also drive the adoption of new user-friendly functionality, as has already happened with some of BlueSky's features.[375]

VI. Mandate technology usage limits and education within schools

One other potential avenue for legislation that does not necessarily involve mandates for technology platforms is to address impact via students' use of technology within the school system. As of November, eight states had passed laws to restrict the use of potentially harmful or distracting technology within school settings.[376] Ideas within these laws include:

- Education about the responsible use of social media and emerging technologies.
- Prohibiting the use of and access to services deemed unsafe.
- Limiting the use of wireless communication devices.
- Restricting the possession of wireless communication devices.
- Limiting the instructional usage of technology that may encourage students to use services they may not want to use.

Many states, including Minnesota,[377] have passed policies that require a policy to be created, but allow for local flexibility as to the specifics of that policy. Minnesota's bill also required the development of school specific recommendations which has since been released[378] and recommends a full ban on cellphone access during the entire academic day citing research suggesting that a ban would lead to increased academic performance, a better teaching environment, and improved mental health. School districts nationwide and within Minnesota have experimented with a wide variety of policies, and school districts have generally reported positive experiences with clear restrictions that mirror the toolkit's primary recommendation[379] as opposed to more permissive policies that put teachers in the unwanted role of attempting to enforce restrictions, rather than having them be enforced at the administrative level.

While restrictions for elementary and middle school students are relatively uncontroversial, there are those who want to provide for the autonomy of high school students and Minnesota's Cell Phone Kit recommendations do provide an alternative policy that allows high school students specifically to use their phones during passing time and lunch. Most all policies allow for understandable exceptions to cellphone usage limits for cases of educational accommodations, health needs, and emergencies. Given the almost universal desire from teachers for support regarding classroom device usage,[380] we would recommend clear separation from devices throughout the school day enforced by schools, not teachers, who do not want to be put in the position of enforcing policies on a class-by-class basis. Exceptions that accommodate the most common objections to such policies are well known and can be based on existing precedent.[381] Beyond restrictions on usage, we would also recommend that schools be restricted from using social media platforms as the primary means for communicating with students, given many students desires not to use these products[382] and that they be encouraged to provide classes on digital literacy, building on existing established curricula.[383]

VII. Protect youth from the current harms of AI

Now that we have greater understanding of AI's current impact on youth, we are better positioned to create targeted legislation to mitigate harmful effects. Since AI generated harmful content is often generated or consumed within the context of social media platforms,[384] regulation of social media will mitigate some part of potential harm. However, not all harms are mediated via social media and given the serious nature of potential harm,[385] we would suggest targeted legislation that mitigates the worst such harms. At a minimum, we would recommend these steps:

- Age limits for the use of chatbots that can potentially engage in sensitive or personal conversations. Device-based age settings can facilitate this in a privacy safe manner.
- Design limitations on chatbots to ensure that vulnerable citizens do not perceive them to be actually human. These need to go further than disclosures that may be ignored by vulnerable users who focus instead on the lifelike qualities of these systems.
- Mandate that all parties take appropriate responsibility in reducing the creation and spread of non-consensual imagery. Tennessee's ELVIS act,[386] which imposes liability for non-consensual use of a person's likeness may provide a model for expanding Minnesota's current protections.

Together, these proposed changes can help us address the current, urgent risks of Generative AI, even as measures like tracking user experiences and understanding product experimentation results can help us anticipate future risk.

Conclusion and next steps, including model bills

There is considerable consensus that youth, including youth in Minnesota, experience reduced well-being as compared to earlier generations.[387] We can also clearly see that the specific product design choices of companies are contributing to reduced youth mental health for an unfortunately large number of our youth.

As such, our focus in our legislative policy recommendations is not on fixing the entire youth mental health crisis, but instead fixing technology's impact upon key aspects of it. There is clear consensus that bullying, lack of sleep due to overuse, negative social comparison, unwanted contact, privacy violations, and the substitution of in-person interactions with online social interactions have indeed led to reduced well-being for many technology users, with new risks emerging as AI gains wider adoption. There are aspects of functional technology design that contribute to these experiences. The aim of our recommendations is not to eliminate these experiences—a result which may be beyond the reach of any legislation—but rather to eliminate known functional design practices that encourage and promote negative experiences that the majority of users would otherwise choose to avoid.

In early 2024, legislation was introduced that mirrored our previous report,[388] and the Legislature ultimately passed cutting-edge transparency provisions.[389] Having seen the same harms in their communities, numerous other jurisdictions introduced legislation targeted at technology facilitated harms, with some passing, and courts beginning to clarify how to balance free expression and society's interest in protecting youth. Based on these collective experiences, we are pleased to offer model legislation (contained in the appendices to this report) to accompany our recommendations that we hope will be useful not only in Minnesota but also across jurisdictions - both nationally and internationally.

Accompanying this report are six model bills that turn the recommendations from this report into specific legislative text that is responsive to the legal and political concerns that have previously emerged in response to tech legislation. The first model bill[390] includes prohibitions on the functional aspects of platform design that often deceive users into harmful and unwanted experiences. These prohibitions are aimed at "protected users", which includes minors identified at the device level or known to platforms. These prohibitions could also be included in other legislation, and several similar prohibitions have been introduced within the Age Appropriate Design Code and Kids Online Safety Act. It is hoped that this language can provide a broader set of potential prohibitions.

A second standalone bill[391] is offered to independently identify minors at the device level, requiring such functionality be provided by operating system providers. The bill contains provisions similar to industry sponsored bills[392] but does not eliminate industry responsibility in cases where they have knowledge of user age through other means. It also contains fewer requirements for device operating system providers and allows for device owners to opt into protections, in cases where someone who may be otherwise impaired or wanting of protections would like to be treated as a "protected user"

even if older (*e.g.* adults with special needs or the elderly). This bill is complementary to other bills that place requirements on platforms to protect those identified as minors, as it provides a robust privacy safe way for parents to opt-in to such protections.

A third bill[393] focuses on protecting the misuse of individuals' images via generative AI. It is based on Tennessee's ELVIS Act which protects individuals against the commercial exploitation of an individuals' images and voice, including after death. This modified bill addresses existing concerns with Tennessee's bill, by including exceptions for cover artists and satire, but also strengthens protections beyond commercial exploitation, for private individuals and for the sexual exploitation of public figures. This addresses one of the most common AI driven harms, and it is our hope that one of the main others—chatbots—is addressed through age aware devices that AI companies leverage to exclude younger users from such products, until they are adults.

Until the Supreme Court sets a firm line on what design can and cannot be regulated, we cannot be certain that any bill will withstand court challenges. Accordingly, three more bills are provided that attempt to address the impact of platforms outside of the design affordances these platforms provide. A fourth bill[394] focuses on interoperability, by adapting the federal ACCESS act[395] to a state context by limiting the requirements of regulators and instead relying on complaints from competing companies to identify issues to be enforced upon. A fifth model bill[396] builds on previous bills that tax digital advertising[397] and uses those funds to monitor platform specific user experiences.[398] Finally, a sixth bill[399] offers youth a break from online life by mandating full day phone free schools, which mirrors the first recommendation from the Cell Phone Toolkit developed under current Minnesota statute. This bill was developed by the Becca Schmill Foundation. It is under current consideration in Massachusetts and many of these bills will be shared with jurisdictions beyond Minnesota, given the widespread desire to address these commonly observed harms.

To be clear, if this legislation is adopted, there will still be bullying online, but the same forces of accountability that operate offline will mitigate online bullying and engagement-based applications will not amplify the messages of bullies. There may still be those who exploit and sexualize the images of youth, and law enforcement and platforms should continue to address that issue via enforcement. However, algorithms will no longer recommend or amplify such content such that the monetization incentive will no longer be there to encourage such practices. Further, it will be harder for predators to research and contact potential victims of bullying or exploitation, as most youth will not change their default privacy settings and rate limits will make it hard for predators to engage in mass solicitation campaigns. Our proposed recommendations cannot eliminate all online harms, as individuals who seek to engage in risky behaviors will still be able to do so in any free society. However, we do hope to significantly change technology platform dynamics such that risky behaviors are subject to the same mitigating forces as in the offline world. At the very least, it should not be more common to experience harm using online platforms as compared to offline life, and society will be able to confirm this empirically through regular public health measurement. Unfortunately, that is not yet the world we live in today.

This report owes a great deal to the hundreds of researchers, technologists and lawmakers who have worked to improve technology's impact on society and especially our youth. It is a goal that is shared among the vast majority of society, including those working at technology companies. It is our hope that this report can represent yet another step forward in this work, by synthesizing previous efforts and proposing a path forward for Minnesotans and potentially for other jurisdictions who may be experiencing similar issues. We look forward to continuing to work with all interested parties on legislation that builds upon the recommendations laid out herein.

Endnotes

1 Cory Combs, *Amid rising concern about harms of social media, experts, stakeholders gather to strengthen online protections for kids*, Issue One (Oct. 23, 2023), https://issueone.org/press/experts-stakeholders-gather-to-strengthen-online-protections-for-kids/.

2 *Id.*

3 Rick Claypool, *Chatbots Are Not People: Designed-In Dangers of Human-Like A.I. Systems*, Public Citizen (Sept. 26, 2023), https://www.citizen.org/article/chatbots-are-not-people-dangerous-human-like-anthropomorphic-ai-report/.

4 Elizabeth Laird, Maddy Dwyer, Kristin Woelfel, *In Deep Trouble: Surfacing Tech-Powered Sexual Harassment in K-12 Schools*, Center for Democracy & Technology (Sept. 26, 2024) https://cdt.org/insights/report-in-deep-trouble-surfacing-tech-powered-sexual-harassment-in-k-12-schools/.

5 Tech Justice Law Project, Knight-Georgetown Institute, and USC Neely Center, *Platform Design Taxonomy*, Google Docs, https://docs.google.com/spreadsheets/d/1GVO7sNuCNmNwqVK64PHQI7wxd8-Gmr9PqdkW12elmus/edit?gid=941162555#gid=941162555.

6 Special thanks to the Tech Law Justice Project and the Knight-Georgetown Institute for their help in synthesizing legislation and litigation.

7 Laws like Illinois' Biometric Information Privacy Act have proven successful in setting a technology standard that many other states have since followed. Elements of our 2024 MN legislative efforts are now being introduced in other states (see https://malegislature.gov/Bills/194/HD3070).

8 Johnathan Haidt *et al.*, *Social media and mental health: A collaborate review*, New York University (unpublished manuscript), https://docs.google.com/document/d/1w-HOfseF2wF9YIpXwUUtP65-olnkPyWcgF5BiAtBEy0/edit#heading=h.ld9vqxg7lr05.

9 Candice L. Odgers,*The great rewiring: is social media really behind an epidemic of teenage mental illness?*, Nature (March 29, 2024), https://www.nature.com/articles/d41586-024-00902-2.

10 *Health and Health-Related Behaviors: University of Minnesota-Twin Cities Students*, University of Minnesota Boynton Health (2024), https://boynton.umn.edu/sites/boynton.umn.edu/files/2024-10/UMN_TwinCities_CSHSReport_2024.pdf.

11 *Wave 2 Research findings:Digital Well-Being Index*, Snapchat Inc. (June 2023), https://assets.ctfassets.net/kw9k15zxztrs/5YeLYk9Rzh2RTOGuGa37aq/09fcac523225cdfd955ab0e06f386ba7/Snap-__2023_Digital_Well-Being_Index_Wave_2_Report.pdf?lang=en-US.

12 Elizabeth Laird, Maddy Dwyer and Kristin Woelfel, I*n Deep Trouble: Surfacing Tech-Powered Sexual Harassment in K-12 Schools*, Center for Democracy & Technology (Sept. 26, 2024), https://cdt.org/insights/report-in-deep-trouble-surfacing-tech-powered-sexual-harassment-in-k-12-schools/.

13 Elena Bozzola *et al.*,*The Use of Social Media in Children and Adolescents: Scoping Review on the Potential Risks*, 19 Int. J. Environ. Res. Health (Aug. 2022), https://pmc.ncbi.nlm.nih.gov/articles/PMC9407706/.

14 Our original report referred to these as "dark patterns", consistent with the Federal Trade Commission's terminology, but these practices are increasingly being referred to as "deceptive patterns" - see https://www.reddit.com/r/UXDesign/comments/11xaopb/dark_patterns_are_now_known_as_deceptive_patterns/.

15 Federal Trade Commission, *Bringing Dark Patterns to Light* (Sept. 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

16 Victoria Rideout & Michael B. Robb, *Social Media, Social Life: Teens Reveal Their Experiences, Common Sense Media* (2018), https://www.commonsensemedia.org/sites/default/files/research/report/2018-social-media-social-life-executive-summary-web.pdf.

17 *Protecting Our Children Online: Hearing before the Senate Judiciary Committee*, 118th Cong. (2023) (written testimony of Mitch Prinstein, Ph.D., Chief Science Officer, American Psychology Association), https://www.judiciary.senate.gov/imo/media/doc/2023-02-14%20-%20Testimony%20-%20Prinstein.pdf.

18 Platforms have differing approaches to platform design (see https://medium.com/pinterest-engineering/the-field-guide-to-non-engagement-signals-a4dd9089a176), which lead to fewer negative experiences (see https://psychoftech.substack.com/p/unveiling-the-neely-ethics-and-technology) and less regret (see https://www.nytimes.com/2024/09/17/opinion/social-media-smartphones-harm-regret.html).

19 Federal Trade Commission, *supra* note 15.

20 *See* Ann Johns *et al.*, *Self-Harm, Suicidal Behaviors, and Cyberbullying in Children and Young People: Systematic Review*, 20 J. Med. Internet Res. (2018), https://www.jmir.org/2018/4/e129/, for quantitative evidence. *See, e.g., The truth behind 6 disturbing cyberbullying cases that turned into suicide stories…*, No Bullying (accessed Jan. 29, 2024), https://www.wtps.org/cms/lib8/NJ01912980/Centricity/Domain/745/The%20truth%20behind%206%20disturbing%20cyberbullying%20cases%20that%20turned%20into%20suicide.pdf.

21 *Cyberbullying Parents' Greatest Fear, Survey Says*, The Cybersmile Foundation, https://www.cybersmile.org/news/cyberbullying-parents-greatest-fear-survey-says#:~:text=TOP%20WORRIES&text=The%20majority%20of%20parents%20surveyed,you%20feel%20about%20these%20findings%3F (last visited Jan. 28, 2024).

22 Written Testimony of Arturo Bejar before the U.S. Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law (November 7, 2023), https://www.judiciary.senate.gov/imo/media/doc/2023-11-07_-_testimony_-_bejar.pdf.

23 Prinstein, *supra* note 17.

24 Elena Savoia *et al*., *Adolescents' Exposure to Online Risks: Gender Disparities and Vulnerabilities Related to Online Behaviors*, 18 Int. J. Environ. Res. Health (Jun. 2021), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8199225/#app1-ijerph-18-05786.

25 Emily Vogels, *Teens and Cyberbullying 2022*, Pew Research Center (Dec. 15, 2022), https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/.

26 *Arizona et al. v. Meta Platforms, Inc., et al.*, No. 4:23-cv-05448, Complaint (N.D. Cal. Oct. 24, 2023). Source materials online at https://storage.courtlistener.com/recap/gov.uscourts.nmd.496039/gov.uscourts.nmd.496039.36.2.pdf.

27 *One in six school-aged children experiences cyberbullying, finds new WHO/Europe study*, World Health Organization (March 27, 2024), https://www.who.int/europe/news/item/27-03-2024-one-in-six-school-aged-children-experiences-cyberbullying--finds-new-who-europe-study.

28 Robin Kowalski & Susan Limber, *Electronic Bullying Among Middle School Students*, Journal of Adolescent Health (Dec, 2007), https://www.jahonline.org/article/S1054-139X(07)00361-8/fulltext.

29 Paul Raffile *et al.*, *A Digital Pandemic: Uncovering The Role of 'Yahoo Boys' In the Surge of Social Media-Enabled Financial Sextortion Targeting Minors*, Network Contagion Research Institute (Jan. 2024), https://networkcontagion.us/wp-content/uploads/Yahoo-Boys_1.2.24.pdf.

30 *Recommendation: Brigading & Mass Harassment*, Facebook (Jun. 15, 2021), https://about.fb.com/wp-content/uploads/2021/10/Facebook_PolicyForum-Recommendation_-Brigading-Mass-Harassment.pdf.

31 Meta's recommendation systems largely use AI to optimize for engagement, such as resharing and commenting. *See* Nick Clegg, *How AI Influences What You See on Facebook and Instagram*, Meta (Jun. 29, 2023), https://about.fb.com/news/2023/06/how-ai-ranks-content-on-facebook-and-instagram/. Public reporting has shown how removing some of these engagement optimizations has led to reduced bullying. *See* Jeff Horwitz *et al.*, *Facebook Wanted Out of Politics. It Was Messier Than Anyone Expected*, The Wall Street Journal (Jan. 5, 2023), https://www.wsj.com/articles/facebook-politics-controls-zuckerberg-meta-11672929976.

32 Optimization refers to specifically what algorithms are programmed to maximize.

33 Matthew Hindman, Nathaniel Lubin, and Trevor Davis, *Facebook Has a Superuser-Supremacy Problem*, The Atlantic (Feb. 10, 2022), https://www.theatlantic.com/technology/archive/2022/02/facebook-hate-speech-misinformation-superusers/621617/.

34 *Diverse Motifs Can Improve Civic Conversations*, Bridging.Systems (Jan. 11, 2021), https://bridging.systems/files/Diverse-Positive-Motifs-Can-Improve-Civic-Conversations.pdf.

35 *Project Starship*, FBArchive (July 11, 2019), https://fbarchive.org/doc/odoc9919.

36 Paul Wright *et al*., *Preliminary Insights from a U.S. Probability Sample of Adolescents' Pornography Exposure, Media Psychology, and Sexual Aggression*, 26 J. Health Commun. (Jan. 2, 2021), https://pubmed.ncbi.nlm.nih.gov/33625313, discussing how 70 percent of youth reported viewing pornography); Dylan Williams *et al*., *"Keep it to a limit": The rules young people want protecting their data*, Reset Australia (Sept. 2021), https://au.reset.tech/uploads/resettechaustralia_policymemo_pollingreport_final-oct.pdf; *State of New Mexico v. Meta Platforms, Inc., et al*., Case No. 1:23-cv-01115-MIS-KK (D.N.M. Jan. 19, 2024), Ex. 1 to Am. Compl., https://storage.courtlistener.com/recap/gov.uscourts.nmd.496039/gov.uscourts.nmd.496039.36.2.pdf.

37 Clegg, *supra* note 31.

38 Williams, *supra* note 36.

39 Savoia, *supra* note 24.

40 Anonymous, *supra* note 35.

41 *User Report on Instagram Enforcement Actions*, FBArchive (April, 2021), https://fbarchive.org/doc/odoc5645691738.

42 Michael Robb & Supreet Mann, *Teens and pornography*, Common Sense Media (2022), https://www.commonsensemedia.org/sites/default/files/research/report/2022-teens-and-pornography-final-web.pdf.

43 Jessica Laird *et al*., *Demographic and Psychological Factors Associated With Child Sexual Exploitation*, 3(9) JAMA Network Open (2020), https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2770752.

44 Tawnell Hobbs *et al*., *'The Corpse Bride Diet': How TikTok Inundates Teens With Eating-Disorder Videos*, The Wall Street Journal (Dec. 17, 2021), https://www.wsj.com/articles/how-tiktok-inundates-teens-with-eating-disorder-videos-11639754848.

