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

February 2024

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

Protecting Minnesotans, especially young people, from the threats and harm of technology is key to my role helping Minnesotans afford their lives and live with dignity, safety, and respect. That's why, when the Legislature directed my Office to research and publish a report on the subject, I welcomed the job. *See* 2023 Minn. Laws, Chapter 57, Art. 1, § 4, subd. 3 (Report). As directed by the Legislature, this report:

- Evaluates the impact of technology companies and their products on the mental health and well-being of Minnesotans, with a focus on children;
- Discusses proposed and enacted consumer protection laws across the country and world related to the regulation of technology companies; and
- Makes policy recommendations for the Legislature to consider enacting in order to protect Minnesotans, and especially our youth, from harmful design features in certain technology products and platforms.

Thanks to a one-time grant from the Legislature, my Office was able to enlist the help of a brilliant and highly experienced expert in this field to research and help write this report. Dr. Ravi Iyer is a technologist and academic psychologist who is currently the managing director of USC Marshall School's Neely Center for Ethical Leadership and Decision Making. He previously worked for over four years at Meta (which owns Facebook and Instagram) addressing the large-scale societal impact of Facebook and has published dozens of scholarly articles in his field. This report would not have been possible without his ideas, research, writing, and commitment.

In addition, Alex Barkley, a law clerk with our Office, assisted with every stage of this project, devoting countless hours researching relevant laws and bills in other states and countries and drafting Section Two of this report—a job which they balanced on top of their third-year coursework at the University of Minnesota Law School. My deepest thanks to both Dr. Iyer and Alex for their time, energy, and commitment to helping us complete this thorough and thoughtful report.

This report is just one of many actions that my Office is taking to protect young people from the harms of technology, especially those that have been designed to addict children and teenagers for profit. For example, in October 2023, I joined a bipartisan group of 42 state attorneys general in suing Meta for intentionally creating addictive design features that manipulate children and teens into spending as much time as possible on their platforms despite knowing this often causes them serious physical and mental harm. That litigation is ongoing. Similarly, my Office, along with a large, bipartisan coalition of attorneys general, continues to actively investigate TikTok for similar practices, including design features TikTok uses to capture the attention of young users and addict them to their platform.

Creating products that manipulate young users into overuse and addiction is nothing new—just look at the tobacco companies. What makes emerging technology products like Facebook, Instagram, and TikTok so uniquely dangerous is the new technological ability to learn users' habits and adapt to them in real time using data collection and algorithms, creating a product that becomes more uniquely addictive to each person over time.

These products demand a modern regulatory response. It is my hope that this report can help not only the Minnesotans and Minnesota policymakers who are responsible for designing that response, but people across America and world who want to craft smart and effective solutions to one of the great public-health crises of our time.

Executive Summary

Technology has been and remains an important tool for societal progress. Modern technology companies have created many benefits that previously did not exist, such as allowing for the real-time discussion of important issues[1] or wider access to educational content.[2] At the same time, societal costs have accompanied these benefits, just like other technological advances of previous eras. Cars enabled greater access to employment and medical care, but safety standards were developed to ensure that their use led to as few deadly accidents as possible. Advances in agricultural technology reduced the cost of food, but standards were developed to prevent producers from cutting corners 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 minimum 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 unsafe, yet cheaper products.

Currently, most Americans want government action to ensure that technology companies design their platforms in ways that protect the mental health of children.[3] 80 percent believe that evolving AI technologies will make these problems worse.[4] Fortunately, a great deal of recent regulatory effort across jurisdictions has gone into understanding and attempting to solve these issues. This report attempts to build on those efforts to point towards a way forward for Minnesotans.

This report is divided into five sections. 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 how there are many highly prevalent negative effects of technology that are facilitated by specific product design choices made by technology companies. In particular, technological design choices facilitate the below negative effects on youth:

- Many consumers, especially youth, are experiencing bullying and harassment, facilitated by the choices of technology platforms.
- Many consumers are having experiences with unwanted disturbing, graphic, and sexual content, often recommended by AI-powered algorithms.
- Many users experience envy and upward social comparison, which are encouraged by technology platform dynamics.
- Many cases of manipulation and fraud begin with unwanted contact from strangers 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 youth.
- Platforms facilitate the misuse of user information and images, including that of younger users.

- Excessive and compulsive usage of technology, facilitated by systems that are optimized for 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.

In the second section, we provide more detail as to the many specific legislative efforts that are occurring across jurisdictions, with an eye toward what we can learn. In the third section, the report builds on existing legislative efforts across jurisdictions described in section two to make a set of recommendations for policy makers to address the above harms. There are successes of previous legislative efforts that can be replicated, but also many notable areas where improvement is needed to make maximal impact. In particular, the identified lessons learned are:

- Being too prescriptive about solutions can have negative consequences.
- A lack of specificity can lead to legal challenges, implementation difficulty, and opposition from those who fear misuse of well-intentioned efforts.
- Broad reporting requirements have often not had a material impact.
- Age verification needs to be done in a manner 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.
- Banning social media platforms for youth has 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.

