FALLING DOWN RABBIT HOLES:
THE IMPACT OF BIG TECH ON KIDS

Tom Kemp

In the fall of 2021, reporters with the Wall Street Journal

decided to experiment and see what it would be like to experience TikTok as children aged thirteen to fifteen. To do this, they created a few dozen automated accounts that simulated teen users and programmed them to browse TikTok's For You feed, which is TikTok's feed of never-ending short videos.

Unfortunately, the reporters soon discovered that TikTok's underlying AI systems drove the minors' accounts into "rabbit holes" of "endless spools of adult content." For example, one account registered as a thirteen-year-old saw 569 videos about drug use. Collectively the accounts saw over one hundred videos recommending pornography sites, plus other videos encouraging drinking and eating disorders.

Social media should not create rabbit holes for us to fall in, let alone ones as explicitly dangerous as these. While adults may be able to navigate around or climb out of these rabbit holes, it is much harder for kids, primarily because our brains typically don't fully mature until we are in our mid-twenties.

Moreover, kids find it even more challenging to resist staying online because they lack critical cognitive capabilities. This is especially the case when kids face a nonstop selection of extreme and inappropriate videos that are continuously being algorithmically selected to maximize engagement.

Studies have also shown that children have difficulty determining what's an ad and what's not. They also don't fully understand what they should and should not share online. The teen years are when kids undergo neurological changes that promote the heightened desire

for social attention and feedback, which we already know are vulnerabilities that online businesses can and do exploit.

This exploitation of kids' developmental vulnerabilities is an increasing concern, especially given kids' growing use of online services and mobile devices as we come out of the Covid-19 pandemic.

An estimated one in three internet users is a child. Researchers have also estimated that children under the age of eight now consume two and a half hours of digital media per day, while teens spend, on average, over seven hours per day of screen time that is non–school related.

In addition, over two-thirds of kids aged five to eight have their own tablet, and 94 percent of households with children between eight and eighteen have access to a smartphone. And social media usage by kids is also extensive. For example, with US teens aged thirteen to seventeen, as of mid-2022, over 95 percent use Google's YouTube, 67 percent use TikTok, 62 percent use Meta's Instagram, and 59 percent use Snapchat.

Kids' unique vulnerabilities, combined with their widespread use of technology and social media, must be considered as we look at the increasing mental health issues associated with kids. For example, studies have shown that depression rates among teenagers have doubled between 2009 and 2019, and suicide is now the second leading cause of death among US youth. Tragically, the suicide rate among young people aged ten to twenty-four in the US has increased by 57 percent between 2007 and 2018. In addition, emergency room visits for teen girls aged twelve to seventeen years old that involve eating disorders have doubled from 2019 to 2022.

Researchers have pointed out that the increase in youth mental health issues is attributable to many factors. Still, the growing use of social media and its corresponding exposure to harmful content, unhealthy social comparisons, and cyberbullying have exacerbated the above trends.

Kids' unique vulnerabilities, combined with their widespread use of technology and social media, must be considered as we look at the increasing mental health issues associated with kids.

For example, as revealed in the "Facebook Files," Meta's internal research shows how toxic Instagram could be for teen girls. Internal Meta presentations documented how "aspects of Instagram exacerbate each other to create a perfect storm" that sends struggling kids into a "downward spiral" in which "mental health outcomes . . . can be severe."

And even the American Psychological Association noted that while "Instagram, YouTube, TikTok, and Snapchat have provided crucial opportunities for interaction . . . they've also been increasingly linked to mental health problems, including anxiety, depressive symptoms, and body image concerns."

LEGISLATION

There has been increased activity in Europe and the US to protect kids online. As has been the case with privacy, regulation of AI, and cracking down on abuses of persuasive technology, Europe is taking the lead. Still, California has also taken a significant step forward while US federal law lags.