45 Jeff Horwitz and Katherine Blunt, *Instagram's Algorithm Delivers Toxic Video Mix to Adults Who Follow Children*, The Wall Street Journal (Nov. 27, 2023), https://www.wsj.com/tech/meta-instagram-video-algorithm-children-adult-sexual-content-72874155.

46 *Arizona et al. v. Meta Platforms, Inc., et al*., Case No. 4:23-cv-05448, Complaint (N.D. Cal. Oct. 24, 2023).

47 *Commonwealth of Massachusetts v. Meta Platforms, Inc., et al*., Civ. Action No. 2384cv02397-BLS1, Complaint (Mass. Superior Court, Nov. 6, 2023).

48 Becca Ricks and Jesse McCrosky, *Does This Button Work? Investigating YouTube's ineffective user controls*, Mozilla (Sept. 20, 2022), https://foundation.mozilla.org/en/research/library/user-controls/report/.; *Algorithms of trauma: new case study shows that Facebook doesn't give users real control over disturbing surveillance ads*, Panoptykon Foundation (Sept. 28, 2021), https://en.panoptykon.org/algorithms-trauma-new-case-study-shows-facebook-doesnt-give-users-real-control-over-disturbing.

49 Jesse McCrosky and Brandi Geurkink, *YouTube Regrets*, Mozilla (Jul. 2021), https://assets.mofoprod.net/network/documents/Mozilla_YouTube_Regrets_Report.pdf.

50 Matthew Hindman, Nathaniel Lubin, and Trevor Davis, *supra* note 33.

51 Horwitz, *supra* note 31.

52 Integrity Institute, *Child Safety Online* (Jan. 19, 2024), https://integrityinstitute.org/blog/child-safety-online.

53 *E.g., Handbook of Social Comparison* (Jerry Suls & Ladd Wheeler, eds., 2000). https://link.springer.com/book/10.1007/978-1-4615-4237-7.

54 Dominique Muller and Marie-Pierre Fayant, *On Being Exposed to Superior Others: Consequences of Self-Threatening Upward Social Comparisons*, 4 Social and Personality Psychology Compass (Aug. 2, 2020).

55 Baz Macdonald, *54% of young people want to be influencers - is it a bad thing?*, 1 News (Sept. 29, 2022), https://www.1news.co.nz/2022/09/29/54-of-young-people-want-to-be-influencers-is-it-a-bad-thing/#:~:text=Becoming%20an%20 influencer%20is%20a,as%20their%20top%20career%20choice.

56 Suzanne Bearne, *Reality check: life behind Insta-glam images of 'influencers'*, The Guardian (Mar. 17, 2019), https://www.theguardian.com/money/2019/mar/17/instagram-social-media-influencers-reality.

57 *2018 Allianz Generations Ahead Study - Quick Facts #3*, Allianz (last visited Jan. 28, 2024), https://www.allianzlife.com/-/media/files/allianz/pdfs/newsroom/2018-allianz-generations-ahead-fact-sheet-3.pdf.

58 Robert French, *Report of the Independent Legal Examination into Banning Children's Access to Social Media*, (Sept. 2024) https://www.dpc.sa.gov.au/__data/assets/pdf_file/0006/1069809/34011b0649ad6732bd0538d435305b24e45f6ace.pdf.

59 *Commonwealth of Massachusetts v. Meta Platforms, Inc., et al*., Civ. Action No. 2384cv02397-BLS1, Complaint (Mass. Superior Court, Nov. 6, 2023).

60 Andrea Hamel *et al., Body-Related Social Comparison and Disordered Eating among Adolescent Females with an Eating Disorder, Depressive Disorder, and Healthy Controls*, Nutrients (Sept. 2012), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3475236/.

61 Mary Madden *et al., A Double-Edged Sword: How Diverse Communities of Young People Think About the Multifaceted Relationship Between Social Media and Mental Health*, Common Sense Media (2024), https://www.commonsensemedia.org/sites/default/files/research/report/2024-double-edged-sword-hopelab-report_final-release-for-web-v2.pdf.

62 *Arizona et al. v. Meta Platforms, Inc., et al*., Case No. 4:23-cv-05448, Complaint (N.D. Cal. Oct. 24, 2023); *Social comparison: Topics, celebrities, Like counts, selfies*, The Wall Street Journal (Sept. 29, 2021), https://s.wsj.net/public/resources/documents/social-comparison-topics-celebrities-like-counts-selfies.pdf.

63 Victoria Rideout and Michael B. Robb, *Social media, social life: Teens reveal their experiences*, Common Sense Media (2018), https://www.commonsensemedia.org/sites/default/files/research/report/2018-social-media-social-life-executive-summary-web.pdf.

64 *Reducing social media use significantly improves body image in teens, young adults*, American Psychological Association (Feb, 2023), https://www.apa.org/news/press/releases/2023/02/social-media-body-image.

65 *Arizona et al. v. Meta Platforms, Inc., et al.*, Case No. 4:23-cv-05448, Complaint (N.D. Cal. Oct. 24, 2023).

66 Suyansh Srivastava, E*xploring Instagram's Algorithmic Bias Towards Attractive Women and Its Impact on Users – Cast Study*, Medium (Mar 22, 2023), https://medium.com/@heysuryansh/exploring-instagrams-algorithmic-bias-towards-attractive-women-and-its-impact-on-users-case-79a4c7e6583f; Rosanna Smith *et al., Instagram Face and the Algorithm: How Popularity-Integrated Recommender Systems Homogenize Beauty Standards and Lower User Well-Being*, Social Science Research Network (Sept. 24, 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4964322.

67 Danielle Paddock, *YouTube is limiting recommendations of weight and fitness videos to teenagers – but more wide-ranging change is needed*, The Conversation (Oct. 22, 2024), https://theconversation.com/youtube-is-limiting-recommendations-of-weight-and-fitness-videos-to-teenagers-but-more-wide-ranging-change-is-needed-238954.

68 Ken Dilanian, *Nigeria hands over two suspects in sextortion case linked to suicide of Michigan high school athlete*, NBC News (Aug. 14, 2023), https://www.nbcnews.com/politics/justice-department/us-extradites-nigerians-sextortion-linked-suicide-michigan-teen-rcna99795; Corky Siemaszko, *'Sextortionists' are increasingly targeting young men for money. The outcome can be deadly*, NBC News (May 8, 2022), https://www.nbcnews.com/tech/tech-news/sextortionists-are-increasingly-targeting-young-men-money-outcome-can-rcna27281.

69 *FBI San Francisco Warns of Increase in Sextortion Schemes Targeting Young Boys*, FBI (May 2, 2022), https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/press-releases/fbi-san-francisco-warns-of-increase-in-sextortion-schemes-targeting-young-boys.

70 Savoia, *supra* note 24.

71 *Online Nation: 2023 Report*, Ofcom (Nov. 28, 2023), https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/online-nation/2023/online-nation-2023-report.pdf?v=368355.

72 *Positive or negative?*, Common Sense Media (last visited Jan. 28, 2024), https://www.commonsensemedia.org/sites/default/files/research/report/2023-positive_negative_infographic_final.pdf.

73 *How do predators find children online?*, Beau Biden Foundation (last visited Jan. 28, 2024), https://www.beaubidenfoundation.org/onlinepredatorsblog1/.

74 Jeff Horwitz, *His Job Was to Make Instagram Safe for Teens. His 14-Year-Old Showed Him What the App Was Really Like*, The Wall Street Journal (Nov. 2, 2023), https://www.wsj.com/tech/instagram-facebook-teens-harassment-safety-5d991be1?mod=hp_featst_pos3.

75 See discussion of rate limits in Justin Hendrix, *Broken Code: A Conversation with Jeff Horwitz*, Tech Policy.Press (Nov. 13, 2023), https://www.techpolicy.press/broken-code-a-conversation-with-jeff-horwitz/.

76 Junhui Wu, Daniel Balliet, and Paul A. M. Van Lange, *Reputation, Gossip, and Human Cooperation*, 10(6) Social and Personality Psychology Compass (2016).

77 *Improving Civic Conversations with Conversational Motifs*, Gizmodo Facebook Papers Directory (June 15, 2023), https://s3.documentcloud.org/documents/23691770/tier3_code_hate_pr_undated.pdf.

78 Raffile, *supra* note 29.

79 Online discussions of rate limits show that each platform has varying limits on how often you can take certain actions, such as interacting with other users' content. *E.g. What is Instagram's hourly comment limit?*, Quora (2024), https://www.quora.com/What-is-Instagrams-hourly-comment-limit or *Understanding Automation Rate Limits Across Social Media Platforms*, PhantomBuster (December 17, 2024), https://support.phantombuster.com/hc/en-us/articles/360017014479-Understanding-Automation-Rate-Limits-Across-Social-Media-Platforms.

80 Asia Grace, '*So f-ked up': Instagram slammed for allowing paid content featuring kids in bikinis*, New York Post (Nov. 2, 2022), https://nypost.com/2022/11/02/instagram-slammed-for-paid-content-featuring-kids-in-bikinis/.

81 *Id.*; Jeff Horwitz and Katherine Blunt, *Instagram Connects Vast Pedophile Network*, The Wall Street Journal (Jun. 7, 2023), https://www.wsj.com/articles/instagram-vast-pedophile-network-4ab7189.

82 David Thiel *et al., Cross-Platform Dynamics of Self-Generated CSAM*, Stanford Internet Observatory (Jun. 7, 2023), https://stacks.stanford.edu/file/druid:jd797tp7663/20230606-sio-sg-csam-report.pdf.

83 Brian Neil Levine, *Increasing the Efficacy of Investigations of Online Child Sexual Exploitation*, University of Massachusetts Amherst (May 2022), https://www.ojp.gov/pdffiles1/nij/grants/301590.pdf.

84 Savoia, *supra* note 24.

85 Aaron Smith, *What people like and dislike about Facebook*, Pew Research Center (Feb. 3, 2014), https://www.pewresearch.org/short-reads/2014/02/03/what-people-like-dislike-about-facebook/.

86 *Wave 2 Research findings:, Digital Well-Being Index*, Snapchat Inc. (June 2023), https://assets.ctfassets.net/kw9k15zxztrs/5YeLYk9Rzh2RTOGuGa37aq/09fcac523225cdfd955ab0e06f386ba7/Snap-__2023_Digital_Well-Being_Index_Wave_2_Report.pdf?lang=en-US.

87 *Re: Artificial Intelligence and the Exploitation of Children*, National Association of Attorneys General (Sept. 5, 2023), https://ncdoj.gov/wp-content/uploads/2023/09/54-State-AGs-Urge-Study-of-AI-and-Harmful-Impacts-on-Children.pdf.

88 Tim McNicholas, *New Jersey high school students accused of making AI-generated pornographic images of classmates*, CBS News (updated Nov. 2, 2023), https://www.cbsnews.com/newyork/news/westfield-high-school-ai-pornographic-images-students/.

89 *E.g.* Jennifer Valentino-DeVries and Michael H. Keller, *She Was a Child Instagram Influencer. Her Fans Were Grown Men.*, The New York Times (Nov. 10, 2024), https://www.nytimes.com/2024/11/10/us/child-influencer.html.

90 Ana Da Silva Pinho *et al., Youths' sensitivity to social media feedback: A computational account*, Science Advances (Oct. 23, 2024), https://www.science.org/doi/10.1126/sciadv.adp8775.

91 University of Minnesota, 2024 College Student Health Survey Report, *supra* note 10.

92 Emily A. Vogels and Risa Gelles-Watnick, T*eens and Social Media: Key Findings from Pew Research Center Surveys*, Pew Research (April 24, 2023), https://www.pewresearch.org/short-reads/2023/04/24/teens-and-social-media-key-findings-from-pew-research-center-surveys/.

93 *Accountable Tech: Frequency Questionnaire*, GQR (Jun. 2021), https://accountabletech.org/wp-content/uploads/Accountable-Tech-Parents-Poll.pdf.

94 *APA Chief Scientist Outlines Potential Harms, Benefits of Social Media for Kids*, American Psychological Association (Feb 14, 2023), https://www.apa.org/news/press/releases/2023/02/harms-benefits-social-media-kids.

95 University of Minnesota, 2024 College Student Health Survey Report, *supra* note 10.

96 *Are you TikTok Tired? 93% of Gen Z admit to staying up past their bedtimes due to social media*, American Academy of Sleep Medicine (Sept. 7, 2022), https://aasm.org/are-you-tiktok-tired-93-of-gen-z-admit-to-staying-up-past-their-bedtime-due-to-social-media/.

97 Jenny S. Radesky, Heidi M. Weeks, Alexandria Schaller, Michael B. Robb, Supreet Mann and Amanda Lenhart, *Constant Companion: A Week in the Life of a Young Person's Smartphone Use*, Common Sense Media (2023), https://www.commonsensemedia.org/sites/default/files/research/report/2023-cs-smartphone-research-report_final-for-web.pdf.

98 *Arizona et al. v. Meta Platforms, Inc., et al.*, Case No. 4:23-cv-05448, Complaint (N.D. Cal. Oct. 24, 2023).

99 Alex Hern, *'Never get high on your own supply' – why social media bosses don't use social media*, The Guardian (Jan. 23, 2018), https://www.theguardian.com/media/2018/jan/23/never-get-high-on-your-own-supply-why-social-media-bosses-dont-use-social-media.

100 Treboy Haynes, *Dopamine, Smartphones & You: A battle for your time*, Harvard University Graduate School of Arts and Sciences (May 1, 2018), https://sitn.hms.harvard.edu/flash/2018/dopamine-smartphones-battle-time/; Mark D. Griffiths, *Adolescent social networking: How do social media operators facilitate habitual use?*, 36.3 Education and Health 66 (2018); Rasan Burhan and Jalal Moradzadeh, *Neurotransmitter Dopamine and its Role in the Development of Social Media Addiction*, 11 Journal of Neurology & Neurophysiology 507 (2020), https://www.iomcworld.org/open-access/neurotransmitter-dopamine-da-and-its-role-in-the-development-of-social-media-addiction.pdf; Simon Parkin, *Has dopamine got us hooked on tech?*, The Guardian (Mar. 4, 2018), https://www.theguardian.com/technology/2018/mar/04/has-dopamine-got-us-hooked-on-tech-facebook-apps-addiction#:~:text=To%20achieve%20this%20goal%2C%20Facebook's,then%2C%20built%20upon%20a%20molecule.

101 Jenny Radesky, *What Teens Want Adults to Know About Their Relationships with Smartphones*, Common Sense Media (Sept. 26, 2023), https://www.commonsensemedia.org/kids-action/articles/what-teens-want-adults-to-know-about-their-relationships-with-smartphones ("For me, even throughout the day, I keep 'do not disturb' on, not even because I wanna not respond to people or anything like that. I like being able to not have my phone buzzing, but being able to click on...I don't know if I can show you guys, but like here, you see this. Like you have to click on that to see all of the notifications that people have sent or everything that...All the notifications that you would have gotten if you weren't on 'do not disturb.' For me, I like the extra step because then it's like me having to do more work to be on my phone, and I don't know, I feel like it's a little strategy for me. —11th grader").

102 Jenny S. Radesky, Heidi M. Weeks, Alexandria Schaller, Michael B. Robb, Supreet Mann and Amanda Lenhart, *Constant Companion: A Week in the Life of a Young Person's Smartphone Use,* Common Sense Media (2023), https://www.commonsensemedia.org/sites/default/files/research/report/2023-cs-smartphone-research-report_final-for-web.pdf.

103 Avery Hartmans, *These are the sneaky ways apps like Instagram, Facebook, Tinder lure you in and get you 'addicted'*, Business Insider (Feb. 17, 2018), https://www.businessinsider.com/how-app-developers-keep-us-addicted-to-our-smartphones-2018-1#instagram-sends-dozens-of-push-notifications-each-week-and-uses-stories-to-attract-you-1.

104 *See: Our approach to explaining ranking*, Meta (updated Dec. 31, 2023), https://transparency.fb.com/features/explaining-ranking, for discussion on how time spent features heavily in ranking models. *See also: Commonwealth of Massachusetts v. Meta Platforms, Inc., et al.*, Civ. Action No. 2384cv02397-BLS1, Complaint (Mass. Superior Court, Nov. 6, 2023).

105 Victoria Rideout and Michael B. Robb, *Social media, social life: Teens reveal their experiences*, Common Sense Media (2018), https://www.commonsensemedia.org/sites/default/files/research/report/2018-social-media-social-life-executive-summary-web.pdf.

106 Mary Madden *et al., A Double-Edged Sword: How Diverse Communities of Young People Think About the Multifaceted Relationship Between Social Media and Mental Health*, Common Sense Media (2024), https://www.commonsensemedia.org/sites/default/files/research/report/2024-double-edged-sword-hopelab-report_final-release-for-web-v2.pdf.

107 Drew Harwell, *Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use*, The Washington Post (Dec. 19, 2019), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

108 Miranda Bogen, *All the Ways Hiring Algorithms Can Introduce Bias*, Harvard Business Review (May 6, 2019), https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias.

109 Racial bias has been shown to be exhibited in data used to make medical decisions. *See*: Ziad Obermeyer, Brian Powers, Christine Vogeli, and Sendhl Mullainathan, *Dissecting racial bias in an algorithm used to manage the health of populations*, 366 Science 447 (2019); Crystal Grant, *Algorithms Are Making Decisions About Health Care, Which May Only Worsen Medical Racism*, American Civil Liberties Union (Oct. 3, 2022), https://www.aclu.org/news/privacy-technology/algorithms-in-health-care-may-worsen-medical-racism.

110 Bogen, *All the Ways Hiring Algorithms Can Introduce Bias, supra* note 79.

111 A government discrimination bill was introduced in Washington. *See*: S. 5356, 68th Legis. Sess. (Wash. 2023).

112 Insurance discrimination laws have been introduced in New Jersey, New York, and Rhode Island. *See*: G.A. A537, 220th Legis., Gen. Assemb. (N.J. 2022); G.A. 843, N.Y. Leg. (N.Y. 2023); H 5734, Gen. Assemb. (R.I. 2023).

113 See *Human Rights Due Diligence of Meta's Impacts in Israel and Palestine*, BSR (Sept. 22, 2022), https://www.bsr.org/en/reports/meta-human-rights-israel-palestine, for a discussion of how platforms are never neutral in their content moderation policies.

114 In the criminal justice system, predictive policing tools have integrated data from jurisdictions with a history of biased policing, leading to the perpetuation of bias. *See*: Rashida Richardson, Jason Schultz, and Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. Law Rev. 192 (2019).

115 Facial recognition algorithms often are trained on data without many minorities and therefore perform worse in those cases. *See*: Joy Buolamwini, *Unmasking the bias in facial recognition algorithms*, MIT Sloan School of Management (Dec. 13, 2023), https://mitsloan.mit.edu/ideas-made-to-matter/unmasking-bias-facial-recognition-algorithms.

116 *See*: Jonathan Stray, *Aligning AI to Human Values means Picking the Right Metrics*, Partnership on AI (Apr. 15, 2020), https://partnershiponai.org/aligning-ai-to-human-values-means-picking-the-right-metrics/.

117 *Digital lives of Aussie teens*, Australian Government eSafety Commissioner, https://www.esafety.gov.au/research/digital-lives-of-aussie-teens.

118 *Being a new, female user is not a great experience in most emerging markets.*, FBArchive (September 10, 2020), https://fbarchive.org/doc/odoc2425418629.

119 Jonathan Haidt, *The Dangerous Experiment on Teen Girls*, The Atlantic (Nov. 21, 2021), https://www.theatlantic.com/ideas/archive/2021/11/facebooks-dangerous-experiment-teen-girls/620767/.

120 Emily A. Vogels and Risa Gelles-Watnick, *Teens and social media: Key findings from Pew Research Center surveys*, Pew Research Center (April 24, 2023), https://www.pewresearch.org/short-reads/2023/04/24/teens-and-social-media-key-findings-from-pew-research-center-surveys/.