In the fourth 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. Our goal is to learn from previous efforts and identify the most effective legislative possibilities that directly address the concerns and challenges that have arisen in improving technology's impact on society. Our recommendations are:

- Ban "Dark Patterns" within platform design:
  - Ban design features (*e.g.*, optimizing for time spent, infinite scroll, auto-play, aggressive notifications) that encourage greater usage for children beyond their explicit desires. Offer all users accessible tools to limit their platform usage.
  - Mandate aggressive privacy defaults to limit the unwanted sharing of data and images, especially for sexual content.
  - Mandate responsible amplification through limits on engagement-based optimization.
  - Mandate transparent, sensible rate limits that would limit the ability of small groups of users to manipulate others.
- Mandate transparency of product experimentation that can illuminate new harmful "dark 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 to encourage consumer choice.
- Mandate usage limits and education within schools.

Finally, in our fifth section, we discuss the likely impact on the youth mental health crisis given this proposed legislation, especially in a world of increasingly ubiquitous AI. In particular, we review debates and evidence as to the net effect of technology on Minnesota youth, elaborate why we chose to focus on how specific design choices are facilitating specific negative effects in Section One, and discuss how the increasing ubiquity of AI-powered algorithms is likely to affect current trends.

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.[5] Given the complex heterogeneous nature of both technologies and individuals, a focus on the average aggregate effect may be misplaced. 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. For each of these categories, we can also demonstrate **causality**, by pointing to evidence that these harms are often exacerbated by "dark patterns," 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."[6] These dark 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.[7] Greater integration of AI into society is likely to further exacerbate these issues. This rising threat to Minnesota youth suggests that government action is necessary. Not all technology products exhibit these same dark patterns, which proves that a better technological future that still makes room for corporate innovation and profits is possible.

A list of common unwanted harmful experiences reported by consumers is elaborated below. Notably, 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.[8]

Many Consumers, Especially Youth, are Experiencing Bullying and Harassment, Facilitated by the Choices of Technology Platforms

> **"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

In Meta's own internal surveys[14]

Among Instagram users:

28.3%
reported witnessing bullying and harassment in a seven day period

8.1%
reported being a target

Among teens aged 13-15:

27.2%
reported witnessing bullying

10.8%
reported being a target

Online bullying is a primary societal concern, having been linked to numerous suicides[9] and with many parents reporting it as a top concern[10] Bullying and harassment is often not readily perceptible by outsiders 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, to understand online bullying and harassment it is helpful 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[11] 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 online bullying or harassment by friends or acquaintances.[12] A Pew Survey including US teens ages 13-17 found that 46 percent reported experiencing cyberbullying.[13] In Meta's own internal surveys, 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.[14]

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. Between 40 and 50 percent of young victims of cyberbullying do not know their perpetrator's identity and popular applications that permit anonymous messaging allow perpetrators to bully without revealing their identity to their victims.[15] Platforms have developed policies to enforce on such harassment,[16] 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.[17] In contrast to simple engagement optimization,[18] platforms could incentivize signals of positive engagement from diverse sources, which would instead amplify sources that are less likely to be reported for bullying.[19]

Many Consumers are Having Experiences with Unwanted Disturbing, Graphic, and Sexual Content, Often Recommended 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[20] and youth[21] 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,[22] rather than explicit user preference. In a study of Australian 16-17 year olds,[23] 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.[24]

Internal platform studies confirm that unwanted experiences, across categories, are common. In one leaked report from Meta,[25] 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. According to a US study by Common Sense Media,[26] 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.[27] Investigations by the Wall Street Journal have shown how algorithmic recommendations can lead users to be served content relating to eating disorders[28] and the sexualization of minors.[29] 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.[30]

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,[31] and even when used, they often do not have the impact that users expect.[32] A Mozilla study on regretted YouTube experiences found that most unwanted content was surfaced by recommendations[33] rather than from user choice. Recommendation algorithms are largely optimized for engagement, which tends to be dominated by small groups of relatively abusive users.[34] Product changes that reduce engagement incentives have been shown to reduce exposure to unwanted content.[35] 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.[36]

According to a US study by Common Sense Media [26]

12
the average age of pornography exposure online

15%
reported seeing pornography at age **10 or younger**

58%
of youth said they came across pornography online by accident

>50%
respondents said they viewed violent porn

Experiences of Envy and Upward Social Comparison are Common and 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.[37] Upward social comparison has been linked to increased feelings of threat and reduced psychological well-being.[38] Many technology platforms have been linked to experiences of upward social comparison, particularly among youth. In one study,[39] 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.[40] A study by the Allianz Life Insurance Company of North America[41] 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.

Internal studies by platforms indicate similar patterns. In one internal study from Meta,[42] 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." 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.[43]

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.[44] Researchers at a Canadian children's hospital found[45] 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.[46]

In one internal study from Meta,[42]

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."

