Written Testimony of Irene Ly

Policy Counsel, Common Sense Media

Before the Ad Hoc Subcommittee on Consumer Privacy

August 23, 2022

My name is Irene Ly, and I am a Policy Counsel for Common Sense Media, where I work on privacy and platform accountability issues. Common Sense Media is the leading organization dedicated to helping kids and families thrive in a rapidly changing digital world. We help parents, teachers, and policymakers by providing unbiased information, trusted advice, and innovative tools to help them harness the power of media and technology as a positive force in all kids' lives.

Testimony Summary: Maryland should pass a strong privacy law that reduces privacy harms against children online as other states take initiative in the absence of federal legislation. Maryland has an important opportunity to be a leader in children's online privacy and should pass a strong state privacy law that protects all consumers, while giving children's data the specific additional protections it deserves. This would not only offer Maryland children unique protections, but it would encourage other states to follow suit, creating a safer online environment for more kids. Children's online privacy law must go beyond the "notice and consent" model to correct the power imbalance between parents and companies. Parents should not bear the burden of keeping their children and their personal information safe online. Instead, state legislatures should adopt data minimization principles, a targeted ad ban, deletion rights, and a knowledge standard that reflects the reality of companies' data practices today. These provisions will lay the groundwork for a safer online environment for kids to play, explore, and learn in.

Thank you for the opportunity to offer comments on this important matter.

I. Absent Federal Legislation, Maryland Must Take Initiative Like Other States and Pass Its Own Privacy Law to Protect Children

Platforms collect millions of data points of personal information about users, and with the use of emerging technologies (e.g., machine learning), they can draw inferences about users based on these data points to hypertarget them in an effort to maximize user engagement and profit. Strong privacy legislation is essential to protecting people online, particularly children, who have unique vulnerabilities, by cutting off the firehose of data that companies are unnecessarily but intentionally collecting on everyone.

A. Federal Legislation

I. Existing Legislation is Insufficient to Protect Consumers Online

Over the last two decades, there have been many attempts to pass a federal comprehensive online privacy law. However, none of these efforts have been successful, which has left states to take the initiative. To date, five states have passed an online privacy law.

If an individual does not live in one of these five states, they do not have any privacy protections over their online personal information except when their data is subject to specific federal laws, such as the Children's Online Privacy Act (COPPA) and the Health Insurance Portability and Accountability Act (HIPAA). COPPA, which protects children's online data by requiring a company to obtain parental opt-in consent before collecting information from a child under 13 years old, is a nearly 25-year old law. Over the last decade, legislators and advocates have called for it to be updated to reflect what the internet, and the harms associated with it, look like today.

II. Despite Movement, There is No Guarantee Current Proposed Federal Privacy Legislation Will Pass

This summer, two congressional committees passed bills that would improve children's online privacy. Although this progress at the federal level is promising, there is no guarantee the legislation will receive final passage. State legislators must not take a "wait and see" approach before proceeding with a state privacy bill. Maryland residents, particularly Maryland children, should not be left vulnerable to online data collection and sharing and the harms associated with it while waiting for an uncertain future of legislation in Congress.

In July, the Senate Commerce Committee passed the bipartisan Children and Teens' Online Privacy Protection Act (COPPA 2.0).[1] This bill would make several long-needed updates to

[1] Press Release, U.S. Senate Committee on Commerce, Science, and Technology, Commerce Committee Approves 2 Bills and 4 Nominations, Including Bipartisan Children's Online Privacy Legislation and OSTP Nomination (July 27, 2022), https://www.commerce.senate.gov/2022/7/commerce-committee-approves-2-bills-and-4-nominations-including-bipartisan-children-s-online-privacy-legislation-and-ostp-nomination.

COPPA, including expanding opt-in consent requirements for teens over 13 and under 17 years old, banning targeted advertising to children under 13 and requiring opt-in consent for targeted advertising for teens, requiring companies to follow data minimization principles around children's data, and replacing the current "actual knowledge" standard with a "reasonably likely to be accessed by children" standard to determine which companies must comply with COPPA. The committee also passed the bipartisan Kids Online Safety Act (KOSA), which addresses platform accountability issues, including by imposing a duty on companies to take steps to prevent or mitigate risks of harm posed to minors on their platforms.