121 Renata Maria Silva Santos *et al., The associations between screen time and mental health in adolescents: a systematic review*, 11 BMC Psychology 127 (April 20, 2023), https://bmcpsychology.biomedcentral.com/articles/10.1186/s40359-023-01166-7.

122 *Arizona et al. v. Meta Platforms, Inc., et al.*, Case No. 4:23-cv-05448, Complaint (N.D. Cal. Oct. 24, 2023). Source materials online at https://storage.courtlistener.com/recap/gov.uscourts.nmd.496039/gov.uscourts.nmd.496039.36.2.pdf.

123 Alana Papageorgiou, Colleen Fisher, and Donna Cross, *"Why don't I look like her?" How adolescent girls view social media and its connection to body image*, 22 BMC Women's Health 261 (June 27, 2022), https://bmcwomenshealth.biomedcentral.com/articles/10.1186/s12905-022-01845-4.; Megan A. Vendemia and Jesse Fox, *How social media images of sexualized young women elicit appearance commentary from their peers and reinforce objectification*, 49 Body Image (June 2024), https://www.sciencedirect.com/science/article/abs/pii/S1740144524000056.; Ivanka Prichard, Brydie Taylor, and Marika Tiggemann, *Comparing and self-objectifying: The effect of sexualized imagery posted by Instagram Influencers on women's body image*, 46 Body Image (Sept. 2023), https://www.sciencedirect.com/science/article/pii/S1740144523000980.

124 *Appearance-Based Social Comparison*, FBArchive (February 1, 2021), https://fbarchive.org/doc/odoc002426w35.

125 Ben Kesslen, I*nstagram is serving kids' accounts sexual content within minutes*, report says, Quartz (June 20, 2024), https://qz.com/instagram-fills-kids-feeds-with-sexual-content-1851550640.; Suyansh Srivastava, *Exploring Instagram's Algorithmic Bias Towards Attractive Women and Its Impact on Users – Case Study,* Medium (Mar 22, 2023), https://medium.com/@heysuryansh/exploring-instagrams-algorithmic-bias-towards-attractive-women-and-its-impact-on-users-case-79a4c7e6583f.

126 *Technology-Facilitated Gender-Based Violence: A Growing Threat*, United Nations Population Fund, https://www.unfpa.org/TFGBV, (last visited Jan. 19, 2025).

127 *Measuring the prevalence of online violence against women*, The Economist (March 1, 2021), https://onlineviolencewomen.eiu.com/.

128 *FBI San Francisco Sextortion: A Growing Threat Preying Upon Our Nation's Teens*, FBI (Jan. 17, 2024), https://www.fbi.gov/contact-us/field-offices/sacramento/news/sextortion-a-growing-threat-preying-upon-our-nations-teens.

129 Raffile, *supra* note 29.

130 *New Tools to Help Protect Against Sextortion and Intimate Image Abuse*, Instagram (April 11, 2024), https://about.instagram.com/blog/announcements/new-tools-to-help-protect-against-sextortion-and-intimate-image-abuse.

131 Many Instagram protections are limited to accounts deemed "suspicious" per *About Instagram teen privacy and safety settings*, Instagram 2024, https://help.instagram.com/3237561506542117.

132 Caroline Hayes *et al., The Manosphere, Rewired: Understanding Masculinities Online And Pathways For Healthy Connection*, Equimundo (2024), https://www.equimundo.org/wp-content/uploads/2024/06/Manosphere-Rewired.pdf.

133 Amanda Holpuch, *Why Social Media Sites Are Removing Andrew Tate's Accounts*, The New York Times (Aug. 24, 2022), https://www.nytimes.com/2022/08/24/technology/andrew-tate-banned-tiktok-instagram.html.

134 *The draw of the 'manosphere': understanding Andrew Tate's appeal to lost men*, The Conversation (Feb. 12, 2023), https://theconversation.com/the-draw-of-the-manosphere-understanding-andrew-tates-appeal-to-lost-men-199179.

135 Sally Weale, *Social media algorithms 'amplifying misogynistic content'*, The Guardian (Feb. 5, 2024), https://www.theguardian.com/media/2024/feb/06/social-media-algorithms-amplifying-misogynistic-content.

136 Ted Late, *How Did Andrew Tate Make His Money? A Deep Dive Into "Top G's" Earnings*, CoinCodex (Nov. 15, 2024), https://coincodex.com/article/37219/how-did-andrew-tate-make-his-money/.

137 *Africa Insights: Toxic Masculinity Online in Kenya and South Africa*, New Lines Magazine (Jan. 30, 2024), https://newlinesmag.com/podcast/africa-insights-toxic-masculinity-online-in-kenya-and-south-africa/.

138 Mary Madden *et al., A Double-Edged Sword: How Diverse Communities of Young People Think About the Multifaceted Relationship Between Social Media and Mental Health*, Common Sense Media (2024), https://www.commonsensemedia.org/research/double-edged-sword-how-diverse-communities-of-young-people-think-about-social-media-and-mental-health.

139 *Reimagine Black Youth Mental Health*, Brooklyn Bridge Alliance for Youth (last visited Jan. 21, 2024), https://www.brooklynsallianceforyouth.org/black-youth-mental-health.

140 Madden, *supra* note 138.

141 Devin English *et al., Trends in Suicidality and Bullying among New York City Adolescents across Race and Sexual Identity: 2009-2019*, 101 J. Urban Health (May 10, 2024), https://link.springer.com/article/10.1007/s11524-024-00860-0.

142 *New Research from Thorn: LGBTQ+ Minors are 3X More Likely to Experience Unwanted and Risky Online Interactions*, Thorn (June 6, 2023), https://www.thorn.org/blog/new-research-from-thorn-lgbtq-minors-are-3x-more-likely-to-experience-unwanted-and-risky-online-interactions/.

143 Jonathan Haidt and Will Johnson, *Gen Z Has Regrets*, The New York Times (Sept. 17, 2024), https://www.nytimes.com/2024/09/17/opinion/social-media-smartphones-harm-regret.html.

144 Mary Madden, Angela Calvin, Alexa Hasse, and Amanda Lenhart, *The Dawn of the AI Era: Teens, Parents, and the Adoption of Generative AI at Home and School*, Common Sense Media (2024), https://www.commonsensemedia.org/sites/default/files/research/report/2024-the-dawn-of-the-ai-era_final-release-for-web.pdf.

145 Madden, *supra* note 138.

146 *Our Approach to Explaining Ranking*, Meta (December 31, 2023), https://transparency.meta.com/features/explaining-ranking/.

147 Becca Ricks and Jesse McCrosky, *Does This Button Work? Investigating YouTube's ineffective user controls*, Mozilla (Sept. 20, 2022), https://foundation.mozilla.org/en/research/library/user-controls/report/.; *Algorithms of trauma: new case study shows that Facebook doesn't give users real control over disturbing surveillance ads*, Panoptykon Foundation (Sept. 28, 2021), https://en.panoptykon.org/algorithms-trauma-new-case-study-shows-facebook-doesnt-give-users-real-control-over-disturbing.

148 Online Safety Act 2023, c. 50 (UK), *see also* Online Safety Act: Explainer (May 8, 2024), https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer.

149 Peter Guest, *The UK's Controversial Online Safety Act is Now Law*, Wired (Oct. 26, 2023), https://www.wired.com/story/the-uks-controversial-online-safety-act-is-now-law/.

150 *Protection of Children Code of Practice for user-to-user services*, Ofcom (May 8, 2024), https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/284469-consultation-protecting-children-from-harms-online/associated-documents/a7-draft-childrens-safety-code-user-to-user-services.pdf?v=336059.

151 *The Digital Services Act package*, European Commission, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

152 Christoph Schmon, *DSA: EU Parliament Vote Ensures a Free Internet, But a Final Regulation Must Add Stronger Priacy Protections*, Electronic Frontier Foundation (Jan. 20, 2022), https://www.eff.org/deeplinks/2022/01/dsa-eu-parliaments-position-ensures-free-internet-human-rights-safeguards-need-be; *EU: Put Fundamental Rights at Top of Digital Regulation*, Human Rights Watch (Jan. 7, 2022), https://www.hrw.org/news/2022/01/07/eu-put-fundamental-rights-top-digital-regulation.

153 Regulation (EU) 2022/2065 of the European Parliament and the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), (2022), https://www.eu-digital-services-act.com/Digital_Services_Act_Article_28.html.

154 Natasha Lomas, *TikTok Lite: EU closes addictive design case after TikTok commits to not bring back rewards mechanism*, TechCrunch (Aug. 5, 2024), https://techcrunch.com/2024/08/05/tiktok-lite-eu-closes-addictive-design-case-after-tiktok-commits-to-not-bring-back-rewards-mechanism/.

155 Simone De La Feld, *The EU has already launched investigations into all major social platforms. The real challenge is concluding them*, EUNews (Jan. 9, 2025), https://www.eunews.it/en/2025/01/09/the-eu-has-already-launched-investigations-into-all-major-social-platforms-the-real-challenge-is-concluding-them/.

156 *Learn about the Online Safety Act*, Australian Government eSafety Commissioner, https://www.esafety.gov.au/newsroom/whats-on/online-safety-act.

157 *Statutory Review of the Online Safety Act 2021*, Australian Government Dept. of Infrastructure, Transport, Regional Development, Communications and the Arts (April 2024), https://www.infrastructure.gov.au/sites/default/files/documents/online-safety-act-2021-review-issues-paper-26-april-2024.pdf.

158 *Banning social media for children*, Government of South Australia (last visited Jan. 19, 2025), https://www.premier.sa.gov.au/media-releases/news-items/banning-social-media-for-children.

159 *Australia plans minimum age for social media use, angering digital rights advocates*, NBC News (Sept. 10, 2024), https://www.nbcnews.com/news/world/australia-plans-minimum-age-social-media-use-rcna170357.

160 Nidhi Suresh, *India's 'draconian' IT laws draw ire from civil society*, Deutsche Welle (May 17, 2023), https://www.dw.com/en/indias-draconian-it-laws-draw-ire-from-civil-society/a-65657406.

161 Mordechai Kremnitzer, *The Bill on Social Media Incitement Is a Danger to Freedom of Expression*, Haaretz (Dec. 30, 2021), https://www.haaretz.com/israel-news/2021-12-30/ty-article/.premium/the-bill-on-social-media-incitement-is-a-danger-to-freedom-of-expression/0000017f-e313-d7b2-a77f-e317f2400000; Jesse Barron, *How Four Posts on Instagram Destroyed Her Life*, The New York Times (Nov. 3, 2024), https://www.nytimes.com/2024/11/03/magazine/israel-free-speech.html.

162 *See*: @ThierryBreton, Twitter (Oct. 10, 2023, 1:20 PM), https://twitter.com/ThierryBreton/status/1711808891757944866; Foo Yun Chee and Sudip Kar-Gupta, *EU industry chief warns Alphabet CEO on tech rules compliance after Hamas attack*, Reuters (Oct. 13, 2023), https://www.reuters.com/technology/eu-industry-chief-warns-alphabet-ceo-tech-rules-compliance-after-hamas-attack-2023-10-13/.

163 Peter Chapman, *Advancing Platform Accountability: The Promise and Perils of DSA Risk Assessment*, Tech Policy Press (Jan. 9, 2025), https://www.techpolicy.press/advancing-platform-accountability-the-promise-and-perils-of-dsa-risk-assessments/.

164 *NetChoice v. Bonta*, No. 22-cv-08861-BLF, Pet. Suppl. Br. in Supp. of Mot. for Prelim. Inj.

165 S. 7072, Fla. S. (Fla. 2021).

166 *NetChoice, LLC v. Moody*, 546 F. Supp. 3d 1082 (N.D. Fla. 2021).

167 *NetChoice, LLC v. Moody*, 34 F.4th 1196 (11th Cir. 2022).

168 HB 20, 87th Legis. Sess., Tex. Leg. (Tex. 2021).

169 *NetChoice, LLC v. Paxton*, 573 F. Supp. 3d 1092 (W.D. Tex. 2021).

170 *NetChoice, LLC. v. Paxton*, 49 F.4th 439 (5th Cir. 2022); Emergency Appl. for Immediate Administrative Relief and to Vacate Stay of Prelim. Inj., *NetChoice, LLC. v. Paxton*, No. 21-A720, 2022 WL 2358461 (U.S. May 13, 2022), https://www.supremecourt.gov/DocketPDF/21/21A720/225388/20220513192559757_Supreme%20Court%20Vacatur%20Application.pdf.

171 *NetChoice, LLC v. Paxton*, 142 S. Ct. 1715 (2022).

172 *NetChoice, LLC. v. Paxton*, 49 F.4th 439 (5th Cir. 2022), cert. granted in part sub nom. *NetChoice, LLC v. Paxton*, 216 L. Ed. 2d 1313 (Sept. 29, 2023).

173 *Moody v. NetChoice, LLC*, SCOTUSblog, https://www.scotusblog.com/case-files/cases/moody-v-NetChoice-llc/.

174 Megan Iorio, Schuyler Standley, and Tom McBrien, *Four Key Takeaways from the Moody v. NetChoice and NetChoice v. Paxton Oral Arguments*, Electronic Privacy Information Center (Feb. 28, 2024), https://epic.org/four-key-takeaways-from-the-netchoice-v-moody-and-paxton-oral-arguments/.

175 *See: Miami Herald Publishing Co v. Tornillo*, 418 U.S. 241, 261 (1974).

176 Megan Iorio, Schuyler Standley, and Tom McBrien, *Four Key Takeaways from the Moody v. NetChoice and NetChoice v. Paxton Oral Arguments*, Electronic Privacy Information Center (Feb. 28, 2024), https://reason.com/wp-content/uploads/2025/01/netchoice-v-bonta-order-preliminary-injunction.pdf.

177 68th Montana Legis. Sess., SB0419 (banning TikTok), https://leg.mt.gov/bills/2023/billpdf/SB0419.pdf.

178 *Alario v. Knudsen*, No. CV 23-56-M-DWM, 2023 U.S. Dist. LEXIS 213547 (D. Mont. Nov. 30, 2023).

179 Nate Raymond, *US judge blocks Ohio law restricting children's use of social media,* Reuters (Feb. 13, 2024), https://www.reuters.com/legal/us-judge-blocks-ohio-law-restricting-childrens-use-social-media-2024-02-12/.; *Judge Blocks Arkansas Law that Would Have Placed Unconstitutional Age-Verification and Parental Consent Requirements on Social Media Use*, ACLU (Sept. 1, 2023), https://www.aclu.org/press-releases/judge-blocks-arkansas-law-that-would-have-placed-unconstitutional-age-verification-and-parental-consent-requirements-on-social-media-users.

180 *See: TikTok Inc. and ByteDance Ltd. v. Garland*, 604 U.S. __, 2025 WL 222571 (Jan. 17, 2025).

181 Larry Magid, *Social media and children's rights in the global village*, Connect Safely (Nov. 6, 2015), https://connectsafely.org/rights-of-children-in-the-digital-age/.

182 Sapna Maheshwari, *Judge Halts TikTok Ban in Montana*, The New York Times (Nov. 30, 2023), https://www.nytimes.com/2023/11/30/business/tiktok-montana-ban-blocked.html.

183 The Kids Online Safety Act has at times been combined with privacy provisions in a combined package known as the Kids Online Safety and Privacy Act (KOSPA).

184 Kids Online Safety Act, S. 1409, 118th Cong. § 1 (2023).

185 *The Kids Online Safety Act*, https://www.blumenthal.senate.gov/imo/media/doc/kids_online_safety_act_-_one_pager.pdf.

186 *RE: Vote "No" on the Kids Online Safety Act*, S. 1409, American Civil Liberties Union (Jul. 27, 2023), https://www.aclu.org/wp-content/uploads/2023/10/2023.07.27-KOSA-Letter.pdf.

187 Matt Lavietes, *Senator Appeared to Suggest Bipartisan Bill Would Censor Transgender Content Online*, NBC News (Sept. 5, 2023), https://www.nbcnews.com/nbc-out/out-politics-and-policy/senator-appears-suggest-bipartisan-bill-will-censor-transgender-conten-rcna103479.

188 *Age appropriate design: a code of practice for online services*, UK Information Commissioner's Office: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/#:~:text=The%20code%20is%20a%20set,designing%20and%20developing%20online%20services

189 *Id*.

190 Jane Wakefield, *Children's internet code: What is it and how will it work?*, BBC (Sept. 1, 2021), https://www.bbc.com/news/technology-58396004.

191 The California Age-Appropriate Design Code, AB-2273, California Assembly (2022).

192 *NetChoice, LLC v. Bonta*, No. 22-cv-08861-BLF, 2023 U.S. Dist. LEXIS 165500, Complaint (N.D. Cal. Dec. 14, 2023).

193 *NetChoice, LLC v. Bonta*, No. 22-cv-08861-BLF, 2023 U.S. Dist. LEXIS 165500 (N.D. Cal. Sep. 18, 2023).

194 *Id*.

195 *NetChoice, LLC v. Bonta*, No. 22-cv-08861-BLF, 2023 U.S. Dist. LEXIS 165500, Notice of Prelim. Inj. Appeal (N.D. Cal.) Oct. 18, 2023.

196 S. 3, 2023 Gen. Assemb. (Conn. 2023).

197 Delaware Online Privacy and Protection Act, 80 Del. Laws, c. 148, §1.

198 S. 7695, State S. (N.Y., 2023).

199 Utah Code Title 13, Chapter 63.

200 *NetChoice, LLC, v. Reyes*, No. CV-00911 (D. Utah), Compl., Dec. 18, 2023; *See also*, Julia Shapero, *Group Representing Social Media Giants Sues Utah Over Parental Consent Law*, The Hill (Dec. 19, 2023), https://thehill.com/policy/technology/4367595-group-representing-social-mediagiants-sues-utah-over-parental-consent-law/.

201 S. 7694, State S. (N.Y., 2023).

202 *Id.*; *See also*, N.Y. Gov. Hochul Press Release (Oct. 11, 2023), https://www.governor.ny.gov/news/governor-hochul-attorney-general-james-senator-gounardes-and-assemblymember-rozic-take-action.

203 *Amicus Briefs NetChoice v. Bonta*, Electronic Privacy Information Center (Dec 2024), https://epic.org/documents/netchoice-v-bonta-2/.

204 *See, e.g., id.* Chronological feeds have been shown to increase experiences of harm. *See* Adam Kovacevich, *New York's Chronological Social Media Feeds Legislation Could Backfire. Here's Why*, Lohud. (March 27, 2024), https://www.lohud.com/story/opinion/2024/03/27/ny-legislation-on-chronological-social-media-fees-could-backfire/73057315007/.

205 Regulation (EU) 2016/679 (General Data Protection Regulation), https://gdpr-info.eu/.

206 *Comparing U.S. State Data Privacy Laws vs. the EU's GDPR*, Bloomberg Law (Jul. 11, 2023), https://pro.bloomberglaw.com/insights/privacy/privacy-laws-us-vs-eu-gdpr/.

207 *See, e.g.*, Cal. Civ. Code § 1798.100 *et seq*.; Colo. Rev. Stat. § 6-1-1301, *et seq*.; Conn. Public Act No. 22-15; 84 Del. Laws, c. 197; 2023 Ind. Acts, Public Law 94; 2023 Mont. Laws Ch. 681; 2023 Or. Laws ch. 369; 2023 Tenn. Pub. Act Ch. 408; 2023 Tex. Gen. Laws, 88(R), H.B. 4; 2023 Utah Laws Ch. 462; Va. Code Ann. § 59.1-571, *et seq*.