Many Cases of Manipulation and Fraud Begin with Unwanted Contact from Strangers, Facilitated by Loose Privacy Defaults and High Rate Limits, with Especially Serious Consequences for Youth

> **"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

In one study of adolescents in Utah[49]

26%
reported getting involved in an unwanted conversation

17%
reported a stranger trying to meet them

Per internal research detailed in the Wall Street Journal[52]

1/8
users under the age of 16 said they experienced unwanted sexual advances on Instagram

Both parents and teens report serious concerns about the ability of strangers to find and contact youth. There are many documented cases[47] of foreign individuals targeting youth online, such that the FBI recently issued a public safety alert.[48] In one study of adolescents in Utah,[49] 26 percent reported getting involved in an unwanted conversation and 17 percent reported a stranger trying to meet them. Generally, per a Common Sense Media report,[50] youth report the ability of strangers to contact them as having a negative effect. Once contacted, youth are particularly vulnerable to being manipulated.[51]

These trends are corroborated by internal research by technology platforms. Per internal research detailed in the Wall Street Journal,[52] 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. They are also facilitated by the capabilities that platforms provide new untrusted users to contact numerous strangers without the limits that exist in offline life,[53] where such behavior would have negative consequences. In contrast, having a history of trustworthiness plays an important part in reducing risk across domains,[54] including in internal social media research.[55] Platforms have intermittently acknowledged this risk by removing capabilities for untrusted users during times of stress, but such product changes are often ad-hoc. 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.

Technology Platforms Facilitate User Information and Images Being Misused by Others, 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[56]

Recent press articles[57] based on investigations from Stanford University[58] and the University of Massachusetts[59] 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 study in Utah,[60] six percent of 8th/9th graders reported having their photos used in an inappropriate way. In a Pew study,[61] "others posting things about you or pictures of you without asking permission" was one of the top complaints about Facebook (36 percent strongly disliked). Numerous state attorneys general, including Minnesota's, have recently written about the increased urgency of these problems given the ubiquity of generative AI[62] and there have already been reports of students using generative AI to create fake nude photos using images of their classmates.[63]

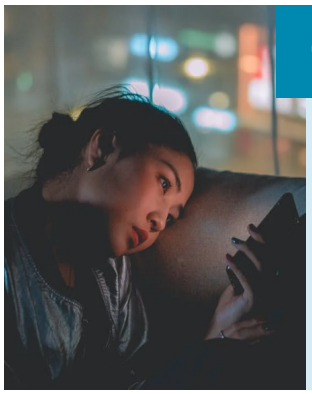
In some cases, the sexualization of youth is a direct result of incentives that platforms encourage and foster through facilitating monetary rewards for popular content creators. Without that monetary incentive, such content would not likely be created. Access to content that can be misused is also often 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.

Excessive Compulsive Use of Technology Displaces Beneficial Activities like Sleep and In-person Socialization, Leading to Reduced Well-being

> **"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

Many users, especially youth, report using technology more than they would ideally like, leading to negative consequences in their life. For example, 55 percent of Minnesota college students in one study[64] report having an issue with excessive computer/internet use and 47 percent report that this excessive use is affecting their academics. 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.[65] In a study of parents by Accountable Tech,[66] 23 percent reported that their kids were "addicted to the phone."

Sleep, in particular, is widely reported to be affected by technology use. For instance, 46 percent of Minnesota college students report getting adequate sleep on three or fewer days a week.[67] 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



Of Minnesota College Students...

55%
report having an issue with excessive computer/internet use[64]

47%
report that excessive computer/internet use is affecting their academics[64]

46%
report getting adequate sleep on three or fewer days a week[67]

Gen Z admit to staying up past their bedtime due to social media.[68] 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.[69] 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,[70] "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,[71] these features were designed intentionally to increase time spent through features that "give you a little dopamine hit every once in a while." Cognitive psychologists[72] 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.[73] 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.[74] Instagram uses an array of push notifications that require users to navigate complex settings in order to disable.[75] Many algorithms within technology platforms are designed to maximize users' time spent on the platform.[76] 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.[77]

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.[78]

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.[79] Unfortunately, there is little visibility of training data being provided to those in society who are ultimately affected by these algorithms. 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,[80] workplace hiring,[81] government decision making,[82] insurance,[83] content moderation,[84] and criminal justice decision making.[85] 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[86] or mis-specified objective functions[87] and so society has a role to play in overseeing such technological decision making.

Section Two: The Legislative Landscape

In this section, we provide more detail as to the many specific legislative efforts that are occurring across jurisdictions, to inform what we can learn and how those learnings ladder up collectively to our recommendations in the next section.

Social Media Regulation

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

Australia
- Open Safety Act 2021

International Models

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 2023 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.[88] 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.[89]

In the European Union, the Digital Services Act has similar goals and 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.[90] 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.[91]

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.[92] The Act further required technology platforms to develop new codes to scan for illegal and harmful content, such as graphic sexual or violent imagery.

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.[93] 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 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.

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.[94] 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.[95] The Eleventh Circuit Court of Appeals upheld the injunction in May 2022.[96]

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.[97] As in Florida, the law was promptly challenged in court, and the federal district court judge granted a preliminary injunction enjoining the law.[98] 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.[99] The Supreme Court vacated the appellate court's stay, allowing the injunction to remain in place.[100] 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.[101]

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* will be heard together in oral argument on February 26, 2024.[102]

We hope that the Supreme Court's decision in these cases will provide further guidance on how to regulate harmful content online without running afoul of First Amendment protections. Our prescribed policy choices focus on design choices, rather than content moderation, which should mitigate potential litigation on First Amendment challenges.

