Zachary Lilly
Deputy Director of State & Federal Affairs, NetChoice
1401 K Street NW, Ste 502
Washington, DC 20005

NetChoice
Defending Free Speech and Free Enterprise Online

COMMENT FOR THE RECORD

NetChoice Comments to NTIA on Kids Online Health & Safety

NetChoice is a trade association of leading internet businesses that promotes the value, convenience, and choice that internet business models provide American consumers. Our mission is to make the internet safe for free enterprise and for free expression. We also work to promote the integrity and availability of the internet on a global stage, and are engaged on issues in the states, in Washington, D.C., and in international internet governance organizations.

Introduction

The National Telecommunications and Information Administration (NTIA) seeks to learn more about social media and online platforms' impacts on minors, current industry practices, and ways in which the private sector, caregivers and the U.S. government may counter negative effects. We commend NTIA's focus on leveraging its unique role as a convener of various stakeholders to learn more about this topic. It is of vital importance to better understand the best ways to keep America's young people safe online. It is similarly pressing to ensure that these "solutions" don't have even worse privacy and security risks attached.

NetChoice's comments will focus on the information requested by NTIA. We wish to highlight in particular:

- The practices some of our members employ to keep kids safe online;
- The major gap that exists between online reporting and resources for law enforcement;

- How many government-mandated online "safety" provisions have already been deemed unconstitutional attempts to regulate online speech;
- That those same government-mandated "safety" provisions have major privacy and security ramifications for minors; and
- Proposals that can both keep kids safe and respect the constitutional rights of every American.

With that in mind, we would like to provide the agency with the following input regarding its request for comments.

How Companies Keep Kids Safe on their Platforms

NetChoice's members include thirty five companies from all corners of the internet ecosystem. Retailers, social media platforms, transportation companies, and hospitality sites all depend on building trust with their customers. A big part of that trust means making sure that the company's site is safe and secure. Social media platforms in particular to take steps to enhance user safety and build in guardrails to protect younger users. Commercially viable online platforms don't want to be known for being unsafe or a haven for illegal and disturbing content. Advertisers don't want their brands listed next to offensive content, and most users don't want to expose themselves to it either.[1]

NetChoice regularly publishes the topline content moderation numbers from our social media members.[2] This helps policymakers get a better sense of just how seriously companies take their responsibility to their users and how challenging of an issue content moderation is. While our most recent report is still forthcoming, our different members publish their content moderation numbers independently.

Platforms like TikTok, Reddit, YouTube, Instagram, X, and Snap all have specific content moderation policies related to child safety, child abuse, or child sex abuse material (CSAM). In the first quarter of 2023, 30.6% of the videos removed on TikTok were related to the safety of minors, making it the largest subset of videos removed across the platform.[3] Snap enforced 548,509 reports of CSAM and reported 292,489 submissions to NCMEC on top of

[1] Hatespeech and Digital Ads: The Impact of Harmful Content on Brands, CCIA, Sept 2023
[2] By the Numbers: What Content Social Media Removes and Why
[3] Community Guidelines Enforcement Report, TikTok, Q1 2023

millions of enforcement actions for content violating the company's policies on sexual content, self-harm, bullying, and drugs. Of the CSAM Snap enforced against, 98% of it was found and removed proactively using detection technology.[4] From January until June of this year, Youtube removed 196,477 channels related to child safety concerns.[5] 34.1% of the individual videos removed from YouTube from April to June were related to violations of the company's child safety policy. The vast majority of individual videos were removed using Google's own automated flagging technology, and 73.4% of those videos were removed before garnering more than 10 views.

There is an enormous amount of this data publicly available and they paint a clear picture of innovative companies leveraging significant resources and new technologies to identify bad behavior and keep their users safe.

That technology is also leveraged on the user-facing side of platforms. Content filters, parent guides, family discussion resources, and other tools are available to better protect young people across the digital ecosystem.

The Competitive Enterprise Institute recently published a list of the online safety tools that exist for parents, a much needed compendium whose absence has fed many misconceptions about the role child safety plays in digital products.[6] This list links to the parental controls for: nine social media sites, eight video game services, thirteen streaming services, five operating systems, four web browsers, eighteen standalone tools, five home networking products, and seven internet service providers. That is a total of at least sixty-four tools and services available to parents to control what online content is best for their children.

Many states have considered mandating certain types of parental filters come baked in at the device level. Besides carrying with them worrying First Amendment implications, these types of bills ignore the enormous amount of innovation in this space. Technology companies should continue to be able to experiment with and expand their offerings in order to most effectively keep their users safe and meet the specific needs of families and caregivers.