European legislation

The regulatory environment around protecting children on the internet has increasingly centered around the concept of "age-appropriate design." Pioneered by the 5Rights Foundation, its regulatory approach to kids' online safety "is to consider the privacy and protection of children in the design of any digital product or service that children are likely to access." Thus, tech companies and Big Tech, in particular, are being asked to consider the impact and potential harms of the design of their products on children.

The 5Rights Foundation championed the UK's Age Appropriate Design Code (AADC). It is not a new law per se but regulations and guidance from the UK's data protection authority—the Information Commissioner's Office (ICO)—that went into effect in 2020. It provides a set of fifteen standards that act as a set of "technology-neutral design principles and practical privacy features" aimed at protecting kids under eighteen in the digital world.

The achievements by the UK's AADC have been impressive, and a wide range of online services have made hundreds of changes, including these by Big Tech firms:

- Google's YouTube turns off autoplay for under eighteens and has turned on by default break and bedtime reminders.

- The Google Play Store prevents under-eighteens from being able to view and download apps rated as adult-only.

- Google lets anyone under eighteen request their images be removed from Google's image search.

- TikTok and Meta's Instagram have disabled direct messaging between kids and adults they do not follow.

- TikTok does not push notifications after nine p.m. to children aged thirteen to fifteen and after ten p.m. to sixteen and seventeen-year-olds.

- Meta has updated its policies limiting ad-targeting for kids under eighteen based on age, gender, and location.

In addition, enforcement of the UK AADC has begun, as evidenced by the announcement by the UK ICO in the fall of 2022 that it intends to fine TikTok £27 million for alleged children's violations.

Moving on to the European Union, Europe's comprehensive privacy law—the General Data Protection Regulation or GDPR—requires parental consent for data collection of kids under sixteen. Furthermore, European regulators are now cracking down on privacy and other online child safety issues.

Social media should not create rabbit holes for us to fall in, let alone ones as explicitly dangerous as these.

For example, Ireland's Data Protection Commission (DPC), the regulatory agency responsible for enforcing the GDPR in Ireland, fined Meta €405 million in the fall of 2022 for making children's Instagram accounts public by default based on an inquiry it made in 2020. In response to this investigation, Meta made updates in 2021 to Instagram to make kids' accounts private by default and to block adults from messaging children who don't follow them.

Finally, the European Union passed the Digital Services Act (DSA) in 2022, which enforces more strict content moderation, bans "dark patterns" and other persuasive techniques that trick users, and entirely bans behavioral advertising to children under eighteen years of age. The DSA will come into effect by 2024.

US state legislation

The most significant state law for kids' online safety that has passed is the California Age-Appropriate Design Code (Cal AADC). It was signed into law in the fall of 2022 and will go into effect in 2024. It was also sponsored by the 5Rights Foundation and is modeled on the UK's code with the same name.

Key to the bill is a focus on online services that are "likely to be accessed by children," not just services specifically aimed at kids. In addition, the Cal AADC puts significant "privacy by design" obligations on online services, including the following:

- Stop selling kids' data and restrict data from being collected from them.

- Restrict profiling of children in ways that are either risky or harmful to kids.

- Set the highest level of privacy settings by default.

- Switch off geolocation by default for kids.

- Document in a Data Protection Impact Assessment whether the service uses persuasive technologies that extend the use of the service via autoplay, rewards for time spent (e.g., streaks), and notification or nudging.

- Provide tools to report privacy concerns and flag inappropriate behavior.

This landmark law also extends the protection of children using online services beyond what is currently offered by the federal children's privacy law that is now in place—the Children's Online Privacy Protection Rule (COPPA).

For example, the Cal AADC protects children up to eighteen, while COPPA applies only to kids under thirteen. Cal AADC also ensures that kids receive better protection regarding data collection and default privacy settings. It also provides visibility into the impact of AI systems that can cause addictive behavior.