This is encouraging, and we applaud the committee for its action, but, again, there is no guarantee that COPPA 2.0 will be completed this year.

Furthermore, even if COPPA 2.0 were to pass, a state children's privacy law would still stand. COPPA only preempts inconsistent state law.[2] Thus, states can build on COPPA's protections by passing additional protections not found in COPPA. For example, Maryland could pass a privacy bill that bans targeted advertising to all covered minors, a step we strongly recommend. This would not conflict with COPPA 2.0 because the federal statute bans targeted advertising to children under 13 while allowing it for teens under 17 years old who consent.

Meanwhile, and also last month, the House Energy and Commerce Committee passed a bipartisan comprehensive privacy bill, the American Data Privacy and Protection Act (ADPPA).[3] ADPPA includes data minimization principles and offers consumers rights to their data such as deletion and access rights, civil rights protections, and stronger children's protection provisions. Under ADPPA, opt-in consent requirements would be extended to teens over 13 and under 17 years old, targeted advertising would be banned for all covered minors, and a tiered knowledge standard would be implemented to determine when companies must comply with these protections.[4] ADPPA preempts state law and though it lays out many carveout exceptions, it does not provide one for children's privacy. Were ADPPA to become law, a Maryland children's privacy law would be preempted.

However, like COPPA 2.0, there is no guarantee that ADPPA will be approved this year. While it has been approved in committee, it is not clear when it might get considered by the full House and it has not been introduced in the Senate. Meanwhile, there are a limited number of legislative days remaining in this Congress.

---

[2] 15 U.S.C. 6502(d).

[3] Press Release, House Committee on Energy and Commerce, Bipartisan E&C Leaders Hail Committee Passage of the American Data Privacy and Protection Act (July 20, 2022), https://energycommerce.house.gov/newsroom/press-releases/bipartisan-ec-leaders-hail-committee-passage-of-the-american-data-privacy.

[4] Under the tiered knowledge standard, high impact social media companies must comply with the children's protections under ADPPA if they had constructive knowledge of children being on their platform. Large data holders need to show actual knowledge or willful disregard. All other entities need to show actual knowledge.

Despite their uncertain futures, progress on COPPA 2.0 and ADPPA this year demonstrates strong bipartisan interest in comprehensive privacy, and children's privacy issues in particular. Maryland and other state legislatures must forge ahead with efforts to pass strong privacy laws that protect children's data and the harm we know is associated with its inappropriate and unnecessary collection, storage and sharing.

B. State Legislation

In 2018, California made history by becoming the first state to pass an online privacy law, the California Consumer Privacy Act (CCPA).[5] Since then, four other states have passed comprehensive privacy laws: Virginia, Colorado, Utah, and most recently, Connecticut.

Yet out of these five state privacy laws, only two offer specific protections around children's data. California's CCPA first raised the bar by requiring that companies obtain opt-in consent for sharing and selling of data of minors under 16 years old.[6] Similarly, the Connecticut Data Privacy Act (CTDPA) requires a company to obtain opt-in consent from minors under 16 before selling their personal data or using it for targeted advertising.[7]

Meanwhile, Virginia, Colorado, and Utah's laws do not have substantive child protections. This means children's data in 48 states, including Maryland, is still very vulnerable. Maryland can help now to expand protections for children online by passing its own data privacy law with strong children's provisions.

C. Without State or Federal Privacy Legislation, Children are Vulnerable to Online Harms

Children are online more than ever,[8] and are sharing more information than ever without realizing the consequences of that sharing.[9] They do not appreciate the volume of data that companies collect from them while they're online nor what companies do with that data.