---

[4] Transparency Report, Snap, Jan-June, 2023
[5] Google Transparency Report, YouTube Community Guidelines enforcement, 2023
[6] Children Online Safety Tools, Competitive Enterprise Institute

Empowering Law Enforcement to Bring Online Predators to Justice

It is difficult to look at the numbers related to online child sex abuse material (CSAM) and conclude that we don't have an enforcement problem in this country. NetChoice member companies pass on to law enforcement billions of actionable CSAM tips a year with that number steadily climbing year-to-year. The number of arrests and prosecutions, however, have remained, statistically, near zero.

The United States Sentencing Commission's fiscal year 2021 data shows that reporting of CSAM jumped 18.8% over the previous year, though the number of offenders stayed statistically flat over five years.[7] FY22 shows a slight increase in convictions, though not enough to break the statistical stagnation of the preceding years. Compared to the numbers that NetChoice members and other companies are reporting to law enforcement and the National Center for Missing and Exploited Children (NCMEC), a mere 1,435 offenders locked up should be a national embarrassment.[8]

To grasp the extent of the enforcement problem, we can also look at the FY 2022 data to see the types of CSAM offenders being put away. 45% of the federal CSAM offenders that year were convicted of possession, 43.9% for trafficking, and 11.1% for receiving.[9] We can safely assume that, regardless of arrests or convictions, traffickers of CSAM are in the overwhelming minority. There are far more consumers of the vile content than there are individuals creating or disseminating it. But, as we see from the federal data, traffickers and consumers of CSAM are being imprisoned at roughly the same rate, suggesting an extreme underrepresentation of CSAM consumers in the federal prison population. We should be seeing far more consumers of CSAM being locked up alongside the criminals who supply them. This disparity needs to be addressed with increased resources and coordination.

Most legislative responses to the proliferation of online CSAM have taken a confrontational approach to social media and other online platforms while ignoring traffickers. The EARN IT Act, for example, led by Senators Blumenthal and Graham, seeks to strip away

[7] US Sentencing Commission, Report: Fiscal Year 2021 Overview of Federal Criminal Cases
[8] US Sentencing Commission, Quick Facts FY22, Child Pornography Offenders
[9] Ibid

encryption protection and institute mandated reporting. Besides the Fourth Amendment, privacy, and cybersecurity concerns this raises, the basic fact is that the legislation doesn't address the underlying problem of enforcement. Unfortunately, while the EARN IT Act has been repeatedly reintroduced year after year, the bill sponsors have refused to address the major concerns from industry, academia, and civil society. Instead of pursuing solutions everyone can agree on, Congress is trapped in a cycle of unending political theater.

Real solutions exist. Senator Wyden's Invest in Child Safety Act directs federal resources towards the identification, enforcement and eventual prosecution of criminals related to CSAM. If we were able to bring together the mountain of material directed towards NCMEC by online platforms with a sufficient law enforcement capacity, the number of criminals arrested and sent to prison would skyrocket. As of now, with all the focus squarely on reporting from online platforms and not the actual criminals, no deterrent against CSAM and other exploitative crimes meaningfully exists.

Unintended Consequences: The Shortcomings of Age Verification

Age verification has been the policy dejure for lawmakers at the federal and state levels looking to improve online child safety. Unfortunately, many of these proposals have been pursued in such a hasty manner that they have failed to seriously consider the clear constitutional problems presented by government-mandated age verification.

Almost by definition, government-mandated age verification creates significant constitutional problems. There is no way to adequately verify a user's age without also verifying the *identity* of that user. Therefore, when governments mandate age verification they eliminate the ability to speak anonymously.[10] This alone creates a chilling effect on speech and disincentivizes those who do not wish to verify their identities from speaking. It will also prevent those who are unable to verify their age from speaking entirely. These hurdles create an impermissible chilling effect on speech and the free exchange of ideas.

When age verification is paired with other requirements, such as a requirement that any minor receive parental consent before accessing constitutional speech, it creates separate

[10] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995)

hurdles which are themselves unconstitutional. The government may not substitute its judgment about what is inappropriate content for that of a parent. Yet, by imposing age-verification and parental consent requirements this is precisely what the government does. Indeed, these requirements impose the government's will by default—only to be overridden by parental veto.[11]

NetChoice itself has brought lawsuits on behalf of internet users and our members against the states of California and Arkansas for their poorly conceived age verification laws. We have been successful in both cases, securing preliminary injunctions against both pieces of legislation. Similarly ill-considered bills have been introduced at the federal level and in other states and contain equally unconstitutional and harmful provisions. NTIA should avoid adopting any recommendations that call for the adoption of legislation that has already been shown to violate the Constitution and the privacy of both children and adults. It is one thing to recommend the use of an age-verification service. It is another thing entirely for the government to mandate its use.