208 Such bills have been passed or considered in Hawaii, New Hampshire, Pennsylvania, Rhode Island, and Minnesota. *See*, S. 974, State Leg. (Haw. 2023); H.R. 708, Gen. Assemb. (Pa. 2023); H.R. 6236, Gen. Assemb. (R.I. 2023); H.R. 2309, H. (Minn. 2023).

209 *Riding the Wave: US Privacy Laws Continue to Proliferate in 2024*, Latham & Watkins (May 20, 2024), https://www.lw.com/admin/upload/SiteAttachments/Riding_the_Wave_US_Privacy_Laws_Continue_to_Proliferate_in_2024.pdf.

210 Florence G'Sell, *Regulating Under Uncertainty: Governance Options for Generative AI*, Stanford Cyber Policy Center, Freeman Spogli Institute Stanford Law School (last visited Jan. 21, 2025), https://fsi9-prod.s3.us-west-1.amazonaws.com/s3fs-public/2024-10/GenAI_Report_REV_Master_2%20final%20as%20of%20Oct%2025%202024.pdf.

211 The White House, *Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence* (Oct. 30, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/.

212 David Shepardson, *Trump revokes Biden executive order on addressing AI risks*, Reuters (Jan. 21, 2025), https://www.reuters.com/technology/artificial-intelligence/trump-revokes-biden-executive-order-addressing-ai-risks-2025-01-21/.

213 *Artificial Intelligence 2024 Legislation*, National Conference of State Legislatures (Sept. 9, 2024), https://www.ncsl.org/technology-and-communication/artificial-intelligence-2024-legislation.

214 New York City Department of Consumer and Worker Protection, Notice of Adoption of Final Rule relating to Automated Employment Decision Tools (AEDT), https://rules.cityofnewyork.us/wp-content/uploads/2023/04/DCWP-NOA-for-Use-of-Automated-Employment-Decisionmaking-Tools-2.pdf.

215 *Illinois Becomes Second State to Pass Broad Legislation on the Use of AI in Employment Decisions*, Jones Day (Oct. 29, 2024), https://www.jonesday.com/en/insights/2024/10/illinois-becomes-second-state-to-pass-broad-legislation-on-the-use-of-ai-in-employment-decisions#:~:text=Effective%20January%201%2C%202026%2C%20amendments,basis%20of%20a%20protected%20class.

216 CalChamber, *CalChamber Wraps Historic Legislative Year with Major Wins for Business*, Advocacy (Sept. 3, 2024), https://advocacy.calchamber.com/2024/09/03/calchamber-wraps-historic-legislative-year-with-major-wins-for-business/.

217 Kirk J. Nahra *et al., Colorado State Legislature Passes AI Bill With the Potential to Broadly Regulate AI*, WilmerHale (May 17, 2024), https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20240517-colorado-state-legislature-passes-ai-bill-with-the-potential-to-broadly-regulate-ai.

218 *Deepfakes & Synthetic Media*, Multistate (last visited Jan. 21, 2025), https://www.multistate.ai/deepfakes-synthetic-media.

219 H.R. 1063, Gen. Assem. (Penn. 2023).

220 Lawrence Norden, Niyati Narang, and Laura J. Protzmann, *States Take the Lead in Regulating AI in Elections – Within Limits*, Brennan Center for Justice (Aug. 7, 2024), https://www.brennancenter.org/our-work/research-reports/states-take-lead-regulating-ai-elections-within-limits.

221 Va. Penal § 18.2-386.2 (2019), https://lis.virginia.gov/cgi-bin/legp604.exe?191+sum+HB2678.; N.Y. SB 1042A, amending N.Y. Penal Law § 245.15 (2024), https://www.nysenate.gov/legislation/bills/2023/S1042/amendment/A.; Tex. SB 1361, Unlawful Production or Distribution of Certain Sexually Explicit Videos, Tex. Penal tit. 5 § 21.165 (2024), https://capitol.texas.gov/tlodocs/88R/billtext/html/ HB02700H.htm.

222 CA, IL - Cal. AB-602 (2019), Depiction of individual using digital or electronic technology: sexually explicit material, https://leginfo.legislature.ca.gov/faces/billTextClient. xhtml?bill_id=201920200AB602.; 1813 Ill. Pub. Act 103-0571 (2023), https://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=103-0571.

223 Fla. SB 1798 (2022), https://www.flsenate.gov/Committees/BillSummaries/2022/html/2658.; 99th South Dakota Legis. Sess., SB 79, https://sdlegislature.gov/Session/Bill/24991/264651.; Wash. HB 1999 (2023), https://app.leg.wa.gov/billsummary?BillNumber=1999&Year=2023&Initiative=false.

224 *State of Minnesota v. Casillas*, Case No. A19-0576, (Minn. 2020). Source materials online at https://mn.gov/law-library-stat/archive/supct/2020/OPA190576-123020.pdf.

225 Elizabeth Nolan Brown, *Minnesota 'Acting as a Ministry of Truth' With Anti-Deep Fake Law, Says Lawsuit*, Reason (Oct. 2, 2024), https://reason.com/2024/10/02/minnesota-acting-as-a-ministry-of-truth-with-anti-deep-fake-law-says-lawsuit/.

226 Daniel Wu, *His daughter was murdered. Then she reappeared as an AI chatbot.*, The Washington Post (Oct. 15, 2024), https://www.washingtonpost.com/nation/2024/10/15/murdered-daughter-ai-chatbot-crecente/.

227 Tenn. HB 2091 (2024), https://publications.tnsosfiles.com/acts/113/pub/pc0588.pdf.; Stuart D. Levi *et al., Tennessee Law Addresses Proliferation of Deepfakes*, Skadden (April 2, 2024), https://www.skadden.com/insights/publications/2024/04/tennessee-law-addresses-proliferation-of-deepfakes.

228 *Id.*

229 *See*, H.R. 2060, Tex. Leg. (2023); S. 1103, Gen. Assem. (Conn. 2023); S. 0117, Gen. Assem. (R.I. 2023).

230 *European Artificial Intelligence Act comes into force*, European Commission (July 31, 2024), https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4123.

231 *EU AI Act: First Regulation on Artificial Intelligence*, European Parliament (last updated Dec. 19, 2023), https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

232 Laura Schertel Mendes and Beatriz Kira, *The road to regulation of artificial intelligence: the Brazilian experience*, Internet Policy Review (Dec. 21, 2023), https://policyreview.info/articles/news/road-regulation-artificial-intelligence-brazilian-experience/1737.

233 *NetChoice, LLC v. Bonta*, No. 22-cv-08861-BLF, 2023 U.S. Dist. LEXIS 165500 (N.D. Cal. Sep. 18, 2023).

234 David Stauss and Shelby Dolen, *Ninth Circuit Issues Opinion on Constitutionality of California's AADC*, Byte Back Husch Blackwell's Data Privacy and Cybersecurity Legal Resource (Aug. 20, 2024), https://www.bytebacklaw.com/2024/08/ninth-circuit-issues-opinion-on-constitutionality-of-californias-aadc/.

235 Matt Lavietes, *Senator Appeared to Suggest Bipartisan Bill Would Censor Transgender Content Online*, NBC News (Sept. 5, 2023), https://www.nbcnews.com/nbc-out/out-politics-and-policy/senator-appears-suggest-bipartisan-bill-will-censor-transgender-conten-rcna103479.

236 Casey Newton, *How the Kids Online Safety Act Puts Us All At Risk*, The Verge (Aug. 4, 2023), https://www.theverge.com/2023/8/4/23819578/kosa-kids-online-safety-act-privacy-danger.

237 Caroline Cummings, *Minnesota House Panel Revives Discussion About Bill Prohibiting Social Media Algorithms Targeting Teens*, WCCO News (Mar. 1, 2023), https://www.cbsnews.com/minnesota/news/house-panel-bill-prohibiting-social-media-algorithms-targeting-teens/.

238 *NetChoice, LLC v. Yost*, No. 2:24-cv-00047, 2024 U.S. Dist. LEXIS 6349 (S.D. Ohio Jan. 9, 2024).

239 *See* Tom Kemp, *Falling Down Rabbit Holes: The Impact of Big Tech on Kids*, Porchlight Books (Aug. 23, 2023), https://www.porchlightbooks.com/blog/changethis/2023/containing-big-tech.

240 A chronological feed presents content in order of recency, rather than by an algorithm that maximizes engagement. *See* Thomas Macaulay, *Facebook Whistleblower Has an Obvious Solution to Fix the News Feed*, The Next Web (Oct. 6, 2021), https://thenextweb.com/news/facebook-whistleblower-wants-ditch-algorithmic-engagement-ranking-restore-chronological-news-feeds.

241 Luis Ferre-Sadurni, *New York Seeks to Limit Social Media's Grip on Children's Attention*, The New York Times (Oct. 11, 2023), https://www.nytimes.com/2023/10/11/nyregion/tiktok-instagram-algorithm-children.html.

242 Paresh Dave, *Meta Just Proved People Hate Chronological Feeds*, Wired (Jul. 27, 2023), https://www.wired.com/story/meta-just-proved-people-hate-chronological-feeds/.

243 Matthew Hindman, Nathaniel Lubin, and Trevor Davis, *supra* note 33.

244 Carolyn Thompson and Haleluya Hadero, '*Addictive' Social Media Feeds that Keep Children Online Targeted by New York Lawmakers*, AP News (Oct. 11, 2023), https://apnews.com/article/data-privacy-regulation-facebook-instagram-social-media-798dbfa6004da3a2aa2c36031369a909.

245 Aliya Bhatia and Asha Allen, *Auditing in the Dark: Guidance is Needed to Ensure Maximum Impact of DSA Algorithmic Audits*, Center for Democracy & Technology (Nov. 20, 2023), https://cdt.org/insights/auditing-in-the-dark-guidance-is-needed-to-ensure-maximum-impact-of-dsa-algorithmic-audits/.

246 Based on conversations an author of this report has had with people familiar with the reaction to these reports. *See also*, Clothilde Goujard, *Critics Hit Out at Social Media Platforms' Disinformation Reports*, Politico (Feb. 9, 2023), https://www.politico.eu/article/critics-social-media-platforms-disinformation-report-european-union-meta-youtube-twitter-tiktok/.

247 Peter Chapman, *Advancing Platform Accountability: The Promise and Perils of DSA Risk Assessment*, Tech Policy Press (Jan. 9, 2025), https://www.techpolicy.press/advancing-platform-accountability-the-promise-and-perils-of-dsa-risk-assessments/.

248 Federal Trade Commission, *Children's Online Privacy Protection Rule ("COPPA")*, FTC (last visited Jan. 22, 2025), https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa.

249 *Study: Average teen received more than 200 app notifications a day*, Michigan Medicine at the University of Michigan (Sept. 26, 2023), https://www.michiganmedicine.org/health-lab/study-average-teen-received-more-200-app-notifications-day.

250 Natasha Singer, *Sweeping Children's Online Safety Bill Is Passed In California*, The New York Times (Aug. 30, 2022), https://www.nytimes.com/2022/08/30/business/california-children-online-safety.html. Notably, supporters of such laws dispute this characterization and have adjusted language accordingly in subsequent versions to specifically exclude journalistic enterprises as a result.

251 *Kids Online Safety Act Remains A Threat to Minors and Free Speech*, TechFreedom (May 2, 2023), https://techfreedom.org/kids-online-safety-act-remains-a-threat-to-minors-and-free-speech/.

252 Michigan Medicine, *supra* note 249.

253 Jonathan Haidt, *The Anxious Generation: How the Great Rewiring of Childhood is Causing an Epidemic of Mental Illness* 267 (2024).

254 *NetChoice, LLC, v. Bonta*, No. 22-cv-08861-BLF, 2023 U.S. Dist. LEXIS 165500 (N.D. Cal Sep. 18, 2023).

255 Eric Goldman, *The Constitutionality of Mandating Editorial Transparency*, 73 Hastings Law Journal 1203 (2022).

256 Brett Frischmann and Susan Benesch, *Friction-In-Design Regulation as 21st Century Time, Place, and Manner Restriction*, 25 Yale J.L. & Tech. 376 (2023).

257 David Stauss and Shelby Dolen, *Ninth Circuit Issues Opinion on Constitutionality of California's AADC*, Byte Back Husch Blackwell's Data Privacy and Cybersecurity Legal Resource (Aug. 20, 2024), https://www.bytebacklaw.com/2024/08/ninth-circuit-issues-opinion-on-constitutionality-of-californias-aadc/.

258 *In re Social Media Adolescent Addiction/Personal Injury Products Liability Litigation*, MDL No. 3047, Case No. 4:22-md-03047-YGR, Order Granting in Part and Denying in Part Defendants' Motions to Dismiss (N.D. Cal., Nov. 14, 2023).

259 *NetChoice, LLC v. Bonta*, No. 5:24-cv-07885-EJD (N.D. Cal. Dec. 31, 2024). Source materials online at https://reason.com/wp-content/uploads/2025/01/netchoice-v-bonta-order-preliminary-injunction.pdf.

260 *See id*.

261 Among the mandates upheld in this decision were: Mandating parental controls, mandating options to self-restrict time, bans on making it challenging to delete accounts, mandating not using robust age verification, making it challenging to report content, offering appearance altering filters, not labeling filtered content, timing and clustering of notifications to increase use, not implementing protocols to allow reporting of CSAM without login.

262 *Digital Discourse for a Thriving Democracy and Resilient Communities*, Convergence Collective Project, https://convergencepolicy.org/our-work/democracy-and-civic-engagement/thriving-democracy/.

263 *Brand Safety vs. Brand Suitability: What's the Difference?*, Oasis Consortium (last visited Jan. 22, 2025), https://www.oasisconsortium.com/insights/brand-safety-vs-brand-suitability; and Check My Ads (https://checkmyads.org/) have sought to provide advertiser transparency.

264 Tim Walker, *Take Cellphones Out of the Classroom, Educators Say*, NEA Today (Oct. 3, 2024), https://www.nea.org/nea-today/all-news-articles/take-cellphones-out-classroom-educators-say#:~:text=A%202024%20National%20Education%20Association,to%20the%20entire%20school%20day.

265 Susannah Luthi, *'Functionally Useless': California Privacy Law's Big Reveal Falls Short*, Politico (Aug. 5, 2021), https://www.politico.com/states/california/story/2021/08/05/functionally-useless-california-privacy-laws-big-reveal-falls-short-1389429.

266 *Arizona et al. v. Meta Platforms, Inc., et al*., Case No. 4:23-cv-05448, Complaint (N.D. Cal. Oct. 24, 2023).

267 A 2021 internal Meta document found that "when [D]aisy controls are opt-in, only 0.72% of people choose to hide like counts, but when they're opt-out, 35% leave their like counts hidden." *See Commonwealth of Massachusetts v. Meta Platforms, Inc., et al.*, Civ. Action No. 2384cv02397-BLS1, Complaint (Mass. Superior Court, Nov. 6, 2023). Research conducted on Twitter in 2022 concluded that the "percent of all users that opt out [of the algorithmic feed] is between one and ten percent." *See* Smitha Milli *et al., Causal Inference Struggles with Agency on Online Platforms*, Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency, pp. 357-65 (2022).

268 Manish Singh, *Facebook Rolls Out Feature to Help Women in India Easily Lock Their Accounts*, TechCrunch.com (May 21, 2020), https://techcrunch.com/2020/05/21/facebooks-new-safety-feature-for-women-in-india-easily-lock-the-account-from-strangers/.

269 *See, e.g.*, SB0419, 68th Montana Legis. Sess., (banning TikTok).

270 Leonardo Bursztyn, *et al., When Product Markets Become Collective Traps: The Case of Social Media*, Becker Friedman Institute for Economics at the University of Chicago (Oct. 3, 2023), https://bfi.uchicago.edu/wp-content/uploads/2023/10/BFI_WP_2023-131.pdf.

271 Emily A. Vogels and Risa Gelles-Watnick, *Teens and Social Media: Key Findings from Pew Research Center Surveys*, Pew Research (Apr. 24, 2023), https://www.pewresearch.org/short-reads/2023/04/24/teens-and-social-media-key-findings-from-pew-research-center-surveys/.

272 Matt Motyl, *What Do Negative Experiences Look Like On Different Social Media Platforms?*, Substack Blog (Jul. 17, 2023), https://psychoftech.substack.com/p/what-do-negative-experiences-look.

273 *See, e.g.*, https://fbarchive.org/doc/odoc9919.

274 Sheera Frenkel and Mike Isaac, *Inside Facebook's Election 'War Room'*, The New York Times (Sept. 19, 2018), https://www.nytimes.com/2018/09/19/technology/facebook-election-war-room.html.

275 Justin Hendrix, *Read the January 6 Committee Social Media Report*, Tech Policy.Press (Jan. 17, 2023), https://www.techpolicy.press/read-the-january-6-committee-social-media-report/.

276 Written Testimony of Arturo Bejar before the U.S. Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law (November 7, 2023), https://www.judiciary.senate.gov/imo/media/doc/2023-11-07_-_testimony_-_bejar.pdf.

277 Farnoush Amiri and Barbara Ortutay, *Ex-Twitter Execs Deny Pressure to Block Hunter Biden Story*, AP News (Feb. 8, 2023), https://apnews.com/article/technology-politics-united-states-government-us-republican-party-business-6e34ad121a1e52892b782b0b7c0e59c3.

278 Angel Diaz and Laura Hecht-Felella, *Double Standards in Social Media Content Moderation*, Brennan Center (Aug. 4, 2021), https://www.brennancenter.org/our-work/research-reports/double-standards-social-media-content-moderation.

279 *NetChoice v. Bonta*, No. 22-cv-08861-BLF, Pet. Suppl. Br. in Supp. of Mot. for Prelim. Inj. Notably, the latest version of the Minnesota AADC attempts to address this by clarifying a design focus.

280 *See: Moody v. NetChoice and NetChoice v. Paxton*.

281 Sabhanaz Rashid Diya, *The UN's Blueprint for the Internet Could End Up Breaking It*, Tech Policy Press (Nov 1, 2023), https://techpolicy.press/the-uns-blueprint-for-the-internet-could-end-up-breaking-it/.

282 Hashtag Generation *et. al., Joint Letter to the Ministry of Public Security Sri Lanka Concerning Online Safety Bill 19.01.20*, https://docs.google.com/document/d/1yplUx3kB_5eT65Ur_ev4G_UiYGKdjVe8W1MiPjk61tA/edit.

283 *Group Invite Rate Limit Experiment Analysis*, FBArchive (published on web May 15, 2023), https://fbarchive.org/doc/odoc4224824417.

284 Andrew Hutchinson, *Facebook Limits Content Sharing in Ethiopia to Limit the Spread of Misinformation and Hate Speech*, Social Media Today (Nov. 9, 2021), https://www.socialmediatoday.com/news/facebook-limits-content-sharing-in-ethiopia-to-limit-the-spread-of-misinfor/609784/.

285 Mark Scott, *How a British baroness is shaping America's tech laws for kids*, POLITICO (June 14, 2023), https://www.politico.com/news/2023/06/14/british-baroness-online-safety-laws-00101854.

286 *Google announcement shows impact of Childrens Code*, 5Rights, https://5rightsfoundation.com/in-action/google-announcement-shows-impact-of-childrens-code.html.

287 *Furthering our safety and privacy commitments for teens on TikTok*, TikTok Newsroom (Aug. 12, 2021), https://newsroom.tiktok.com/en-us/furthering-our-safety-and-privacy-commitments-for-teens-on-tiktok-us.

288 *Giving Young People a Safer, More Private Experience*, Instagram Blog, https://about.instagram.com/blog/announcements/giving-young-people-a-safer-more-private-experience.