The Cal AADC is another example of the "California effect." It will likely force Big Tech firms to offer these kid-friendly designs in their products for the entire US, as it will be costly to offer one solution for kids in California versus the rest of the US.

However, Big Tech is not going quietly in terms of accepting the Cal AADC. NetChoice, an industry trade group representing tech companies such as Amazon, Google, Meta, and TikTok, sued the State of California in December 2022 over the AADC. NetChoice claimed in its lawsuit that the AADC was unconstitutional in allegedly violating these companies' First Amendment rights by infringing on the editorial rights over their websites and apps.

US federal legislation

The Children's Online Privacy Protection Act (COPPA) was enacted in 1998 and empowered the Federal Trade Commission (FTC) to issue and enforce regulations concerning kids' online privacy. The goal of COPPA is to give parents consent over what personal information is collected from their children under the age of thirteen. Parents can also request their kids' data be deleted or made available for review and request that their kids' data not be made available to third parties.

COPPA applies to online services and websites directed to children under thirteen or to "general audience" online services and websites that have "actual knowledge" the user is under thirteen. These services must enforce data minimization by collecting only reasonably necessary data and retaining collected data for only as long as needed to fulfill the purpose for which it is collected.

The FTC has only enforced COPPA forty times through 2022. The vast majority of the fines have been in the sub-$1 million range. However, the largest COPPA penalty of $275 million was levied in December 2022 against Epic Games, the maker of the Fortnite video game, for illegally collecting personal information from children without parents' consent. The second largest fine of $170 million was imposed in 2018 against Google's YouTube for a similar allegation.

The good news is that the need for kids' online safety has reached national consciousness.

Privacy advocates have many concerns with COPPA, including that it does not cover kids from thirteen to eighteen, does not address addictive design issues, has had spotty enforcement, and many "general audience" online services are claiming they don't have "actual knowledge" of kids using their service. Hence COPPA "Version 2"–the Children and Teens' Online Privacy Protection Act–was proposed in 2021.

One of the sponsors of this new bill, Senator Ed Markey, was one of the authors of the original COPPA. It would cover teens up to sixteen and outright ban behavioral advertising for those under sixteen. It would also close the "actual knowledge" loophole by creating a new "constructive knowledge" standard that requires online services to determine if kids are accessing their services. It would also set up a Youth Marketing and Privacy Division at the FTC to put more weight behind enforcement. And it would create an "eraser button" that would make it easier to delete information.

The Kids Online Safety Act (KOSA) was proposed in 2022 by Senators Richard Blumenthal and Marsha Blackburn. Like the AADC, it would require online services to prioritize kids' well-being and best interests when designing their services and have the most robust default privacy settings for kids.

In addition, it would require audits that assess the risks to children of online services' AI systems and would need those services to provide parents with more tools to protect their kids' privacy. And these online services would need to reduce the impact of potentially harmful content on their platforms. Finally, online services would be required to open up "black box" algorithms to academics and nonprofits to assist in research on the harms of AI systems to kids.

The Protecting the Information of our Vulnerable Children and Youth (PRIVCY) Act was introduced in 2021 by Representative Kathy Castor. It also builds upon the AADC by requiring sites likely to be accessed by children to have the best interests of children in mind and also requires risk assessments of AI systems. Like the COPPA version 2 proposal, it too establishes a Youth Marketing and Privacy Division at the FTC and bans behavioral advertising for kids under eighteen. Finally, it lets parents sue tech firms if they violate kids' privacy rights.

Lastly, the Kids Internet Design and Safety (KIDS) Act was introduced in 2021 by Senators Ed Markey and Richard Blumenthal and Representative Kathy Castor. It would "stop online practices such as manipulative marketing, amplification of harmful content, and damaging design features, which threaten young people online." For example, it would ban persuasive and addictive technologies such as autoplay, nudges, and streaks while eliminating likes and follower counts for children.

Despite strong support from consumer protection groups, all of these federal bills have failed to move forward as of the end of 2022.