1st Amendment Violations: In both the California and Arkansas cases, NetChoice advanced the argument that the provisions of those bills represented an unconstitutional attempt to regulate speech. California attempted to argue that they were regulating conduct, not speech. Arkansas insisted that they were acting in the interest of children by regulating access to the internet rather than attempting to restrict access to speech. Both judges took their states to task. The judge in Arkansas put it succinctly: the "[l]oss of First Amendment freedoms, even for minimal periods of time, constitute[s] irreparable injury," and that there was "no compelling evidence" that children would be protected by the legislation.[12]

Privacy Violations: Both states also suggested that passing their respective age verification and speech regulation bills would improve children's online privacy. NetChoice vehemently rejected that claim. Indeed, such a claim is so at odds with the facts of the

[11] Brown v. Entm't Merchs. Ass'n., 564 U.S. 786, 795 fn. 3 (2011)

[12] US District Court, Western District of Arkansas, Preliminary Injunction in NetChoice v. Griffin

matter that one must seriously consider what was happening in the offices of the California and Arkansas Attorneys General.

For one, mandated age-verification makes no differentiation between adult and minor, since the distinction can only be made after private data has been collected, stored, and analyzed by third parties. This had the practical effect of requiring massive amounts of personal information to be forcibly taken and kept on every adult in California and Arkansas who wanted to use the internet.

For another, it mandated the same regime for children. This would have created massive data stores containing personally identifiable information of virtually every minor in those states. It does not take a mastermind to discover such information would be valuable in the hands of criminals and other bad actors. The judge in California was clear: age verification mandates are "likely to exacerbate the problem by inducing…children to divulge additional personal information."[13] Given the government's abysmal track record with privacy and data protection, the creation of these data stores should be absolutely avoided.

Policy Recommendations

While the government is extremely restricted in passing any sort of legislation that attempts to directly or indirectly affect the creation and dissemination of constitutionally protected speech, that does not mean we are powerless to protect our children from the threats they face online.

Student and Parent Education: Last year, the Florida legislature passed legislation that mandated digital literacy and safety education in Florida schools. The bill also required any curriculum that is developed and implemented in schools be made publicly available so that parents could have a better understanding of what their children are learning about good safety practices. This has the additional benefit of exposing parents more to the resources they can use to monitor and guide their children through the digital world.

[13] US District Court, Northern District of California, Preliminary Injunction in NetChoice v. Bonta

The state of Utah has taken a slightly different track, creating an entire resource website dedicated to educating the public on the best safety practices for social media and other digital services. While the state has taken a straightforwardly negative posture when it comes to these services, the website demonstrates the ways the state can act without trampling on the free expression rights of its citizens.

Privacy Legislation: We have said it before and we will continue to say it until legislation is signed by the President: America needs a comprehensive, federally preemptive data privacy law. As it relates to child online safety, many of the proposals out of the state and federal governments are directly related to an anxiety born out of a lack of clear privacy protections. If consumers better understood how they and their childrens' privacy was protected online, they would have greater confidence in online services. It would also help policymakers better understand where gaps still existed that needed to be filled. Privacy is to child safety as broadband mapping is to broadband buildouts: it should be foundational to the entire conversation. We cannot afford for Congress to remain locked in a stalemate on this issue.

Partners, Not Enemies: Remember, in any policies or programs NTIA pursues, technology companies are strong allies in the fight for improving outcomes for young people online. Similarly, online tools improve connection, boost creativity, and help kids and adolescents build skills that they will use for the rest of their lives. Recognizing the good why addressing the bad is vital in creating strategies that will actually lead to positive change. Remembering these things will help you avoid the pitfalls we regularly see of tech policy that demonizes the internet, leading to a disempowerment of users and an aggressive expansion of government power.

Conclusion

Keeping our children safe online is of paramount importance, both to NetChoice and to all its member companies. The government, when it understands its proper role, can be a great partner in that effort. We ask NTIA to view the private sector as a partner in solving problems. Too many other agencies and politicians have chosen to see platforms as obstacles

to be overcome. This has, in turn, limited the effectiveness of the proposals those agencies and politicians have crafted. It has also driven most of them towards legislation that undermines childrens' privacy and violates the First Amendment. As you go about your important work we would encourage you to remember that you cannot make a child safer by undermining the constitutional protections that they stand to fully inherit.

Thank you for your consideration of our comments.

Sincerely,

Zachary Lilly
Deputy Director, State & Federal Affairs,
NetChoice