289 John Wihbey, *Facing pressure, lawsuits and Congress, Instagram rolls out sweeping changes for teens*, Northeastern University College of Social Sciences and Humanities (Sept. 20, 2024), https://cssh.northeastern.edu/facing-pressure-lawsuits-and-congress-instagram-rolls-out-sweeping-changes-for-teens/.

290 Matthew Lane, *KOSA Won't Make The Internet Safer For Kids. So What Will?*, Techdirt (Oct. 5, 2023), https://www.techdirt.com/2023/10/05/kosa-wont-make-the-internet-safer-for-kids-so-what-will/.

291 *Teen and Young Adult Perspectives on Generative AI: Patterns of use, excitements, and concerns*, Common Sense Media (last visited Jan. 22, 2025), https://www.commonsensemedia.org/sites/default/files/research/report/teen-and-young-adult-perspectives-on-generative-ai.pdf.

292 Ann Newton, *Neely Center Introduces First-of-its-Kind Artificial Intelligence Index*, USC Marshall School of Business (June, 29, 2023), https://www.marshall.usc.edu/posts/neely-center-introduces-first-of-its-kind-artificial-intelligence-index.

293 Mary Madden, Angela Calvin, Alexa Hasse, and Amanda Lenhart, *The Dawn of the AI Era: Teens, Parents, and the Adoption of Generative AI at Home and School*, Common Sense Media (2024), https://www.commonsensemedia.org/sites/default/files/research/report/2024-the-dawn-of-the-ai-era_final-release-for-web.pdf.

294 *Artificial Intelligence and the Exploitation of Children*, National Association of Attorneys General (Sept. 5, 2023), https://ncdoj.gov/wp-content/uploads/2023/09/54-State-AGs-Urge-Study-of-AI-and-Harmful-Impacts-on-Children.pdf.

295 *Teen and Young Adult Perspectives on Generative AI: Patterns of use, excitements, and concerns*, Common Sense Media (last visited Jan. 22, 2025), https://digitalthriving.gse.harvard.edu/wp-content/uploads/2024/06/Teen-and-Young-Adult-Perspectives-on-Generative-AI.pdf.

296 Tim McNicholas, *New Jersey high school students accused of making AI-generated pornographic images of classmates*, CBS News (Nov. 2, 2023), https://www.cbsnews.com/newyork/news/westfield-high-school-ai-pornographic-images-students/.; Lauraine Langreo, *Students Are Sharing Sexually Explicit 'Deepfakes.' Are Schools Prepared?*, Ed Week (Sept. 26, 2024), https://www.edweek.org/leadership/students-are-sharing-sexually-explicit-deepfakes-are-schools-prepared/2024/09.; *AI nudes of Victorian students were allegedly shared online. How can schools and parents respond to deepfake porn?* Gabrielle Hunt and Daryl Higgens for the Conversation, The Guardian (June, 12, 2024), https://www.theguardian.com/australia-news/article/2024/jun/12/ai-nudes-of-victorian-students-were-allegedly-shared-online-how-can-schools-and-parents-respond-to-deepfake-porn.

297 Elizabeth Laird, Maddy Dwyer and Kristin Woelfel, *In Deep Trouble: Surfacing Tech-Powered Sexual Harassment in K-12 Schools*, Center for Democracy & Technology (Sept. 26, 2024), https://cdt.org/wp-content/uploads/2024/09/FINAL-UPDATED-CDT-2024-NCII-Polling-Slide-Deck.pdf.

298 Mary Madden, Angela Calvin, Alexa Hasse, and Amanda Lenhart, *The Dawn of the AI Era: Teens, Parents, and the Adoption of Generative AI at Home and School*, Common Sense Media (2024), https://www.commonsensemedia.org/sites/default/files/research/report/2024-the-dawn-of-the-ai-era_final-release-for-web.pdf.

299 *What is My AI on Snapchat and how do I use it?*, Snapchat (2024), https://help.snapchat.com/hc/en-us/articles/13266788358932-What-is-My-AI-on-Snapchat-and-how-do-I-use-it.

300 Jessica Lucas, *The teens making friends with AI chatbots*, The Verge (May 4, 2024), https://www.theverge.com/2024/5/4/24144763/ai-chatbot-friends-character-teens.

301 Rebecca Klar, *Open AI exec warns AI can become 'extremely addictive'*, The Hill (Sept. 29, 2023), https://thehill.com/policy/technology/4229972-open-ai-exec-warns-ai-can-become-extremely-addictive/.

302 Hannah R. Marriott and Valentina Pitardi, *One is the loneliest number… Two can be as bad as one. The influence of AI Friendship Apps on users' well-being and addiction*, Psychology and Marketing (Sept. 18, 2023), https://onlinelibrary.wiley.com/doi/10.1002/mar.21899. Note that only a subset of AI chatbots are personalized for companionship.

303 Julian De Freitas, *AI Companions Reduce Loneliness*, The Wharton School of the University of Pennsylvania (July 26, 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4893097.

304 Jessica Lucas, *The teens making friends with AI chatbots*, The Verge (May 4, 2024), https://www.theverge.com/2024/5/4/24144763/ai-chatbot-friends-character-teens.; and Kevin Roose, *A Conversation With Bing's Chatbot Left Me Deeply Unsettled*, New York Times (Feb 16, 2023), https://www.nytimes.com/2023/02/16/technology/bing-chatbot-microsoft-chatgpt.html.

305 Janya Sundar, *Character.ai lawsuit sets up legal fight over companion chatbots after Florida teen's tragic suicide*, Fast Company (Oct. 24, 2024), https://www.fastcompany.com/91215310/character-ai-app-lawsuit-legal-complaint-teen-suicide-chatbot-google.

306 Lauren Walker, *Belgian man dies by suicide following exchanges with chatbot*, The Brussels Times (Mar. 28, 2023), https://www.brusselstimes.com/430098/belgian-man-commits-suicide-following-exchanges-with-chatgpt.; Imane El Atillah, *Man ends his life after an AI chatbot 'encouraged' him to sacrifice himself to stop climate change*, Euro News (Mar. 31, 2023), https://www.euronews.com/next/2023/03/31/man-ends-his-life-after-an-ai-chatbot-encouraged-him-to-sacrifice-himself-to-stop-climate-.

307 Rick Claypool, *Chatbots Are Not People: Designed-In Dangers of Human-Like A.I. Systems*, Public Citizen (Sept. 26, 2023), https://www.citizen.org/article/chatbots-are-not-people-dangerous-human-like-anthropomorphic-ai-report/.

308 Leonardo De Cosmo, *Google Engineer Claims AI Chatbot Is Sentient: Why That Matters*, Scientific American (July 12, 2022), https://www.scientificamerican.com/article/google-engineer-claims-ai-chatbot-is-sentient-why-that-matters/.; "The Cognitive Revolution" AI Builders, Researchers, and Live Player Analysis, *Mind Hacked by AI: A Cautionary Tale, From a LessWrong User's Confession*, Turpentine (Oct. 26, 2024), https://podcasts.apple.com/us/podcast/the-cognitive-revolution-ai-builders-researchers-and/id1669813431?i=1000674558110.

309 *Garcia v. Character Technologies, Inc.*, No. 6:24-cv-0193, 121 (Fla. Cir. Ct. Oct. 22, 2024). Source materials online at https://drive.google.com/file/d/1vHHNfHjexXDjQFPbGmxV5o1y2zPOW-sj/view.

310 U.S. Dept. of Health and Human Services, *Our Epidemic of Loneliness and Isolation* (2023), https://www.hhs.gov/sites/default/files/surgeon-general-social-connection-advisory.pdf.

311 Turkle, Sherry. *2011. Alone Together: Why We Expect More from Technology and Less from Each Other*. 1st edition. New York: Basic Books.

312 Ciriello, Raffaele F, Oliver Hannon, Angelina Ying Chen, and Emmanuelle Vaast. 2024. *'Ethical Tensions in Human-AI Companionship: A Dialectical Inquiry into Replika'.* In Proceedings of the 57th Hawaii International Conference on System Sciences.

313 Elizabeth Laird, Maddy Dwyer and Kristin Woelfel, *In Deep Trouble: Surfacing Tech-Powered Sexual Harassment in K-12 Schools*, Center for Democracy & Technology (Sept. 26, 2024), https://cdt.org/insights/report-in-deep-trouble-surfacing-tech-powered-sexual-harassment-in-k-12-schools/.

314 *E.g. What is My AI on Snapchat and how do I use it?*, Snapchat (2024), https://help.snapchat.com/hc/en-us/articles/13266788358932-What-is-My-AI-on-Snapchat-and-how-do-I-use-it. & *Start a chat with an AI on Messenger*, Facebook (2024), https://www.facebook.com/help/messenger-app/667776101667447.

315 *New law criminalizes creating sex-related deep fake activity*, Minnesota House of Representatives (2023), https://www.house.mn.gov/NewLaws/story/2023/5514.

316 USC Neely Center, *Neely Center Design Code for Social Media*, Google Docs, https://neely.usc.edu/design-code.

317 Kaitlyn Tiffany, *The Biggest Change to Instagram in Years*, The Atlantic (Sept. 17, 2024), https://www.theatlantic.com/technology/archive/2024/09/instagram-teen-safety-features/679904/.; Pinterest Engineering, *The Field Guide to Non-Engagement Signals*, Medium (Mar 26, 2024), https://medium.com/pinterest-engineering/the-field-guide-to-non-engagement-signals-a4dd9089a176.

318 Paul Bischoff, *MLB.tv Blackouts Workaround using a VPN: Tested For 2024*, (Mar. 29, 2019), https://www.comparitech.com/blog/vpn-privacy/mlb-tv-blackout-workaround-vpn/.

319 Federal Trade Commission, supra note 15, referring to "design tricks or psychological tactics . . . that get consumers to part with their money or data" and that "have the effect of obscuring, subverting, or impairing consumer autonomy and decision-making."

320 Nathaniel Lubin and Ravi Iyer, *How Tech Regulation Can Leverage Product Experimentation Results*, Lawfare (July 11, 2023), https://www.lawfaremedia.org/article/how-tech-regulation-can-leverage-product-experimentation-results.

321 The 2024 version of this report has been shared and discussed with regulators in the UK, Australia, and the EU, in advance of the development of their codes of practice for protecting minors.

322 Justin Hendrix, *Transcript: Senate Hearing on Social Media and Teen Mental Health with Former Facebook Engineer Arturo Bejar*, TechPolicy. Press (Nov. 8, 2023), https://www.techpolicy.press/transcript-senate-hearing-on-social-media-and-teen-mental-health-with-former-facebook-engineer-arturo-bejar/.

323 Federal Trade Commission, *Epic Games: Complaint for Permanent Injunction* (Dec. 19, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2223087EpicGamesComplaint.pdf.

324 Federal Trade Commission, *supra* note 15.

325 Brief for Design Scholars as Amici Curiae Supporting Appellants, *NetChoice, LLC v. Bonta* (Case No.: 23-2969, 9th Circ.) (Dec. 20, 2023), https://cdn.sanity.io/files/3tzzh18d/production/e1af7241bc4852390bfab82d7980a36640797c58.pdf.

326 *NetChoice, LLC v. Moody*, 34 F.4th 1196 (11th Cir. 2022).

327 Joey Garrison, *Facebook readying 'break-glass' tools to restrict content if violence erupts after election*, USA Today (Sept. 22, 2020), https://www.usatoday.com/story/news/politics/elections/2020/09/22/election-2020-facebook-has-break-glass-measures-if-violence-erupts/5866803002/.

328 Tech Justice Law Project, Knight-Georgetown Institute, and USC Neely Center, *Platform Design Taxonomy*, Google Docs, https://docs.google.com/spreadsheets/d/1GVO7sNuCNmNwqVK64PHQI7wxd8-Gmr9PqdkW12elmus/edit?gid=941162555#gid=941162555.

329 Google Scholar Search for "Revealed vs. Stated Preference", Google Scholar, https://scholar.google.com/scholar?q=revealed+vs+stated+preference&hl=en&as_sdt=0&as_vis=1&oi=scholart.

330 *FTC Halts Online Subscription Scheme that Deceived People with "Free Trial" Offers*, Federal Trade Commission (May 7, 2020), https://www.ftc.gov/news-events/news/press-releases/2020/05/ftc-halts-online-subscription-scheme-deceived-people-free-trial-offers.

331 Prinstein, *supra* note 17.

332 Rachel Kraus, *Teens know social media is manipulative, but they still use it more than ever*, Mashable (Sept. 10, 2018), https://mashable.com/article/common-sense-media-teenagers-social-media.

333 Jenny S. Radesky, Heidi M. Weeks, Alexandria Schaller, Michael B. Robb, Supreet Mann and Amanda Lenhart, *Constant Companion: A Week in the Life of a Young Person's Smartphone Use*, Common Sense Media (2023), https://www.commonsensemedia.org/sites/default/files/research/report/2023-cs-smartphone-research-report_final-for-web.pdf.

334 Radesky, *supra* note 102.

335 Susannah Luthi, *'Functionally useless': California privacy law's big reveal falls short*, POLITICO (Aug. 5, 2021), https://www.politico.com/states/california/story/2021/08/05/functionally-useless-california-privacy-laws-big-reveal-falls-short-1389429.

336 Mallory Newall and Johnny Sawyer, *A majority of Americans are concerned about the safety and privacy of their personal data*, Ipsos (May 5, 2022), https://www.ipsos.com/en-us/news-polls/majority-americans-are-concerned-about-safety-and-privacy-their-personal-data.

337 Brooke Auxier, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

338 *See: Defeated Virginia candidate whose explicit videos surfaced says she may not be done with politics*, Associated Press (Nov. 17, 2023), https://ny1.com/nyc/all-boroughs/ap-top-news/2023/11/17/defeated-virginia-candidate-whose-explicit-videos-surfaced-says-she-may-not-be-done-with-politics; Tom Felle, *Online abuse could drive women out of political life - the time to act is now*, The Conversation (Sept. 26, 2023), https://theconversation.com/online-abuse-could-drive-women-out-of-political-life-the-time-to-act-is-now-214301.

339 Jeff Horwitz and Katherine Blunt, *supra* note 81; *Canadian man sentenced to prison over AI-generated child pornography: report*, Fox News (Apr. 28, 2023), https://nypost.com/2023/04/28/canadian-man-steven-larouche-sentenced-to-prison-over-ai-generated-child-porn-report/.

340 Villius Petkauskas, *ChatGPT tied to Samsung's alleged data leak*, Cybernews (November 15, 2023), https://cybernews.com/news/chatgpt-samsung-data-leak/.

341 California's recent prohibitions on using personal data in engagement based algorithms were upheld. *See e.g. NetChoice, LLC v. Bonta*, No. 5:24-cv-07885-EJD (N.D. Cal. Dec. 31, 2024). Source materials online at https://reason.com/wp-content/uploads/2025/01/netchoice-v-bonta-order-preliminary-injunction.pdf.

342 Various, *supra* note 329.

343 *Better Recommender Systems - A How To Guide for Policymakers and Product Designers*, Knight-Georgetown Institute (2025).

344 Smitha Milli, Micah Carroll, Yike Wang, Sashrika Pandey, Sebastian Zhao, and Anca D. Dragan, *Engagement, User Satisfaction, and the Amplification of Divisive Content on Social Media* (Dec. 22, 2023), https://arxiv.org/abs/2305.16941

345 *See*: Loveday Morris, *In Poland's politics, a 'social civil war' brewed as Facebook rewarded online anger*, The Washington Post (Oct. 27, 2021), https://www.washingtonpost.com/world/2021/10/27/poland-facebook-algorithm/; Keach Hagey and Jeff Horwitz, *Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead*, The Wall Street Journal (Sep. 15, 2021), https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215.

346 Cloudflare, *What is rate limiting?*, Cloudflare.com (retrieved Jan 29, 2024), https://www.cloudflare.com/learning/bots/what-is-rate-limiting/.

347 Matthew Hindman, Nathaniel Lubin, and Trevor Davis *supra* note 33.

348 Steve Kovach, *History will not be on Facebook's side, no matter what Zuckerberg says*, (Oct. 18, 2019), https://www.cnbc.com/2019/10/18/mark-zuckerberg-georgetown-speech-history-isnt-on-facebooks-side.html.

349 Matthew Hindman, Nathaniel Lubin, and Trevor Davis *supra* note 33.

350 *See* Brett Frischmann and Susan Benesch, *Friction-in-Design Regulation as 21st Century Time, Place, and Manner Restriction*, 25 Yale J. L. & Tech. 376 (2023), https://yjolt.org/sites/default/files/frischmann_benesch.friction-in-design_regulation.376.pdf, for an extended discussion of time, place and manner restrictions.

351 Danielle Fallon-O'Leary, *Text Message Laws Every Business Needs to Follow*, Business.com (Jan. 15, 2025), https://www.business.com/articles/text-message-laws/.

352 Nathaniel Lubin and Ravi Iyer *supra* note 322.

353 SF 4907, Sec. 63, 93rd Legis. Sess. (Minn. 2023).

354 Massachusetts recently introduced the STUDY Act, which contains similar provisions. *See* HD 3070, 194th Legis. Sess. (Mass. 2024).

355 *Family Link from Google*, Google Family Safety & Parental Control Tools (Apr. 29, 2023), https://families.google/familylink/.

356 *Getting started with Microsoft Family Safety*, Microsoft Support, https://support.microsoft.com/en-us/account-billing/getting-started-with-microsoft-family-safety-b6280c9d-38d7-82ff-0e4f-a6cb7e659344.

357 *Manage Family Sharing Settings*, Apple Support, https://support.apple.com/guide/personal-safety/manage-family-sharing-settings-ips75b3b794f/web.

358 *See. e.g.*, Robert French, *Report of the Independent Legal Examination into Banning Children's Access to Social Media* (Sept. 2024), https://www.dpc.sa.gov.au/__data/assets/pdf_file/0006/1069809/34011b0649ad6732bd0538d435305b24e45f6ace.pdf.

359 Clare Y. Cho, *Identifying Minors Online*, Congressional Research Service (Jan. 2, 2024), https://crsreports.congress.gov/product/pdf/R/R47884/6.; Sam Schechner and Jeff Horwitz, *How Governments Are Trying to Keep Young Children Off Social Media*, From Face Scans to ID Checks, The Wall Street Journal (May 22, 2023), https://www.wsj.com/articles/as-preteens-ignore-social-media-age-limits-governments-push-for-better-checks-b21f5ae7.

360 *Online Nation: 2023 Report*, Ofcom (Nov. 28, 2023), https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/online-nation/2023/online-nation-2023-report.pdf?v=368355.

361 *Id.*

362 Nitish Pahwa, *Facebook Asked Users What Content Was "Good" or "Bad for the World." Some of the Results Were Shocking*, Slate (Nov. 15, 2021), https://slate.com/technology/2021/11/facebook-good-bad-for-the-world-gftw-bftw.html.

363 Nathanael Fast, Juliana Schroeder, Matt Motyl, and Ravi Iyer, *Unveiling the Neely Ethics & Technology Indices*, Designing Tomorrow (June 22, 2023), https://psychoftech.substack.com/p/unveiling-the-neely-ethics-and-technology.

364 Aisha Counts and Eari Nakano, *Twitter's Surge in Harmful Content a Barrier to Advertiser Return*, Bloomberg (July 19, 2023), https://www.bloomberg.com/news/articles/2023-07-19/twitter-s-surge-in-harmful-content-a-barrier-to-advertiser-return.

365 Jeff Horwitz, *His Job Was to Make Instagram Safe for Teens. His 14-Year-Old Showed Him What the App Was Really Like*, The Wall Street Journal (Nov 2, 2023), https://www.wsj.com/tech/instagram-facebook-teens-harassment-safety-5d991be1.