Social Media Bans

Only one state has considered a ban on social media. Montana became the first state to ban TikTok[103], though a federal judge granted a preliminary injunction enjoining the law in November 2023.[104] It is likely that any law that bans access to social media platforms, in part or in whole, will continue to face legal challenges and First Amendment concerns.[105] Our recommendations do not advocate for any state-wide bans on social media, and in instances where social media bans might be appropriate (such as in schools), we suggest legislation that would allow individual school districts to adopt locally-sensitive policies.

Social Media Reform Focusing on Minors

Congress has considered the unique harms to children online in recent years. The Kids Online Safety Act ("KOSA") is a bill introduced first in 2022 and again in May 2023 with bipartisan and presidential support.[106] 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.[107] 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.[108] For example, 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.[109]

United States Legislation

Federal Legislation
- Kids Online Safety Act ("KOSA")
- Executive Order 14110, on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

At least 25 states and the District of Columbia
- introduced bills related to Artificial Intelligence

California
- California Age Appropriate Design Code

Connecticut
- S. 3, 2023 Gen. Assemb. (Conn. 2023).

Delaware
- General data privacy act

Florida
- State Bill 7072

Montana
- TikTok Ban

New York
- Stop Addictive Feeds Exploitation (SAFE) for Kids Act

Texas
- Texas House Bill 20

Utah
- Social Media Regulation Act

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.[110] Online platforms are required to set minors' accounts with the strongest privacy setting options by default (and must not use dark 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.[111] 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.[112]

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.[113] 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.[114] The court granted the preliminary injunction, finding that the Age Appropriate Design Code does regulate expression and speech in violation of the First Amendment.[115] The court also expressed concern that the Act might cause greater harm by mandating increased collection of private data.[116] The State of California appealed to the Ninth Circuit Court of Appeals in October 2023.[117]

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.[118] Delaware's general data privacy act also prohibits sites from marketing specific products, including alcohol and tobacco, firearms, and body modifications, to children.[119] New York is currently debating a similar bill that would prohibit sites from collecting, using, sharing, or selling minors' personal data for purposes of targeted advertising without consent.[120]

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 require social media companies to restrict minor access to accounts from 10:30 p.m. to 6:30 a.m.[121] NetChoice recently sued the State of Utah, alleging that the Act represented an "unconstitutional attempt to regulate both minors' and adults' access to—and ability to engage in—protected expression" in violation of the First Amendment.[122] New York is considering a bill 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, currently in committee, would mandate a default chronological feed for minor users, and would allow parents to set limitations on total hours a day their minor children could spend on online platforms.[123] Platforms would also be prohibited from 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.[124]

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 design changes that companies should undertake could lead to reduced opposition and legal challenges. However, some laws recommend specific changes that may not be effective[125] 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,[126] passed by the European Union in 2016, has served as a model both internationally and within the United States.[127] 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.[128] Other states have passed similar legislation, and more, including Minnesota, have such bills under current consideration.[129] Our recommendation to mandate default settings with greater privacy protection complements the consumer rights protected by these bills.

AI Specific Legislation

President Biden issued Executive Order 14110, on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, on October 30, 2023.[130] 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. Public reports and other deliverables from federal agencies will be due throughout 2024.

The European Union has provisionally passed the Artificial Intelligence Act to regulate AI across a broad range of sectors. The Act was proposed in 2021 and provisionally passed by the Council and Parliament in December 2023, and will take effect progressively beginning in 2025. 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.[131]

In 2023, lawmakers in at least 25 states and the District of Columbia introduced bills related to AI, and 18 states adopted resolutions or enacted legislation.[132] Several states and municipalities in the U.S. have passed or introduced legislation about 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.[133] New York is also considering the Digital Fairness Act, which would expand the law to state agencies. California has introduced a bill to prohibit automated decision tools that result in algorithmic discrimination on the basis of race, sex, disability, or other protected classifications.[134] D.C. introduced a similar bill in 2023, which would "prohibit users of algorithmic decision making from utilizing algorithmic eligibility determination in a discriminatory manner," as did New Jersey.[135] In Colorado, a 2021 bill requires insurance companies to document that their use of automated systems does not result in discrimination.[136]

Other states have also discussed legislation relating specifically to the use of visual AI. Michigan enacted a bill last year requiring disclaimers of AI in political advertising. New York is considering a statute that would require the disclosure of AI and "deepfake" technology in advertising and social media.[137] Pennsylvania introduced a bill that would criminalize some categories of AI-generated sexual imagery, including content involving minors.[138]

States have also evaluated laws concerning specific applications of AI. Arizona's legislature passed a bill that would have prohibited AI in voting machines, though it was ultimately vetoed by the governor. Last year, Georgia enacted a law that regulates the use of AI and other assessment mechanisms in eye exams.

Finally, some 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.[139] New Jersey's governor issued a new training requirement for state employees on responsible AI use.[140]

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 and the use of generative AI for non-

consensual sexual imagery. Many laws 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.

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.