Road map to contain the impact of Big Tech on kids

One may conclude that the best way forward to protect kids online is to avoid having kids use technology. But in today's modern age, that is not practical or possible, especially given our dependence on products from Big Tech firms and the reality that the digital world is a necessary and significant part of our kids' lives. To prepare young people for a world in which AI will automate many jobs, we want and need kids to be tech literate and savvy. But we also want to keep them safe.

The good news is that the need for kids' online safety has reached national consciousness, and laws are being passed in Europe and at the US state level. In addition, there is a push to get laws passed at the US federal level, as evidenced by President Biden's 2022 State of the Union speech.

He stated, "We must hold social media platforms accountable for the national experiment they're conducting on our children for profit." He added, "It's time to strengthen privacy

protections, ban targeted advertising to children, demand tech companies stop collecting personal data on our children."

I agree.

We should pass comprehensive privacy legislation that, among other capabilities, limits data collection to what is needed to perform the necessary task, bans selling kids' data, and bans behavioral advertising targeting children.

President Biden also added to his list the need for safety by design for kids in his 2023 State of the Union address, which I agree also needs addressing. For children, this means that autoplay and notifications are off by default, included is support for save buttons (so kids don't have to continue to stay online to complete a given task), and no more encouraging or rewarding streaks or the number of likes and followers.

In addition, kids' geolocation should be off by default, and their privacy settings should be set to the highest levels. And, of course, eliminate dark patterns for everyone. So, implementing the AADC at the national level makes sense.

Online services should also be required to perform Childhood Impact Assessments and audit their AI systems for potential harm if their products are likely to be accessed by children. Furthermore, the data sets from these "black boxes" should be accessible to academics and nonprofits to facilitate research regarding the harm to the well-being and safety of kids.

We also need to fund more research on the mental health impact of technology use and kids. The passage of the Children and Media Research Advancement Act (CAMRA) bill at the

end of 2022 is a significant first step. This law requires the Department of Health and Human Services (HHS) to study the impact of social media and smartphones on children and teens.
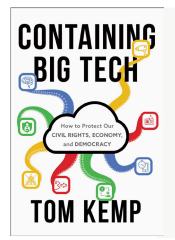
We should raise awareness of screen addiction and cyberbullying by having public service announcements (PSA) akin to the PSAs for tobacco. School districts should also seek to add discussions of screen addiction and cyberbullying to their health courses taught at schools.

In summary, strengthening our privacy laws and requiring online platforms to design their services with kids in mind would shift Big Tech and other tech firms from focusing on kids' time spent on their platforms to time well spent. And we need to redesign digital services that children use with their vulnerabilities in mind to support their well-being versus interfering with it.

We have booster seat laws for children in cars, lead paint laws, and countless other regulations for childhood safety in the physical world, so it makes sense to have the same in the digital world, **and it should start with the most prominent tech players.** ⬚

Info

Ready to dig deeper into the book?
Buy a copy of <u>Containing Big Tech</u>.

Want copies for your organization or for an event?

We can help: customerservice@porchlightbooks.com

800-236-7323

ABOUT THE AUTHOR

Tom Kemp is a Silicon Valley–based CEO, entrepreneur, and investor. He has served as a technology policy advisor for political campaigns and advocacy groups, including leading the campaign marketing efforts in 2020 to pass California Proposition 24—the California Privacy Rights Act (CPRA)—and co-drafting bills such as the California Delete Act of 2023. Tom writes extensively on technology policy on his blog (tomkemp.ai) and has been interviewed by the *Guardian, Politico, the Washington Post, CNBC, Fox News*, and others. Tom holds a bachelor of science degree in computer science and in history from the University of Michigan. You can follow Tom on Twitter at @TomKemp00.

SHARE THIS
Pass along a copy of this manifesto to others.

SUBSCRIBE
Sign up for e-news to learn when our latest manifestos are available.