366 Hendrix *supra* note 322.

367 See Alessia Zornetta and Thomas Ash, *Shearing the Sheep Without Skinning It*, UCLA Institute for Technology Law & Policy (Oct. 2024), https://itlp.law.ucla.edu/wp-content/uploads/2024/10/UCLA_ITLP_Shearing_The_Sheep.pdf.

368 For example, the CDC's Youth Risk Behavior Survey allows for the identification of risks specific to female, LGBTQ+, and minority youth. *See* U.S. Centers for Disease Control and Prevention, *2023 Youth Risk Behavior Survey Results*, Youth Risk Behavior Surveillance System (Sept. 29, 2024), (https://www.cdc.gov/yrbs/results/2023-yrbs-results.html).

369 Elizabeth Laird, Maddy Dwyer and Kristin Woelfel, *In Deep Trouble: Surfacing Tech-Powered Sexual Harassment in K-12 Schools*, Center for Democracy & Technology (Sept. 26, 2024), https://cdt.org/insights/report-in-deep-trouble-surfacing-tech-powered-sexual-harassment-in-k-12-schools/.

370 *What Is the Network Effect?*, Wharton Online (Jan. 17, 2023), https://online.wharton.upenn.edu/blog/what-is-the-network-effect/.

371 Leonardo Bursztyn, Benjamin Handel, Rafael Jiménez-Durán, and Christopher Roth, *When Product Markets Become Collective Traps: The Case of Social Media*, Becker Friedman Institute (Oct 12, 2023), https://bfi.uchicago.edu/insight/research-summary/when-product-markets-become-collective-traps-the-case-of-social-media/.

372 S. 6686, N.Y. S. (2023).

373 *The Three-Legged Stool: A Manifesto for a Smaller, Denser Internet*, Initiative for Digital Public Infrastructure (Mar. 29, 2023), https://publicinfrastructure.org/2023/03/29/the-three-legged-stool/.

374 *Digital Spaces Directory*, New_ Public, https://newpublic.org/directory.

375 Sarah Perez, *As Bluesky soars, Threads rolls out custom feeds globally*, Tech Crunch (Nov. 20, 2024), https://techcrunch.com/2024/11/20/as-bluesky-soars-threads-rolls-out-custom-feeds-globally/.

376 Nirmita Panchal and Sasha Zitter, *A Look at State Efforts to Ban Cellphones in Schools and Implications for Youth Mental Health*, KFF (Sept. 5, 2024), https://www.kff.org/mental-health/issue-brief/a-look-at-state-efforts-to-ban-cellphones-in-schools-and-implications-for-youth-mental-health/.

377 Karen Fluegge, *NPS School Board discusses new cell phone legislation*, The Journal (Aug. 16, 2024), https://www.nujournal.com/news/local-news/2024/08/16/nps-school-board-discusses-new-cell-phone-legislation/#:~:text=NICOLLET%20%E2%80%94%20Minnesota%20Statute%20121A.,school%20by%20March%2015%2C%202025.

378 *The Cellphone Toolkit*, Minnesota School Boards Association (July 2024), https://mnmsba.org/wp-content/uploads/2024/07/CellPhoneToolkit.pdf.

379 Luc Rinaldi, *Schools vs. Screens*, Maclean's (Nov. 12, 2024), https://macleans.ca/society/schools-vs-screens/.

380 Tim Walker, *Take Cellphones Out of the Classroom, Educators Say*, NEA Today (Oct. 3, 2024), https://www.nea.org/nea-today/all-news-articles/take-cellphones-out-classroom-educators-say#:~:text=A%202024%20National%20Education%20Association,to%20the%20entire%20school%20day.

381 *Becca Schmill Foundation and Phone-Free Schools Movement Phone and Social Media Free Schools Model Legislation*, Google Docs, https://docs.google.com/document/d/1NQ5vuWxTtKewNFQ7LDGfm8t6mrn08Jw0dNOEQ3e_Nbc/edit?tab=t.0.

382 AJ Skiera, *What Gen Z thinks about its social media and smartphone usage*, The Harris Poll (Sept. 10, 2024), https://theharrispoll.com/briefs/gen-z-social-media-smart-phones/.

383 *See, e.g.*, https://www.anxiousgeneration.com/resources#educator.

384 *See* Elizabeth Laird, Maddy Dwyer and Kristin Woelfel, *In Deep Trouble: Surfacing Tech-Powered Sexual Harassment in K-12 Schools*, Center for Democracy & Technology (Sept. 26, 2024), https://cdt.org/wp-content/uploads/2024/09/2024-09-26-final-Civic-Tech-Fall-Polling-research-1.pdf.; *Resource Library,* The Anxious Generation (last visited Jan. 21, 2024), *What is My AI on Snapchat and how do I use it?*, Snapchat (2024), https://help.snapchat.com/hc/en-us/articles/13266788358932-What-is-My-AI-on-Snapchat-and-how-do-I-use-it.

385 Kevin Roose, *Can A.I. Be Blamed for a Teen's Suicide?*, The New York Times (Oct. 24, 2024), https://www.nytimes.com/2024/10/23/technology/characterai-lawsuit-teen-suicide.html.

386 Stuart D. Levi *et al*., *Tennessee Law Addresses Proliferation of Deepfakes*, Skadden (April 2, 2024), https://www.skadden.com/insights/publications/2024/04/tennessee-law-addresses-proliferation-of-deepfakes.

387 University of Minnesota, 2024 College Student Health Survey Report, *supra* note 10.

388 HF 4400, 93rd Legis. Sess. (Minn. 2023).

389 SF 4907, Sec. 63, 93rd Legis. Sess. (Minn. 2023).

390 *See* Appendix A - Model Bill: Prohibiting Deceptive Patterns.

391 *See* Appendix B: Model Bill - Device Based Age Settings.

392 Bob Mercer, *Meta: South Dakota should have app stores check ages*, Keloland (Oct. 2, 2024), https://www.keloland.com/news/capitol-news-bureau/meta-south-dakota-should-have-app-stores-check-ages/.

393 *See* Appendix C: Model Bill - Preventing Identity Appropriation Act.

394 *See* Appendix D: Model Bill - State Version of ACCESS ACT.

395 Adi Robertson, *How would opening up Facebook change the internet?*, The Verge (Oct. 23, 2019), https://www.theverge.com/2019/10/23/20926792/facebook-access-act-interoperability-data-portability-warner-hawley-bill-explainer.

396 *See* Appendix E: Model Bill - Digital Advertising Tax for Public Health Monitoring.

397 Alessia Zornetta and Thomas Ash, *Shearing the Sheep Without Skinning It*, UCLA Institute for Technology Law & Policy (Oct. 2024), https://itlp.law.ucla.edu/wp-content/uploads/2024/10/UCLA_ITLP_Shearing_The_Sheep.pdf.

398 *Arizona et al. v. Meta Platforms, Inc., et al.*, Case No. 4:23-cv-05448, Complaint (N.D. Cal. Oct. 24, 2023). Source materials online at https://storage.courtlistener.com/recap/gov.uscourts.nmd.496039/gov.uscourts.nmd.496039.36.2.pdf.

399 *See* Appendix F: Model Legislation to Promote Safe, Effective, and Distraction Free Education for PreK-12 Students.

Appendix A – Model Bill: Prohibiting Deceptive Patterns.

Background and Goal:

Legislators across the world want to improve the impact of social media on their citizens - especially children and other vulnerable users - as well as on society as a whole without infringing on free expression. Design based legislation can achieve this goal in a content agnostic fashion that is compatible with free expression principles. The below model law draws from effective legislative design regulation ideas across jurisdictions and can be customized depending on the concerns and needs of any particular jurisdiction.

Section 1. Introduction

A bill for an act relating to consumer protection; regulating online platforms.

This chapter may be cited as the “Online Consumer Protection Act of [LOCATION]”

Section 2. Definitions

For purposes of this chapter, the following terms have the meanings given.

"Accessible user interface" means a way for a user to input data, make a choice, or take an action on a covered platform in two clicks or less.

"Connected account" means an account on the covered platform service that is directly connected to:

(a) the account holder's account; or
(b) an account that is directly connected to the account holder's account.

“Covered platform” means a public or semipublic internet-based service or application that has users in [LOCATION] and that meets both of the following criteria:

(a) A substantial function of the service or application is to connect users in order to allow users to interact with each other within the service or application.
(b) The service or application allows users to do all of the following:
    i. construct a profile for purposes of signing into and using the service or application;
    ii. populate a list of other users with whom an individual shares a connection within the system; and
    iii. create or post content accessible primarily to other users through an algorithmically prioritized set of content.

"Device operating system provider" means a business that manages or develops operating system software for mobile or desktop devices, including but not limited to personal computers, smartphones, and tablets, which manage device resources and are loaded by a boot program.

"Existing extended network" means a user's existing network plus the set of account holders on a covered media platform who are all directly connected to the account holders within that user's existing network.

"Existing network" means the set of account holders on a covered media platform with whom a user has consented to have a direct connection.

“Monthly Active Users” means the number of unique individuals who engage with a covered media platform within a typical 30 day period.

"Personal data" means information that is persistently associated with the user or user's device or that concerns the user's previous interactions with media generated or shared by other users.

"Protected user" means any user who has indicated a desire for heightened protections, whether at the device or application level, or whom the service knows is under the age of 18 or has reduced decision making capacity [Optional: without that user having explicitly opted out of protected user status].

Section 3. Scope; Exclusions.

An entity is subject to this chapter if:

- It operates a covered platform.
- It does business in [LOCATION] or provides products or services that are targeted to [LOCATION].
- It has more than [XXX] monthly active users of an operated covered platform in [LOCATION].
    - For the purposes of this chapter, the location of active users may be based on:
        - the account holder's own supplied address or location;
        - global positioning system-level latitude, longitude, or altitude coordinates;
        - cellular phone system coordinates;
        - Internet protocol device address; or
        - other mechanisms that can be used to identify an account holder's location.

Section 4. Requirements for Covered Platforms.

[General Requirement following Deceptive Patterns]

Regardless of protected user status, it shall be unlawful for any covered platform to employ a user interface of a covered platform with the purpose or substantial effect of subverting or impairing user autonomy, decision-making, or choice. This shall include any pattern, practice, or feature that the [US Federal Trade Commission or Other Regulatory Body] categorizes as deceptive or unfair.

[Product Experimentation Transparency]

A covered platform must publicly and conspicuously post the following information on the platform's website:

A description of all product experiments that have been conducted on 1,000 or more users, including a description of the experimental conditions and the results of the product experiment for all experimental conditions on any outcome that could relate to a negative user experience. This includes any outcome related to:

(i) user surveys about their experience
(ii) user preference or use of platform functionality related to user preference including reporting and hiding
(iii) violations of platform policies
(iv) increased user engagement, including increases amongst heavy users and during nighttime hours

Platforms must conform to industry best practices in the collection of data related to the above outcomes and must take reasonable measures to evaluate all experiments along these dimensions. Any disclosure of proprietary trade secrets that are not already known may be redacted from these disclosures.

[Requirement for Opting into Protected User status at Device and App Level]

A covered platform must provide an accessible user interface to allow a user to opt in to being considered a "protected user" for the purposes of this law.

- A covered platform may make "protected user" settings the default settings for all users or all account holders.
- By default, any user who indicates that they are under 18 or for whom the platform has knowledge of them being under 18 shall be considered a "protected user". For purposes of this Act, knowledge includes all information and inferences known to a covered platform relating to the age of a user. In the absence of identity verification, which is not required under this Act, what is "known" to a covered platform includes any information or data relating to, estimating, signaling, or otherwise suggesting the age of a user where the covered platform has received, collected, created, or benefited from such information or data in connection with marketing, product development, or any other business-related purpose. Further, such knowledge shall be imputed to the covered platform when it is used by any other entity acting on behalf or for the benefit of the covered platform.

A device operating system provider must provide an option for a device owner to automatically opt in to being considered a "protected user" across all covered platforms managed by the operating system on the user's device.

- If a device owner selects the option under this paragraph, the device operating system provider must inform all platforms managed by the provider's operating system of the device owner's preferences and/or voluntarily provided age.
- A device operating system provider must, by default, consider any device with parental controls enabled to have opted in to "protected user" status.
- A device operating system provider may provide a device owner with the ability to opt out of "protected user" status.
- A device operating system provider must include the option for a device owner to set the age or age range of the device user that will then be shared with any platform requesting this information. Any device that is indicated to be used by a minor shall be considered as having opted into "protected user" status.

[Limit harm from unconnected accounts/strangers]

[General] A covered platform must take reasonable care to ensure that protected users default settings prioritize maximum privacy, including, but not limited to the below settings. Maximum privacy includes limits on the use of protected user data to what is necessary to provide the core functioning of the requested service, limits on unsolicited contact, and limits on unwanted viewing of the protected users' information and content.

[Specific] A covered platform must provide default settings for a protected user that:

- restrict messaging, requests, reactions, comments, or other contact from account holders that are not already within the user's existing connected accounts;
- restrict the visibility of a user's account to only connected accounts;
- limit the visibility of a user's content to only connected accounts;
- restrict any data collection and sale of data from a user's account that is not required for core functioning of the covered platform's service;
- disable search engine indexing of a minor's account profile such that the account does not show within searches outside of connected accounts;
- restrict visibility of a minor's location to other users, unless the user specifically shares the user's location;
- restrict visibility of a minor's personal data or content outside of connected accounts, whether registered or not;
- restrict visibility of a minor's connections to any account, regardless of connection;

The default settings required in this section may be changed only to comply with the user's expressed preferences. A covered platform must not utilize a system, user interface, or prompt that encourages a user to change the user's privacy settings toward allowing the user's information or user-generated content to be shared or disseminated more broadly.

[Alternatives to engagement based algorithms]

[General + Transparency] A covered platform must provide a detailed description of their algorithmic ranking system(s) including how the platform measures and operationalizes expressed preferences within its systems as well as any other factors being used. A covered platform must provide details as to how these measures and predictions are used and weighted relative to each other within their systems. Protected users must not have their personal data used within recommendation systems primarily to extend their usage of the platform.

[Specific] A covered platform must provide default settings for protected users that:

- Provides an accessible user interface for a user to indicate their explicit expressed preferences, both positive and negative, for any piece and/or class of media or recommendations.

A covered platform may not use personal data that are not related to explicit expressed preference to prioritize media. This includes, but is not limited to any personalized prediction of what media will lead to greater time spent, more likelihood to comment, greater view time, more likelihood of completely watching a video, more likelihood to click, or any other measure of platform usage that does not indicate explicit preference.

[Remove design patterns that increase problematic/harmful/excessive usage]

[General] A covered platform shall not use a practice, design, or feature that the company knows, or which by the exercise of reasonable care should know, causes a substantial number of users to feel manipulated by the platform in ways that interfere with users' goals, as measured by third party external surveys of user experiences.

[Specific] A covered platform shall not implement the following practices, functional designs, and features for any protected user:

1. Infinite scroll or any practice, design, or feature that automatically loads and displays anything other than what the user has prompted to display, when a user has not been required to click a button or navigate to a new page or perform any other action that is not scrolling.

2. Auto-playing videos or any practice, design, or feature in which videos automatically begin playing when a user navigates to or scrolls through a set of content.

3. Optimization of the order of presentation of content for time spent or any other usage of the platform including more likelihood to comment, greater view time, more likelihood of completely watching a video, more likelihood to click, or any other measure of platform usage that does not indicate explicit preference.

4. Gamification or any practice, design, or feature that stimulates or emulates elements of gameplay to engage and motivate a user, which includes features such as streaks, badges, or rewards, for either frequent logins or other activities, as well as the use of animated graphics or sound effects to provide positive reinforcement for user engagement on the covered platform, regardless of whether the rewards have any monetary value.

5. Virtual gifts or any practice, design, or feature in which digital items or tokens are purchased with virtual currency or other forms of payment and can be sent by a user to another user on a covered platform as a form of expression. Such digital items may include images, animations, or other graphical representations that are intended to simulate a physical gift but do not have any inherent monetary or tangible value.

6. Quantification of engagement including, but not limited to, providing any visible count of how many likes, comments, shares, clicks, views, or reactions any piece of content has received.

[Data minimization]

A covered platform may not process the personal data of a protected user unless it is strictly necessary in providing an online service, product, or feature requested by a protected user with which a protected user is actively and knowingly engaged.

[Rate Limits Transparency]

A covered platform must publicly and conspicuously post the following information on the platform's website:

(1) an explanation of whether and how the platform limits excessive account interactions, including:
   (i) the maximum limit on the number of times that a user can engage in each specific kind of account interaction in an hour, day, week, and month; and
   (ii) whether and how the platform engages in the reduction in the ability of accounts to affect other users when the user engages in a high number of account interactions that is below the maximum limit; Additional steps beyond these publicly disclosed limits to prevent abusive usage are encouraged and do not need to be disclosed.

(2) statistics on the platform's use with respect to the tenth, 25th, 50th, 75th, 90th, 95th, 99th, and 99.9th percentile of all platform account holders for each distinct type of account interaction or engagement, including but not limited to:
   (i) sending invitations or messages to other platform account holders;
   (ii) commenting on, resharing, liking, voting for, or otherwise reacting to content;
   (iii) posting new user-generated content;
   (iv) disseminating user-generated content to other platform account holders;
   (v) time spent on the platform;

[Follower Demographic transparency]

(3) statistics on the public follower counts of publicly visible accounts including:
   (i) the number of publicly visible accounts
   (ii) the number of publicly visible accounts for groups of publicly visible account holders, based on age range and gender
   (iii) the average number of followers for publicly visible accounts for groups of publicly visible account holders, based on age range and gender
   (iv) the average percentage of followers for each follower age range and follower gender, for groups of publicly visible account holders, based on age range and gender
   (v) the distribution with respect to the tenth, 25th, 50th, 75th, 90th, 95th, 99th, and 99.9th percentiles of publicly visible account followers in (iv) - based on the demographics of followers. Based on these statistics it should be made possible to know what the median demographic distribution is for followers of teenage female accounts, for each follower demographic - as well as for the top 10% of teenage female accounts, as identified by each follower demographic.

[Limit Notifications]

A covered platform shall, by default, restrict notifications sent to protected users to those that are initiated by a connected account that unambiguously intends to communicate directly with the protected user.

A covered platform must publicly and conspicuously post the following information on the covered platform's website:

(1) an explanation of how the platform determines whether a notification is time sensitive and how many time-sensitive and non-time-sensitive notifications are sent to users including:
   (i) how many time-sensitive and non-time-sensitive notifications are sent with respect to the tenth, 25th, 50th, 75th, 90th, 95th, 99th, and 99.9th percentile of all platform account holders in a given day; and
   (ii) how many time-sensitive and non-time-sensitive notifications are sent with respect to the tenth, 25th, 50th, 75th, 90th, 95th, 99th, and 99.9th percentile of all platform account holders during each hour between the hours of 11:00 p.m. and 7:00 a.m.;

Section 5. Enforcement.

[Will require jurisdiction-specific modification]

Section 6. Legal Clauses

[Severability] If any provision of this chapter or the chapter's application to any person or circumstance is held invalid for any reason in a court of competent jurisdiction, the remainder of the chapter or the application of the provision to other persons or circumstances is not affected.

[Nothing interferes with affirmative searches]

Nothing in this bill shall be construed to require a covered platform to prevent or preclude any protected user from deliberately and independently searching for, or specifically requesting, content;

Section 7. Effective Date.

This act is effective XXX.