A Lack Of Specificity 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 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 content.[141] Vagueness in the California AADC's "duty of care" language 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.

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 LGBT content is "harmful" sexual content that a duty of care would mandate limiting exposure to.[142] This threat has led to a loss of support among some who have historically worked toward advocating for a healthier online environment.[143]

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.[144] 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."[145] Indeed, in anticipation of 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 Unintended Negative Consequences

Some laws use broader language in order to be able to adapt to future technologies,[146] 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[147] and legislators have proposed the idea of imposing a chronological feed.[148] However, recent experimental data[149] suggests that chronological feeds may not be beneficial, as it incentivizes hyper-posting, which is often done by problematic actors.[150] New laws continue to propose the removal of algorithms,[151] 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 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 narrow community standard based definition of harm. Platforms are also unlikely to be neutral arbiters as to the risks and harms inherent in their product design choices. 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.[152] Since regulatory bodies are often under-staffed with regards to the research needed to turn general principles into specific rules, it seems unlikely that future iterations of these reports will make a material impact on improving technology's impact on society. Work is currently being done to make the requirements for these reports more specific,[153] but expecting companies to identify risks themselves may predictably continue to lead to disappointing results without more specific guidance from society.

Age Verification Needs to be Done in a Manner That Respects Privacy and Free Expression Concerns

Legislators have been focused on a bipartisan desire to protect children, but 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.[154] 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.[155]

Potential Constitutional Challenges Require the Inclusion of Alternative Mechanisms to Enforcement

Recently, the California Age Appropriate Design Code was enjoined.[156] While many disagree with the broadness of the ruling, which could be read as invalidating almost any compelled design, transparency, or privacy law, 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,[157] even as others disagree with that interpretation.[158]

Other legal decisions[159] suggest that some aspects of design governance are enforceable, while others are not. For example, in one recent decision,[160] 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.[161] Still, the law is unsettled and a robust legislative strategy would include non-coercive ways to improve technology's impact on society.[162] 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. 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,[163] 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.[164] It is established knowledge at companies that very few people use any user control,[165] so 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.[166]

Banning Social Media Platforms for Youth Has Both Pros and Cons

Several jurisdictions[167] have responded to the challenges imposed by social media companies by imposing or proposing bans. A social media ban would almost certainly reduce usage and therefore harm from emerging technologies to youth. Per a University of Chicago study,[168] 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 a ban.

However, experiences with technology platforms and social media are not heterogeneous.[169] Any enforcement of a hard age-gated ban is going to require collecting data on age, which will lead to privacy concerns and have a chilling effect for adults who do not want to identify themselves when accessing certain apps or information.

Policies Relating to Content Have Been Ineffective, and Have Led to Both Opposition Related to Potential Misuse and to 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[170] or internally.[171] Even in cases where platforms have concentrated their moderation efforts, such as in wars or elections,[172] issues have remained rampant.[173] 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.[174] 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[175] and the left.[176]

Efforts to moderate content externally have led to similar issues. Opponents of the California Age Appropriate Design Code have argued that it should be enjoined partially because it could be seen as regulating speech.[177] Consequently, it must be made clear that any proposed law is content agnostic, as this is important for surviving potential constitutional challenges. Recent laws concerning ideological bias in content moderation[178] have been appealed to 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."[179] What's more, a recent 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.[180]

A Design Focus Has Been Impactful Both Within Companies and In Legislation

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[181] or changing algorithmic incentives away from certain kinds of engagement such as reshares.[182] 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.[183] YouTube turned off default Autoplay for users under the age of 18.[184] Tiktok[185] and Instagram[186] removed the ability of strangers to contact teens by default. Critics of the Kids Online Safety Act have been more amenable to design changes,[187] suggesting that a focus on design could lead to reduced opposition.

Section Four: Policy Recommendations

The above section suggests that design focused legislation that provides the right level of specificity could lead to legislation that is both effective and that engenders reduced opposition. It suggests that future legislation should mandate defaults, rather than requiring "opt-in" choices. Rather than banning youth from online platforms, legislation could 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 design focused mandates could lead to legal challenges, we further recommend a modular, fully severable law that also includes non-mandated 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 USC 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.[188] 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.

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.[189] 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, which would protect those who want

protection, which surveys indicate includes the majority of Americans and parents, but not 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 "Dark Patterns" Within Platform Design
   a. Ban Design Features (e.g. optimizing for time spent, infinite scroll, auto-play, aggressive notifications) 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, Especially for Sexual Content
   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 Dark Patterns

III. Mandate User and Parent Empowerment via Consumer-Friendly Device-Based Defaults

IV. Track Technology Platform Specific Impact on User Experience

V. Mandate Interoperability to Encourage Consumer Choice

VI. Mandate Usage Limits and Education within Schools

I. Ban "Dark 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." Dark 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.[190] They often affirmatively increase or create risk, which can be measured by experimental data from platforms themselves.[191] While the Minnesota Attorney General's Office has the authority to address dark 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 legislation would enable more certainty for technology businesses and regulators, as well as streamline the Office's enforcement efforts. 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 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,[192] 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.[193] It has broadly been able to address dark patterns relating to false beliefs, lack of disclosure of material information, unauthorized costs, and design elements that obscure privacy choices.[194] While a focus on design still could lead to First Amendment challenges, at least some scholars believe that design-based approaches are indeed constitutional.[195] 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.[196] The specific design features to address are further enumerated below.