Appendix B – Model Bill: Device Based Age Settings

Background and Goal:

This bill modifies legislation that has been introduced in several jurisdictions to give families the ability to opt-in to age-based protections robustly. Notably, it does not absolve companies of responsibilities to determine age by other means. It does not ask operating system providers to verify age or aid platforms in getting parental consent. It also allows for older users (e.g. the elderly or those with special needs) to opt into protections. This bill is designed to remove some of the uncertainty around age verification from efforts to protect kids in other legislation.

Section 1. Definitions.

For the purposes of this title:

“Accessible Interface” means a user interface that is part of the standard setup process of a new device and also accessible within 2 clicks from the main settings menu of a device.

“Application” means a software application or electronic service that may be run or directed by a user on a computer, a mobile device, or any other general purpose computing device.

“Child” or “children,” unless otherwise specified, means a consumer or consumers who are under 18 years of age.

“Developer” means any person, entity or organization that creates, owns, or controls an application that could be accessed by children and is responsible for the design, development, maintenance, and distribution of the application to end users via a device operating system.

"Device operating system provider" means a business that manages or develops operating system software for mobile or desktop devices, including but not limited to personal computers, smartphones, and tablets, which manage device resources and are loaded by a boot program.

“Online service, product, or feature” does not mean any of the following:

(a) A broadband internet access service, as defined in Section 3100.
(b) A telecommunications service, as defined in Section 153 of Title 47 of the United States Code.
(c) The delivery or use of a physical product.

“Signal” means data sent by real-time secure application programming interface (API) accessible to any application that has been validated and has appropriate credentials.

Section 2.

(a) A covered device operating system provider that provides access to applications that could be accessed by children shall take all of the following actions:
  (1) Provide an accessible interface for device owners to indicate the birth date, age range, or age of the user of that device for the explicit purpose of sharing that information with other applications.
  (2) Provide an accessible interface for device owners to indicate that they would like heightened protections from design patterns or features intended to extend device usage for the explicit purpose of sharing such device owner’s indication with other applications. This setting shall be explicitly offered as an option for cases where a device owner does not choose to share their age or is above the age of 18, but does want to receive heightened protections against design patterns or features intended to extend device usage.
  (3) Set as default the setting under Sec 2.a.2 to indicate a desire for heightened protections for any device that

is (a) under parental/family control or (b) that the application provider has a clear signal that the device owner is at substantially higher risk.

(4) Provide developers whose applications or websites accessed via the device operating system a signal on an ongoing basis regarding, the following:

(i) What the device user's explicit age or age range is, as indicated by the interface in section 2.

(ii) Whether the device owner would like heightened design protections, as indicated by the interface in section 2 a.2.

(b) Developers shall use age and heightened protection signals provided under subsection(a) to comply with applicable laws. The use of this signal shall not limit other requirements of application developers with regards to minors who they have knowledge of through other means. For purposes of this Act, "knowledge" includes all information and inferences known to a covered platform relating to the age of a user. In the absence of identity verification, which is not required under this Act, what is "known" to a covered platform includes any information or data relating to, estimating, signaling, or otherwise suggesting the age of a user where the covered platform has received, collected, created, or benefited from such information or data in connection with marketing, product development, or any other business-related purpose. Further, such knowledge shall be imputed to the covered platform when it is used by any other entity acting on behalf or for the benefit of the covered platform.

Section 3.

(a) Nothing in this Act, or any amendment made by this Act, shall be construed to modify, impair, or supersede the operation of any antitrust laws, unless otherwise specified.

(b) Nothing in this Act, or any amendment made by this Act, shall be construed as requiring the collection of more data from device owners or device users, other than the explicit voluntary settings described in section 2.

(c) A covered device operating system provider shall comply with this Act in a nondiscriminatory manner, including, but not limited to:

(1) A covered device operating system provider shall impose at least the same restrictions and obligations on its own applications and application distribution as it does on those from third party applications or application distributors.

(2) A covered device operating system provider shall not use data collected from third parties, or consent mechanisms deployed for third parties, in the course of compliance with this Act to compete against those third parties, give the covered device operating system provider's services preference relative to those of third parties, or to otherwise use this data or consent mechanism in an anticompetitive manner.

(d) The protections provided by this chapter are in addition to those provided by any other applicable law.

Section. 4.

(a) The attorney general may enforce this action under [state Attorney General enforcement statute], and may seek the following additional relief against any person that violates this title: (1) an injunction against future violations, (2) restitution for harmed individuals, and (3) either: (i) a penalty of up to two thousand five hundred dollars ($2,500) per affected child for each negligent violation, or (ii) up to seven thousand five hundred dollars ($7,500) per affected child for each intentional violation.

(b) Nothing in this title shall be interpreted to serve as the basis for a private right of action under this title or any other law.

Appendix C – Model Bill: Preventing Identity Appropriation Act

Section 1. Definitions.

As used in this part, unless the context otherwise requires:

(1) "Definable group" means an assemblage of individuals existing or brought together with or without interrelation, orderly form, or arrangement, including, but not limited to, a crowd at any sporting event, a crowd in any street or public building, the audience at any theatrical or stage production, a glee club, or a baseball team;

(2) "Appropriation" includes any unauthorized use of another's indicia of identity for the user's own benefit, commercially or otherwise. Appropriation includes commercial use, use to defame an individual, use to mislead or deceive another in the course of business, vocation, or occupation, and sexual use. Commercial use may include use of another's indicia of identity within the user's goods, products, or services, within marketing, advertising, or solicitation, within attempts to gain monetizable social media distribution or followers, or in connection with services rendered by the user. Commercial use does not ordinarily include the use of another's indicia of identity in news reporting, commentary, entertainment, works of fiction or nonfiction, or in advertising that is incidental to such uses. Sexual use may include any use depicting sexual acts or that is obscene, regardless of nudity or veracity.

(3) "Individual" means human being, living or dead;

(4) "Indicia of identity" includes an individual's image, likeness, voice, signature, or other uniquely identifying features, including one's face, mannerisms, distinctive appearance, tattoos, visible body modifications, birthmarks, and distinctive speech patterns, including speech and language disorders. For the purposes of this act, the use of an individual's name, without any other representation of the person, is not considered an Indicia of identity. The use of an individual's name in any technological product that represents itself as having a likeness to the individual would be considered an Indicia of identity.

(5) "Person" means any individual, firm, association, partnership, corporation, joint stock company, syndicate, receiver, common law trust, conservator, statutory trust, or any other concern by whatever name known or however organized, formed, or created, and includes not-for-profit corporations, associations, educational and religious institutions, political parties, community, civic, or other organizations; and

(6) "Photograph" or "likeness" means any photograph, photographic reproduction, digital image, or artifact, still or moving, or any film, videotape, digital recording, or other similar medium, of any individual, so that the individual is readily identifiable; and

(7) "Public Figure" means any individual who has achieved fame or notoriety and is known to many people outside of their personal and professional connections. It includes anyone who has run for government office, holds a position of prominence in society, or has inserted themselves voluntarily into a public debate to influence its outcome.

(8) "Voice" means a sound in a medium that is readily identifiable and attributable to a particular individual, regardless of whether the sound contains the actual voice or a simulation of the voice of the individual.

Section 2. Protection from Appropriation.

(a) Every individual has a right to protection from appropriation of that person's indica of identity in any medium in any manner.

(b) (1) Any person who knowingly appropriates an individual's indicia of identity in any medium, in any manner directed to any person other than such individual, without such individual's prior consent, or, in the case of a minor, the prior consent of such minor's parent or legal guardian, or in the case of a deceased individual, the consent of the executor or administrator, heirs, or devisees of such deceased individual, shall be liable to a civil action.

(2) A person is liable to a civil action if the person knowingly publishes, performs, distributes, transmits, or otherwise makes available to the public an individual's indicia of identity, without such individual's prior consent, or, in the case of a minor, the prior consent of such minor's parent or legal guardian, or in the case of a deceased individual, the consent of the executor or administrator, heirs, or devisees of such deceased individual, shall be liable to a civil action.

(3) A person is liable to a civil action if the person distributes, transmits, or otherwise makes available an algorithm, software, tool, or other technology, service, or device, the primary purpose or function of which is the production of an individual's indicia of identity in any medium without consent from the individual or, in the case of a minor, the minor's parent or legal guardian, or in the case of a deceased individual, the executor or administrator, heirs, or devisees of such deceased individual.

(c) In addition to the civil action authorized by this section and the remedies set out in this Act, any person who commits unauthorized sexual use as defined in this Act commits a Class A misdemeanor.

(d) It is no defense to the unauthorized use defined in subsection (a) that the photograph or likeness includes more than one (1) individual so identifiable; provided, that the individual or individuals affected by the appropriation shall be represented as individuals per se rather than solely as members of a definable group represented in the photograph or likeness.

(e) If an unauthorized use as defined in subsection (a) is by means of products, merchandise, goods or other tangible personal property, all such property, including all instrumentalities used in connection with the unauthorized use by the person violating this section, is declared contraband and subject to seizure by, and forfeiture to, the state in the same manner as is provided by law for the seizure and forfeiture of other contraband items.

Section 3. Assignment of Rights.

(a) The protections provided for in this part shall be deemed exclusive to the individual, subject to the assignment or licensing of such rights as provided in this Act, during such individual's lifetime and to the executors, heirs, assigns, or devisees even after the death of the individual.

(b) (1) Use of the property right by any executor, assignee, heir, or devisee if the individual is deceased shall maintain the right as the exclusive property of the executor, assignee, heir, or devisee until such right is terminated as provided in this subsection (b).

(2) (A) For Public Figures, the exclusive right to non-sexual use of the property rights is terminated by proof of the non-use of the name, likeness, voice or image of any individual for commercial purposes by an executor, assignee, heir, or devisee to such use for a period of two (2) years subsequent to the initial ten (10) year period following the individual's death. For individuals who are not Public Figures, the exclusive right to non-sexual use is only terminated by the assignment or licensing of rights.

(3) The sexual use of the property rights is only terminated by the assignment or licensing of rights by the individual. Once the individual is deceased, such rights cannot be terminated and anyone sexually using their likeness is subject to a civil claim on behalf of any heir of that individual.

(c) For purposes of subdivision (b)(2)(A), "use" includes the public availability of a sound recording or audiovisual work in which the individual's photograph, voice, or likeness is readily identifiable.

Section 4. Remedies.

(a) The court having jurisdiction for any action arising pursuant to this part may grant injunctions on such terms as it may deem reasonable to prevent or restrain the unauthorized use of an individual's indica of identity. As part of such injunction, the court may authorize the confiscation of all unauthorized items and seize all instrumentalities used in connection with the violation of the individual's rights. All instrumentalities seized pursuant to enforcing an injunction under this subsection (a) shall be liquidated and used to satisfy statutory damages, if damages are recovered by the rights holder.

(b) At any time while an action under this part is pending, the court may order the impounding, on such terms as it may deem reasonable, of all materials or any part thereof claimed to have been made or used in violation of the individual's rights, and such court may enjoin the use of all plates, molds, matrices, masters, tapes, film negatives, or other articles by means of which such materials may be reproduced.

(c) As part of a final judgment or decree, the court may order the destruction or other reasonable disposition of all materials found to have been made or used in violation of the individual's rights, and of all plates, molds, matrices, masters, tapes, film negatives, or other articles by means of which such materials may be reproduced.

(d) An individual is entitled to recover whichever is greater of one thousand dollars or the actual damages suffered as a result of the knowing appropriation of indicia of identity and any profits that are attributable to such appropriation which are not taken into account in computing the actual damages. Profit or lack thereof by the unauthorized use or infringement of an individual's rights shall not be a criteria of determining liability.

(e) The remedies provided for in this section are cumulative and shall be in addition to any others provided for by law.

Section 5. Exemptions.

(a) It is deemed a fair use and no violation of an individual's rights shall be found, for purposes of this part, if the use of an individual’s indicia of identity without consent is in connection with any news, public affairs, or sports broadcast or account, to the extent protected by the First Amendment to the United States Constitution.

(b) The use of an indicia of identity in a commercial medium does not automatically constitute unlawful appropriation solely because the material containing such use is commercially sponsored or contains paid advertising. Rather it shall be a question of fact whether or not the use of the complainant individual's indicia of identity was so directly connected with the commercial sponsorship or with the paid advertising as to constitute a use for purposes of advertising or solicitation.

(c) Nothing in this section applies to the owners or employees of any medium used for advertising, including, but not limited to, newspapers, magazines, radio and television stations, billboards, and transit ads, who have published or disseminated any advertisement or solicitation in violation of this part, unless it is established that such owners or employees had knowledge or reasonably should have known of the unauthorized use of the individual's indica of identity as prohibited by this section.

Appendix D – Model Bill: State Version of ACCESS Act

To promote competition and reduce consumer switching costs in the provision of online communications services.

Section 1 – Short Title.

This Act may be cited as the ‘‘Augmenting Compatibility and Competition by Enabling Service Switching Act of [YEAR]”

Section 2 – Definitions.

In this Act:

(1) Attorney General.—The term ‘‘Attorney General’’ means the Attorney General for the state of [STATE].

(2) COMMUNICATIONS PROVIDER.—The term ‘‘communications provider’’ means a consumer-facing communications and information services provider.

(3) COMPETING COMMUNICATIONS PROVIDER.— The term ‘‘competing communications provider’’, with respect to a large communications platform provider, means another communications provider offering, or planning to offer, similar products or services to consumers.

(4) COMPETING COMMUNICATIONS SERVICE.— The term ‘‘competing communications service’’, with respect to a large communications platform, means a similar product or service provided by a competing communications provider.

(5) CUSTODIAL THIRD-PARTY AGENT.—The term ‘‘custodial third-party agent’’ means an entity that is duly authorized by a user to interact with a large communications platform provider on that user’s behalf to manage the user’s online interactions, content, and account settings.

(6) INTEROPERABILITY INTERFACE.—The term ‘‘interoperability interface’’ means an electronic interface maintained by a large communications platform for purposes of achieving interoperability.

(7) LARGE COMMUNICATIONS PLATFORM.—The term ‘‘large communications platform’’ means a product or service provided by a communications provider that—
   (A) generates income, directly or indirectly, from the collection, processing, sale, or sharing of user data; and
   (B) has more than [xxx] monthly active users in [STATE].

(8) LARGE COMMUNICATIONS PLATFORM PROVIDER.—The term ‘‘large communications platform provider’’ means a communications provider that provides, manages, or controls a large communications platform.

(9) USER DATA.—
   (A) IN GENERAL.—The term ‘‘user data’’ means information that is—
      (i) collected directly by a communications provider; and
      (ii) linked, or reasonably linkable, to a specific person.
   (B) EXCLUSION.—The term ‘‘user data’’ does not include information that is rendered unusable, unreadable, de-identified, or anonymized.

Section 3. Portability.

(a) GENERAL DUTY OF LARGE COMMUNICATIONS PLATFORM PROVIDERS.—A large communications platform provider shall, for each large communications platform it operates, maintain a set of transparent, third party-accessible interfaces (including application programming interfaces) to initiate the secure transfer of user data

to a user, or to a competing communications provider acting at the direction of a user, in a structured, commonly used, and machine-readable format.

(b) GENERAL DUTY OF COMPETING COMMUNICATIONS PROVIDERS.—A competing communications provider that receives ported user data from a large communications platform provider shall reasonably secure any user data it acquires.

(c) EXEMPTION FOR CERTAIN SERVICES.—The obligations under this section shall not apply to a product or service by which a large communications platform provider does not generate any income or other compensation, directly or indirectly, from collecting, using, or sharing user data.

Section 4. Interoperability.

(a) GENERAL DUTY OF LARGE COMMUNICATIONS PLATFORM PROVIDERS.—A large communications platform provider shall, for each large communications platform it operates, maintain a set of transparent, third-party-accessible interfaces (including application programming interfaces) to facilitate and maintain technically compatible, interoperable communications with a user of a competing communications provider.

(b) GENERAL DUTY OF COMPETING COMMUNICATIONS PROVIDERS.—A competing communications provider that accesses an interoperability interface of a large communications platform provider shall reasonably secure any user data it acquires, processes, or transmits.

(c) INTEROPERABILITY OBLIGATIONS FOR LARGE COMMUNICATIONS PLATFORM PROVIDERS.—

(1) IN GENERAL.—In order to achieve interoperability under subsection (a), a large communications platform provider shall fulfill the duties under paragraphs (2) through (6) of this subsection.

(2) NON-DISCRIMINATION.—

(A) IN GENERAL.—A large communications platform provider shall facilitate and maintain interoperability with competing communications services for each of its large communications platforms through an interoperability interface, based on fair, reasonable, and nondiscriminatory terms.

(B) REASONABLE THRESHOLDS, ACCESS STANDARDS, AND FEES.—

(i) IN GENERAL.—A large communications platform provider may establish reasonable thresholds related to the frequency, nature, and volume of requests by a competing communications provider to access resources maintained by the large communications platform provider, beyond which the large communications platform provider may assess a reasonable fee for such access.

(ii) USAGE EXPECTATIONS.—A large communications platform provider may establish fair, reasonable, and nondiscriminatory usage expectations to govern access by competing communications providers, including fees or penalties for providers that exceed those usage expectations.

(iii) LIMITATION ON FEES AND USAGE EXPECTATIONS.—Any fees, penalties, or usage expectations assessed under clauses (i) and (ii) shall be reasonably proportional to the cost, complexity, and risk to the large communications platform provider of providing such access.

(iv) NOTICE.—A large communications platform provider shall provide public notice of any fees, penalties, or usage expectations that may be established under clauses (i) and (ii), including reasonable advance notice of any changes.

(v) SECURITY AND PRIVACY STANDARDS.—A large communications platform provider shall, consistent with industry best practices, set privacy and security standards for access by competing communications services to the extent reasonably necessary to address a threat to the large communications platform or user data, and shall report any suspected violations of those standards to the Attorney General.

(C) PROHIBITED CHANGES TO INTERFACES.—A change to an interoperability interface or terms of use made with the purpose, or substantial effect, of unreasonably denying access or undermining interoperability for competing communications services shall be considered a violation of the duty under subparagraph (A) to facilitate and maintain interoperability based on fair, reasonable, and nondiscriminatory terms.

(3) FUNCTIONAL EQUIVALENCE.—A large communications platform provider that maintains interoperability between its own large communications platform and other products, services, or affiliated offerings of such provider shall offer a functionally equivalent version of that interface to competing communications services.

(4) INTERFACE INFORMATION.—

(A) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, a large communications platform provider shall disclose to competing communications providers complete and accurate documentation describing access to the interoperability interface required under this section.

(B) CONTENTS.—The documentation required under subparagraph (A) (i) is limited to interface documentation necessary to achieve development and operation of interoperable products and services; and (ii) does not require the disclosure of the source code of a large communications platform.

(5) NOTICE OF CHANGES.—A large communications platform provider shall provide reasonable advance notice to a competing communications provider, which may be provided through public notice,of any change to an interoperability interface maintained by the large communications platform provider that will affect the interoperability of a competing communications service.

(6) NON-COMMERCIALIZATION BY A LARGE COMMUNICATIONS PLATFORM PROVIDER.—A large communications platform provider may not collect, use, or share user data obtained from a competing communications service through the interoperability interface except for the purposes of safeguarding the privacy and security of such information or maintaining interoperability of services.

(d) NON-COMMERCIALIZATION BY A COMPETING COMMUNICATIONS PROVIDER.—A competing communications provider that accesses an interoperability interface may not collect, use, or share user data obtained from a large communications platform provider through the interoperability interface except for the purposes of safeguarding the privacy and security of such information or maintaining interoperability of services.

(e) EXEMPTION FOR CERTAIN SERVICES.—The obligations under this section shall not apply to a product or service by which a large communications platform provider does not generate any income or other compensation, directly or indirectly, from collecting, using, or sharing user data.

Section 5. Delegatability.

(a) GENERAL DUTY OF LARGE COMMUNICATIONS PLATFORM PROVIDERS.—A large communications platform provider shall maintain a set of transparent third party-accessible interfaces by which a user may securely delegate a custodial third-party agent to manage the user's online interactions, content, and account settings on a large communications platform on the same terms as a user.

(b) REVOCATION OF ACCESS RIGHTS.—A large communications platform provider may revoke or deny access for any custodial third-party agent that—

(1) repeatedly facilitates fraudulent or malicious activity or (2) that fails in the duties specified for Custodial Third-Party Agents within this Act. A large communications platform provider must provide a report of all such revocations or denials to the Attorney General on request.

(c) DUTIES OF A CUSTODIAL THIRD-PARTY AGENT.—A custodial third-party agent—

(1) shall reasonably safeguard the privacy and security of user data provided to it by a user, or accessed on a user's behalf;

(2) shall not access or manage a user's online interactions, content, or account settings in any way that—
(A) will benefit the custodial third-party agent to the detriment of the user;
(B) will result in any reasonably foreseeable harm to the user; or
(C) is inconsistent with the directions or reasonable expectations of the user; and
(3) shall not collect, use, or share any user data provided to it by a user, or accessed on a user's behalf, for the commercial benefit of the custodial third-party agent.

(d) FEES.—A custodial third-party agent may charge users a fee for the provision of the products or services described in subsection (a).

(e) EXTENT OF ACCESS RIGHTS.—Nothing in this section shall be construed to confer greater rights of access for a custodial third-party agent to a large communications platform than are accessible to a user.

Section 6. Implementation and Enforcement.

(a) COMPLIANCE ASSESSMENT.—The Attorney General shall regularly assess compliance by large communications platform providers with the provisions of this Act, including the publication of Complaints.

(b) COMPLAINTS.—The Attorney General shall establish procedures under which a user, a large communications platform provider, a competing communications provider, and a custodial third-party agent may file a complaint alleging that a large communications platform provider, a competing communication provider, or a custodial third party agent has violated this Act.

(c) ENFORCEMENT.—
(1) This Act will be enforced by the Attorney General of [State].
(2) FINES.—In assessing any fine for a violation of this Act, the Attorney General shall consider each individual user affected by a violation of this Act as an individual violation.
(3) RELIANCE ON OPEN STANDARDS.—Any large communications platform provider that establishes and maintains interoperability through an open standard shall be entitled to a rebuttable presumption of providing access on fair, reasonable, and nondiscriminatory terms.

EFFECTIVE DATE.—This Act shall take effect on [xxx].

Section 7. Relation to Other Laws.

Nothing in this Act shall be construed to modify, limit, or supersede the operation of any privacy or security provision in—

(1) section 552a of title 5, United States Code 24 (commonly known as the ''Privacy Act of 1974'');

(2) the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.);

(3) the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(4) the Fair Debt Collection Practices Act (15 6 U.S.C. 1692 et seq.);

(5) the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.);

(6) title V of the Gramm-Leach-Bliley Act (15 10 U.S.C. 6801 et seq.);

(7) chapters 119, 123, and 206 of title 18, United States Code;

(8) section 444 of the General Education Provisions Act (20 U.S.C. 1232g) (commonly referred to as the ''Family Educational Rights and Privacy Act 16 of 1974'');

(9) section 445 of the General Education Provisions Act (20 U.S.C. 1232h);

(10) the Privacy Protection Act of 1980 (42 U.S.C. 2000aa et seq.);

(11) the regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note), as those regulations relate to—
(A) a person described in section 1172(a) of the Social Security Act (42 U.S.C. 1320d– 1(a)); or
(B) transactions referred to in section 1173(a)(1) of the Social Security Act (42 6 U.S.C. 1320d–2(a)(1));

(12) the Communications Assistance for Law Enforcement Act (47 U.S.C. 1001 et seq.); (13) sections 222 and 227 of the Communications Act of 1934 (47 U.S.C. 222, 227); or (14) any other privacy or security provision of Federal law.

Appendix E – Model Bill: Digital Advertising Tax for Public Health Monitoring

Background and Goal

This bill borrows language from previous digital advertising tax initiatives to fund public health monitoring of online experiences within a jurisdiction.

Section 1. General Provisions and Definitions.

This part shall be known, and may be cited, as the Digital Advertising Services Tax and Public Health Monitoring Law.

For purposes of this part, the following definitions shall apply:

(a) "Annual gross revenues" means income or revenue from all sources, before any expenses or taxes, computed according to generally accepted accounting principles.

(b) "Broadcast entity" means an entity that is primarily engaged in the business of operating a broadcast television or radio station.

(c) "Department" means the [STATE REVENUE & TAXATION AUTHORITY].

(d)(1) "Digital advertising services" means advertisement services on a digital interface, including advertisements in the form of banner advertising, search engine advertising, interstitial advertising, and other comparable advertising services.

(2) "Digital advertising services" does not include advertisement services on digital interfaces owned or operated by or operated on behalf of a broadcast entity or news media entity.

(e) "Digital interface" means any type of software, including a website, part of a website, or application, that a user is able to access.

(f)(1) "News media entity" means an entity engaged primarily in the business of newsgathering, reporting, or publishing articles or commentary about news, current events, culture, or other matters of public interest.

(2) "News media entity" does not include an entity that is primarily an aggregator or republisher of third-party content.

(g) "Taxable base" means the annual gross revenues derived from digital advertising services in the state.

(h) "User" means an individual or any other person who accesses a digital interface with a device.

Section 2. Imposition of Tax.

(a) Beginning [xxx], a tax is hereby imposed on the annual gross revenues of a person that are derived from digital advertising services in the state.

(b) The tax imposed by this section shall be at a rate of 5 percent.

(c) The tax imposed by this section shall only apply to persons with at least one hundred million dollars ($100,000,000) in global annual gross revenue.

(d) A taxpayer who derives gross revenues from digital advertising services in the state may not directly pass on the cost of the tax imposed under this section to a customer who purchases the digital advertising services by means of a separate fee, surcharge, or line item.

Section 3. Administration.

The department shall administer and collect the taxes imposed by this part pursuant to [yyy]

(a) The department may prescribe, adopt, and enforce regulations relating to the administration and enforcement of this part, including, but not limited to, provisions governing collections, reporting, refunds, and appeals.

(b) The department may prescribe, adopt, and enforce emergency regulations relating to the administration and enforcement of this part.

(c) It is the intent of the Legislature that net proceeds from the tax imposed by this part shall be used to fund public health measurement of the impact of online digital advertising platforms. Revenue from this Act shall be provided to [STATE PUBLIC HEALTH AGENCY] who are mandated to use these funds to conduct surveys on at least a yearly basis that establish publicly reported population based statistics about:

- What percentage of citizens use popular online platforms.
- How much time citizens report using each platform.
- Whether citizens report feeling manipulated by each platform they use.
- Whether citizens report feeling that the usage of each platform interferes with sleep and/or other important goals.
- Whether citizens report unwanted contact on each platform that they use - including experiences of bullying, unwanted sexual advances, and potential scams.
- Whether citizens report unwanted/harmful experiences on each platform that they use - including feeling worse about their lives, seeing unwanted sexually explicit images/videos, seeing graphic/violent images that disturb them, and witnessing hate or bullying.
- Whether citizens report unwanted/harmful use of their information on platforms - including the unwanted use of their images and/or likeness.

All statistics will include breakdowns by age (with minors reported separately from adults), gender, race/ethnicity as well as by volume of usage (with reports for 25th, 50th, 75th, 90th, 95th, and 99th percentiles of self-reported usage).

Appendix F – Model Bill: Act to Promote Safe, Effective, and Distraction Free Education for PreK-12 Students

Background and Goal

This package of model bills was drafted by the Becca Schmill Foundation in collaboration with The Anxious Generation, the USC Neely Center, Fairplay and the Phone-Free Schools Movement. It was written to establish a gold standard that prioritizes students' mental health and development, academically and socially. This package of model legislation contains two separate bills, each of which is designed to promote children's learning, focus, and emotional health during school hours. The first bill in this package focuses on banning personal electronic communication devices in schools. The second reduces schools' reliance on social media in the classroom and during extracurricular activities.

Model Legislation Findings

The [state] Legislature finds that our children are experiencing a mental health crisis and the heavy use of smartphones and social media is a primary contributor, and:

(a) Virtually all teens (95%) ages 13 to 17 use social media, and more than 1 in 3 report that they use it "almost constantly." Even though most social media platforms set 13 as the minimum age requirement, nearly 40% of kids ages 8 to 12 use social media. *Teens, Social Media and Technology 2024; Teens, Social Media and Technology 2022; The Common Sense Census: Media Use by Tweens and Teens, 2021*.

(b) Studies have shown that higher use among children and adolescents is linked to adverse effects: depression and anxiety; inadequate sleep (which can disrupt neurological development and lead to depression and suicidal behaviors); low self-esteem; poor body image; eating disorder behaviors; and online harassment. *Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory, 2023*. It's often the most vulnerable youth who are most affected by these adverse effects, increasing disparities.

(c) In Jonathan Haidt's 2024 book, The Anxious Generation: How the Great Rewiring of Childhood Is Causing an Epidemic of Mental Illness, he documents the staggering increases since 2010 in clinical diagnoses of anxiety (134%); depression (106%); anorexia (100%); and substance abuse and addiction (33%). *The Anxious Generation: How the Great Rewiring of Childhood is Causing an Epidemic of Mental Illness, 2024*.

(d) The U.S. Surgeon General has emphasized the link between social media and mental health harms to adolescents. He has called for warning labels on social media to address "the defining public health challenge of our time," and has stated that "the risk of not acting could be someone's life." *Surgeon General: Why I'm Calling for a Warning Label on Social Media Platforms, The New York Times, 2024*.

(e) Social media and gaming platforms have evolved to include manipulative and addictive features that pose a significant risk of harm to the mental health and well-being of children and adolescents. *Prevalence and Characteristics of Manipulative Design in Mobile Applications, 2022; Addictive Features of Social Media/ Messenger Platforms and Freemium Games against the Background of Psychological and Economic Theories, International journal of environmental research and public health, 2019*.

(f) Members of historically marginalized groups are disproportionately impacted by cyberbullying online.

- Black teens are more likely than Hispanic or White teens to say they have been cyberbullied because of their race or ethnicity. Black and Hispanic teens are far more likely than White teens to say online harassment and bullying are a major problem for people their age. *Teens and Cyberbullying 2022, Pew Research Center, 2022*.

- According to the 2023 Youth Risk Behavior Survey, LGBTQ+ students were almost twice as likely (25% compared to 16%) than cisgender and heterosexual students to be electronically bullied. Youth Risk Behavior Survey Data Summary & Trends Report 2013-2023, US Centers for Disease Control and Prevention, 2024.

(g) There is growing evidence that unrestricted use of personal electronic devices and access to social media by students at elementary, middle, and secondary schools interferes with the educational and social development mission of schools, lowers student performance (particularly among low-achieving students), promotes cyberbullying, contributes to higher rates of academic dishonesty (i.e., plagiarism and cheating). *Cell Phones, Student Rights, and School Safety: Finding the Right Balance, Canadian Journal of Educational Administration and Policy, 2021*.

(h) A New York Times review of more than 400 fight videos from more than a dozen states — as well as interviews with three dozen school leaders, teachers, police officers, pupils, parents, and researchers — found a pattern of middle and high school students exploiting phones and social media to arrange, provoke, capture and spread footage of brutal beatings among their peers. In several cases, students later died from the injuries. *An Epidemic of Vicious School Brawls, Fueled by Student Cellphones, New York Times, 2024*.

(i) A 2020 study of Norwegian schools that had banned smartphones, found that:

- Banning smartphones lowers the incidence of bullying for both girls and boys,
- Banning smartphones results in girls making gains in both their GPA and externally graded mathematics exams, on the order of 0.22 standard deviations. For comparison, the author notes that reducing class size by one student correlates to an improvement of about 0.00–0.05 standard deviations,
- These benefits are particularly strong for students from low socioeconomic backgrounds,
- The effects are particularly strong at schools with the strictest bans, requiring students to hand in or lock away their phones, not just place them on silent mode. The study's author notes that, even in silent mode, phones can still pull at a student's attention, distracting them as they wonder if someone messaged them, liked their status, or whatever else,
- Banning smartphones reduces the number of consultations for psychological symptoms by about 2–3 visits per child, per year.

Smartphone Bans, Student Outcomes and Mental Health, Institutt for samfunnsøkonomi, 2024.

(j) According to school safety experts, cell phones make children less safe in a school emergency. When students use cell phones during an unfolding emergency, it can distract them from important instructions from school staff and safety professionals. Cell phone use can also make a student easier for a person who intends harm during an emergency to be heard or seen. *Phone-free schools protect kids during emergencies, 2024*.

(k) School should be a safe environment for all students - where social development, learning, and the ability to focus are nurtured and prioritized. It is in the public interest, and is, therefore, the responsibility of this body, to ensure a physically, emotionally, and psychologically safe school environment for every child in [state] - - one where students can learn, make friends, optimize their future potential, and otherwise thrive.

An Act to Create Phone Free Education in PreK-12 Schools

Statement of purpose of bill as introduced:

This bill proposes to prohibit access to personal electronic devices in public schools, education centers, charter schools, or training programs, providing pre-kindergarten, elementary, or secondary education.

Section 1. Definitions.

(a) "Instructional Time" means "the time from when the first bell rings at the start of school day until the dismissal bell rings at the end of the school day, including but not limited to any structured or unstructured learning experiences like recess, lunch periods, time in between classes, and field trips."

(b) "Parent" means "a parent or guardian of a student who is authorized to make education decisions for the student."

(c) "Personal Electronic Communication Device(s)" means "any portable electronic equipment capable of providing voice, messaging, or other data communication between two (2) or more parties or devices, or capable of connecting to a smartphone, the internet, or a cellular or Wi-Fi network, including but not limited to smartphones, cellular phones, bluetooth enabled devices, tablets, smartwatches or other wearables, and gaming devices.

Personal electronic communication devices do not include:
(1) School-owned devices provided to the student in accordance with the limitations placed herein;
(2) Portable devices which meet the definition of a medical device under Section 201(h) of the Food, Drug & Cosmetic Act.

(d) "School" means "any public school, education center, charter school, or training program, providing pre-kindergarten, elementary, or secondary education."

(e) "School-related activity" means "any school sanctioned activity, event, or function, occurring outside of instructional time, where students are under supervision of the school, whether on or off school premises. School-related activities may include bus rides, field trips, sporting events, and school dances.

(f) "Student" means "an individual currently enrolled or registered at a school as defined under subdivision (d) of this section."

Section 2. Prohibition of Personal Electronic Communication Devices.

2.1 Prohibition During Instructional Time

(a) Each school district or applicable governing body shall adopt and implement a policy for schools that:
(1) requires all personal electronic communication devices be turned off, securely locked away, and inaccessible to students during instructional time;
(2) Ensures that students do not have access to personal electronic communication devices, by requiring them to be locked or stowed away in secure lockable pouches, phone lockers, pencil pouches, manila envelopes, or other inaccessible location;
(3) Provides that schools may limit student access to personal electronic communication devices outside of instructional time, during school-related activities;
(4) Includes enforcement provisions to ensure strict compliance with the policy by students and school employees; and
(5) Provides that a student may contact their parent or caregiver during the school day if needed by using a school telephone made available to the student in a manner and location designated by the school.

(b) Notwithstanding subsection (a), a student shall not be prohibited from possessing or using a personal electronic communication device under any of the following circumstances:
  (1) When a licensed physician determines that the possession or use of a personal electronic communication device is necessary for the health or well-being of the student;
  (2) When the possession or use of a personal electronic communication device is required by a student's Individual Education Plan (IEP), or Section 504 Accommodations Plan.

(c) Districts shall collect data annually to measure the impact of its policy on student behavior, mental health, disciplinary incidents, school attendance, and academic performance.

An Act to Reduce Reliance on Social Media in the Classroom and During Extracurricular Activities

Section 1. Definitions.

(a) "Instructional Time" means "the time from when the first bell rings at the start of school day until the dismissal bell rings at the end of the school day, including but not limited to any structured or unstructured learning experiences like recess, lunch periods, time in between classes, and field trips."

(b) "Gaming app" means "a software program that allows users to play games on mobile devices, tablets, or computers."

(c) "Personal Electronic Communication Device(s)" means "any portable electronic equipment capable of providing voice, messaging, or other data communication between two (2) or more parties or devices, or capable of connecting to a smartphone, the internet, or a cellular or Wi-Fi network, including but not limited to smartphones, cellular phones, bluetooth enabled devices, tablets, smartwatches or other wearables, and gaming devices."

Personal electronic communication devices do not include:
  (1) School-owned devices provided to the student in accordance with the limitations placed herein;
  (2) Portable devices which meet the definition of a medical device under Section 201(h) of the Food, Drug & Cosmetic Act.

(d) "Parent" means "a parent or guardian of a student who is authorized to make education decisions for the student."

(e) "School" means "any public school, education center, charter school, or training program, providing pre-kindergarten, elementary, or secondary education."

(f) "School-related activity" means "any school sanctioned activity, event, or function, occurring outside of instructional time, where students are under supervision of the school, whether on or off school premises. School-related activities include but are not limited to bus rides, field trips, sporting events, and school dances."

(g) "Social Media means "any public-facing website, online service, online application, mobile application, or gaming application, used primarily for the purpose of posting and viewing user-generated content. For the purposes of this Act, Social media does not include:
  (1) an online website, application, or mobile application where the exclusive function is e-mail or direct messaging shared only between the sender and intended recipients, without displaying or posting publicly or to other users not specifically identified as the recipients by the sender.

(2) An online website, application, or mobile application where the posting of comments or other interactive functionality is merely incidental to its predominant purpose.
(3) A school sanctioned website, application, or service used for the purpose of publishing student journalism, or school related news, events, and updates."

(h) "Student" means "an individual currently enrolled or registered at a school as defined under subdivision (e) of this section."

Section 2. Prohibition of Social Media In Schools.

2.1 Prohibition of Integration of Social Media Platforms into Education

(a) Each school district or applicable governing body shall adopt and implement a policy that prevents students from relying on social media. Such policy shall:
(1) prohibit schools, school employees, or school volunteers from utilizing social media for communication with students during instructional time or for the facilitation of school-related activities;
(2) prohibit students from accessing social media or gaming apps during instructional time or school-related activities;
(3) prohibit students from accessing social media or gaming apps on school-issued electronic communication devices;
(4) Prohibit students from accessing social media or gaming apps on personal electronic communication devices during instructional time or school-related activities;
(5) Require schools to block access to social media and gaming apps on school provided internet connections;

(b) Schools may allow exceptions to the prohibitions of the policy required under subsection (a) for any of the following:
(1) For work which requires shared documents, emails, or the use of the Internet for the completion or enhancement of homework assignments, and the electronic submission of assignments.
(2) For a school authorized use, where such use:
(A) is limited to school issued devices;
(B) is approved in writing by the school's superintendent or his or her designee;
(C) is required to meet a standards-aligned educational objective that cannot be reasonably achieved without the use of social media or gaming apps.
(D) contains clear instructions on the appropriate use of social media and/or gaming apps to align with the approved educational objectives; and
(E) may be revoked by the school's superintendent or his/her designee at any time."

Office of the

Minnesota Attorney General

helping people afford their lives and live with dignity, safety, and respect

445 Minnesota Street, Suite 600, St. Paul, MN 55101
(651) 296-3353 (Twin Cities Calling Area)
(800) 657-3787 (Outside the Twin Cities)
(800) 627-3529 (Minnesota Relay)
www.ag.state.mn.us