a. Ban Design Features (e.g. optimizing for time spent, infinite scroll, auto-play, aggressive notifications) That Encourage Greater Usage for Children Beyond Their Explicit Desires. Offer All Users Accessible Tools to Limit Their Platform Usage

There are many 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) rather than to the explicit choices or experience of users. Legislation should require accessible user interfaces that allow users to control features that incentivize greater usage. 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, and automatically playing content rather than waiting for users to indicate that they want to consume more. Aside from the examples provided above, legislation can lean on the extensive literature on revealed versus stated preference[197] 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,[198] 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[199] 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 self-identification as outlined later in our recommendations). Indeed, some teens report feeling that platforms are manipulative[200] and therefore create extra barriers for themselves[201] 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,[202] 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, Especially for Sexual Content

Businesses have an incentive to make information publicly accessible as content to other users, even when users may have chosen otherwise. 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.[203] Few users are willing to change their defaults. Users care about privacy[204] but often do not understand enough about their choices to provide consent,[205] 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 legislative language to address future challenges that incorporate 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[206] and that exploits children.[207] Platform-specific legislation can further protect against the misuse of images of minors or non-consenting adults, by prohibiting the distribution of sexualized images (defined by context and not necessarily requiring nudity)

without affirmative consent. AI makes it easy to manufacture such imagery and as such, strong legislation that prohibits the public distribution of sexually explicit content depicting individuals who do not explicitly provide permission is needed given that anyone can now generate 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[208] 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 banning optimizing important/sensitive content for engagement that is not explicitly related to users' stated preference, with an emphasis on content that users perceive to be "sensitive." 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 novel 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[209] can help adjudicate when algorithms are indeed optimizing for explicit stated preference.

To avoid constitutional issues with the government defining "sensitive," companies should anchor on user perceptions of areas where engagement optimization leads to worse user experiences. Any content that depicts or is posted by minors would clearly qualify. To date, there is precedent that this would also encompass discussions of health and politics,[210] but we would anticipate other areas of importance to emerge as well, such as discussions of crime, religion, sexuality, finance and other topics where trustworthy information is critical. This will reduce bullying and harassment, given that heated discussions of such topics 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.[211] If definitions of "sensitive" prove problematic or difficult, we recommend banning all engagement "revealed preference" based optimization in feed algorithms that are not related to explicit stated user preference. This will increase, but not eliminate, the chances that these changes will be deemed not to violate the First Amendment, as the mandate will cover conduct, not content.

In place of engagement based optimization, algorithms should prioritize content and actors that varied users explicitly state a desire for. *Prioritize* means that these actors would get greater relative distribution. User interface elements[212] should be created that allow users to easily and explicitly indicate content they do or do not want, and platforms should be mandated to respect those users' explicit preferences even if contradicted by users' engagement. Facebook's "see more / see less" options[213] are an example of asking for stated preferences. *Varied* refers to a set of users who have minimally different behaviors and histories online. This is meant as a low bar involving individuals who exhibit some degree of differential behavior, rather than requiring universal trust, which would unnecessarily stifle dissent. The goal is to make information spaces more robust to withstand manipulation by extremely narrow groups that may be seeking to manipulate others. Rather than defining exactly how to define varied, we suggest mandating that platforms publish their definition of varied and how they use that definition in their algorithms. Signals of diverse approval have proven useful across

domains in identifying actors that can be trusted and that are perceived to be higher quality and less harmful to other users[214] such that most any shift of public distribution towards the preferences of varied users is likely to have ecosystem and quality benefits.

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.[215] 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.[216] Contrary to marketing that suggests that social media democratizes voice,[217] a lack of reasonable rate limits often allows a small group of motivated partisans to dominate a conversation.[218] 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.

II. Mandate Transparency of Product Experimentation That Can Illuminate New Harmful Dark 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.[219] Platforms already run numerous 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, users' indications they want to "see less" content, views of content later deemed to be policy violating) that would be required to be included.

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.

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,[220] Microsoft,[221] and Apple[222] 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.

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 this 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 and for youth who share devices with adults to voluntarily self-identify as youth in order to receive more restrictive design defaults.

Content-based controls could be considered in legislation, but have both pros and cons, as it may be difficult to enforce any restrictions in a manner that is acceptable to broad groups and that also does not trigger constitutional scrutiny. Ideally, content-based controls should focus on restrictions that are less controversial (*e.g.*, violence, pornography, gambling) and have broader buy-in. One potential solution would be to mandate the ability to outsource parental content controls to trusted sources, such that parents could choose to follow providers like Common Sense Media's recommendations. In that way, the government would be removed from any content level decision making. To insulate design level changes from any potential legal challenges, we would recommend separating out design mandates from any mandate that could be considered relating to content.

IV. Track Technology Platform Specific Impact on User Experience

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. For example, USC's Neely Center has been replicating internal platform research[223] on user experience, by surveying a representative sample of users as to their positive and negative experiences across platforms.[224] The results have been used by the press[225] 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.[226] Recent Senate testimony[227] 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 governments 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 can be especially helpful for mitigating harm due to the increasingly ubiquitous use of AI outside of social media recommendation algorithms. In initial analyses, under 20 percent of people report using generative AI systems,[228] with most of them using it out of curiosity and few using them for companionship or mental health. But as the public's familiarity and access to generative AI systems grow, we should understand both positive and negative experiences across platforms for these new technologies, to mitigate risks before they become widespread.

V. Mandate Interoperability to Encourage Consumer Choice

Many consumers would prefer to leave platforms that engage in product design decisions they don't like, but are locked in by network effects,[229] 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.[230] 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 bill,[231] that would allow users to continue to access data from others in their network, even when they are not using a specific service. 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,[232] and civil society groups like New_Public, which curates a directory[233] of smaller technology platforms seeking to create prosocial spaces. 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.

VI. Mandate 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. A recent Florida law[234] provides ideas including:

- Education about the responsible use of social media and emerging technologies.
- Prohibiting the use of and access to services deemed unsafe during instructional time.
- Limiting the use of wireless communication devices during instructional time.

Notably, this bill does not mandate a specific policy, but rather mandates that individual school districts adopt policies that achieve these goals with room for individual districts to enact locally sensitive policies. Note that any such legislation should not replace avenues toward improving the design of technology platforms, but should be additive to those efforts.

Section Five: Projected Impact on the Youth Mental Health Crisis in a World of AI

In this section, we discuss the likely impact of proposed recommendations on the youth mental health crisis, especially in a world of increasingly ubiquitous AI.

There is considerable consensus that youth, including youth in Minnesota, experience reduced well-being as compared to earlier generations.[235] 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, upward 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. There are aspects of 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 design practices that encourage and promote negative experiences that the majority of users would otherwise choose to avoid.

To be clear, 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. Unfortunately, that is not the world we live in today.

The Likely Impact of AI

With greater usage of AI technologies by malicious actors, we are likely to see the ability of small groups of individuals to target and harm Minnesotans, especially youth, increase. As such, the proposed recommendations elaborated in this report are even more important to make systems robust against scaled AI-enabled "attacks."

The Minnesota Attorney General's Office, along with other state attorneys general, has been seriously concerned about the impact of AI on children,[236] specifically identifying the risks of revealing private information and enabling "deepfakes" of children's voices and images, including in sexualized contexts. 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 sexualized content, we are hopeful that the proposed recommendations would limit the systemic risk posed by current technology platforms. Such proactive risk limitation would complement existing laws that already make such content illegal.[237]

Generally, the harms that concern society about AI 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 on the accessibility of others (via privacy defaults) 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 unfair choices. Hopefully by mandating transparency of how AI training decisions experimentally affect outputs, we will gain the understanding necessary to mitigate such risk. And by tracking user experiences with these novel technologies, we will have the tools to develop new legislation as new negative experiences facilitated by these technologies arise.

Conclusion and Next Steps

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 and 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 Brooke Auxier, *Social media continue to be important political outlets for Black Americans*, Pew Research Center (Dec. 11, 2020), https://www.pewresearch.org/short-reads/2020/12/11/social-media-continue-to-be-important-political-outlets-for-black-americans/.

2 Matt Motyl, *What social media outlets are most informative and helpful to users?*, Designing Tomorrow (Jul. 28, 2023), https://psychoftech.substack.com/p/what-social-media-outlets-are-most.

3 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/.

4 *Id*.

5 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.

6 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.

7 *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.

8 Federal Trade Commission, *supra* note 6.

9 *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.

10 *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).

11 Prinstein, *supra* note 7.

12 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.

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

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

15 Erin Peebles, *Cyberbullying: Hiding behind the screen*, 19 Paediatrics Child Health 527 (2014), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4276384/#b3-pch-19-527.

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

17 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.

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

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

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

21 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.

22 Clegg, *supra* note 17.

23 Williams, *supra* note 21.

24 Savoia, *supra* note 12.

25 Anonymous, *supra* note 20.

26 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.

27 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.

28 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.

29 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.

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

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

32 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/.

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

34 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/.

35 Horwitz, *supra* note 17.

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

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

38 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).

39 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.

40 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.

41 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.

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

43 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/.

44 *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.

45 *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.

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

47 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.

48 *FBI San Francisco Warns of Inrease 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.

49 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.

50 *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.

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

52 Jeff Horwitz, H*is 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.

53 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/.

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

55 *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.

56 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/.

57 *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.

58 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.

59 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.

60 Savoia, *supra* note 12.

61 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/.

62 *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.

63 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/.

64 *Health and Health-Related Behaviors: University of Minnesota-Twin Cities Students*, University of Minnesota Boynton Health (2021), https://boynton.umn.edu/sites/boynton.umn.edu/files/2022-08/umntwincities_cshsreport_2021.pdf.

65 Emily A. Vogels and Risa Gelles-Watnick, *Teens 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/.

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

67 *Health and Health-Related Behaviors*, *supra* note 64.

68 *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/.

69 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.

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

71 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.

72 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.

73 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").

74 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.

75 Avery Hartmans, T*hese 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.

76 *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).

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

78 Drew Harwell, *Federal study confirms racial bias of many facial-recognition systems, casts doubt on theier 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/.

79 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.

80 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.

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

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

83 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).

84 *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.

85 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).

86 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.

87 *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/.

88 Online Safety Act 2023, c. 50 (Eng.).

89 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/.

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

91 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.

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

93 *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/.

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

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

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

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

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

99 *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.

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

101 *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).

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

103 68th Montana Legis. Sess., SB0419 (banning TikTok), https://leg.mt.gov/bills/2023/billpdf/SB0419.pdf.

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

105 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.

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

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

108 *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.

109 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.

110 *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.

111 *Id.*

112 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.

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

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

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

116 *Id.*

117 *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.

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

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

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

121 Utah Code Title 13, Chapter 63.

122 *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-media-giants-sues-utah-over-parental-consent-law/.

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

124 *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.

125 *See, e.g., id.*

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

127 *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/.

128 *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*.

129 Such bills have also been 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).

130 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/.

131 *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.

132 *Artificial Intelligence 2023 Legislation*, National Conference of State Legislatures (last updated Jan. 12, 2024), https://www.ncsl.org/technology-and-communication/artificial-intelligence-2023-legislation.

133 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.

134 Assem. Bill 331, Cal. Leg. (2023).

135 *See*, B25-0114, Council of D.C. (2023); S. 1402, 220th Legis., (N.J. 2022).

136 *See*, S. 21-169, Gen. Assemb. (Colo. 2021).

137 H.R. 5141, 102nd Leg. (Mich. 2023).

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

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

140 *Governor Murphy Announces New Policy to Promote State Employees' Responsible Use of Generative Artificial Intelligence*, State of New Jersey Governor Phil Murphy (Nov. 17, 2023), https://www.nj.gov/governor/news/news/562023/20231117a.shtml#:~:text=The%20new%20policy%20focuses%20on,or%20data%20is%20shared%20or.

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

142 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.

143 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.

144 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/.

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

146 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.

147 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.

148 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.

149 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/.

150 Matthew Hindman, Nathaniel Lubin, and Trevor Davis, *supra* note 34.

151 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.

152 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/.

153 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/.

154 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.

155 *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/.

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

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

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

159 *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).

160 *See id.*

161 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.

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

163 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.

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

165 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).

166 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/.

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

168 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.

169 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/.

170 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.

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

172 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.

173 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/.

174 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.

175 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.

176 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.

177 *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.

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

179 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/.

180 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.

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

182 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/.

183 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.

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

185 *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.

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

187 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/.

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

189 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/.

190 Federal Trade Commission, *supra* note 6, 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".

191 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.

192 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/.

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

194 Federal Trade Commission, *supra* note 6.

195 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.

196 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/.

197 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.

198 *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.

199 Prinstein, *supra* note 7.

200 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.

201 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.

202 Radesky *et. al*, *supra* note 204.

203 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.

204 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.

205 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/.

206 *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, https://theconversation.com/online-abuse-could-drive-women-out-of-political-life-the-time-to-act-is-now-214301.

207 Jeff Horwitz and Katherine Blunt, *supra* note 29; *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/.

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

209 Kraus, *supra* note 200.

210 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.

211 *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.

212 User interface elements are features that allow users to interact with platforms. For example, Meta's "see more / see less" is an example of such an interface, though it is one that could be made far more accessible.

213 Mia Sato, *Facebook adds 'show more' and 'show less' controls to adjust what you see on your Feed*, The Verge (Oct. 5, 2022), https://www.theverge.com/2022/10/5/23388970/facebook-show-more-show-less-settings-newsfeed-recommendations.

214 Plurality Institute, *Plurality Spring Symposium 2023*, YouTube (June 24, 2023), https://www.youtube.com/watch?v=kkIVDWF26I4&list=PL93kCkGKjJQq8ZRe9SktYO81F2zF58zCr&t=6600s.

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

216 Matthew Hindman, Nathaniel Lubin, and Trevor Davis *supra* note 34.

217 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.

218 Matthew Hindman, Nathaniel Lubin, and Trevor Davis, *supra* note 34.

219 Nathaniel Lubin and Ravi Iyer, *supra* note 194.

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

221 *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.

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

223 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.

224 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.

225 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.

226 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.

227 Justin Hendrix, *supra* note 195.

228 Matt Motyl, Nathanael Fast, and Jimmy Narang, *Tracking Chat-Based AI Tool Adoption, Uses, and Experiences* (Jan. 11, 2024), https://psychoftech.substack.com/p/tracking-chat-based-ai-tool-adoption.

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

230 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/.

231 S.6686, 2023-2024 Leg. Sess., (N.Y. 2023).

232 *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/.

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

234 H.R. 379, Gen. Assem. (Fla. 2023).

235 *See Health and Health-Related Behaviors, supra* note 64, discussing how Minnesota college students report more poor mental health days than adults.

236 *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.

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

The Office of the

Minnesota Attorney General

helping people afford their lives and live with dignity, safety, and respect

445 Minnesota Street, Suite 1400, 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