---

[5] Daisuke Wakabayashi, California Passes Sweeping Law to Protect Online Privacy, N.Y. Times (June 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html.
[6] California Consumer Privacy Act §1798.120(c). CCPA also strengthened the knowledge standard seen in COPPA by stating someone who willfully disregards the consumer's age shall be deemed to have had actual knowledge.
[7] Connecticut Data Privacy Act §6(a)(7). CTDPA uses the same knowledge standard found in CCPA.
[8] Rideout, V., Peebles, A., Mann, S., & Robb, M. B. (2022). Common Sense census: Media use by tweens and teens, 2021. San Francisco, CA: Common Sense. Use of screen media is up 17 percent for tweens and teens since the start of the pandemic. In 2021, tweens spent an average of 5.5 hours on screens a day, while teens spent an average of 8.5 hours.
[9] Adriana Galvan, Todd A. Hare, Cindy E. Parra, Jackie Penn, Henning Voss, Gary Glover, B.J. Casey, *Earlier Development of the Accumbens Relative to Orbitofrontal Cortex Might Underlie Risk-Taking Behavior in Adolescents*, J. NEUROSCI. (June 21, 2006), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6673830/; Sonia Livingstone, Mariya Stoilova, and Rishita Nandagirl, Children's Data and Privacy Online: Growing Up in a Digital Age 29 (Jan, 2019), https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf.

By the time a child turns 13 years old, adtech firms have compiled over 72 million data points on that child.[10] These data points include information on the websites the child visited, what content they viewed, and for how long, all of which can be used to sort children into target ad groups. This ability to target children pushes them down dangerous rabbit holes of harmful content. A report by the children's advocacy watchdog group Fairplay showed that Meta, formerly Facebook, knowingly profited from pushing pro-eating disorder content to children on Instagram since at least 2019.[11] This pro-eating disorder bubble on Instagram includes 90,000 unique accounts that reach 20 million unique followers, with at least one-third of the followers in this bubble being underage.[12] This targeting happens quickly, too. Within a day of U.S. Senator Richard Blumenthal (D-CT)'s office creating a fake Instagram account for a 13-year-old girl and following accounts with content related to disordered eating and dieting, the platform began serving content promoting eating disorders and self-harm.[13] It also only took one minute for the office to find TikTok videos promoting illegal steroids.

In 2019, Facebook was revealed to have categorized 740,000 kids under 18 years old as being interested in gambling, and 940,000 minors as being interested in alcoholic beverages.[14] While advertisers cannot target minors with ads for products illegal for them, they can still use this knowledge in a way that harms children, such as by advertising games that contain gambling elements.[15] The harms do not stop there, and they will only get worse as technology continues to advance, such as through virtual reality headsets.[16]

The harms online platforms have imposed on children negatively impact their mental health, and several studies have illustrated this. For example, a 2019 study focusing on young women found frequent use of Instagram to be correlated with depressive symptoms, decreased self-esteem, general and physical appearance anxiety, and body dissatisfaction.[17] The 2020 Facebook study that whistleblower Frances Haugen disclosed reported similar findings on teen girls, including

---

[10] Tim Cross, Ad Tech collects 72 million data points on the average American child by age 13, VideoWeek (Dec. 14, 2017), https://videoweek.com/2017/12/14/ad-tech-collects-72-million-data-points-on-the-average-american-child-by-age-13/. This number is from 2017, so it is likely a substantial underestimate today.

[11] Fairplay, Designing for Disorder: Instagram's Pro-eating Disorder Bubble (Apr. 2022), https://fairplayforkids.org/wp-content/uploads/2022/04/designing_for_disorder.pdf.

[12] Ibid.

[13] *See also* Adam Westbrook, Lucy King, and Jonah M. Kessel, *What's One of the Most Dangerous Toys for Kids? The Internet*, New York Times (Nov. 24, 2021), https://www.nytimes.com/2021/11/24/opinion/kids-internet-safety-social-apps.html.

[14] Alex Hern and Frederik Hugo Ledegaard, Children 'interested in' gambling and alcohol, according to Facebook, The Guardian (Oct. 9, 2019), https://www.theguardian.com/technology/2019/oct/09/children-interested-in-gambling-and-alcohol-facebook.

[15] *Id.*

[16] *See e.g.* Katie Joseff, Behavioral Advertising Harms: Kids and Teens, Common Sense Media, Common Sense Media (Feb. 2022); Katie Joseff, List of Social Media Harms, Common Sense Media (Dec. 2021); Katie Joseff and Nelson Reed, *What are Kids Doing in the Metaverse?*, Common Sense (Mar. 23, 2022), https://www.commonsensemedia.org/kids-action/articles/what-are-kids-doing-in-the-metaverse.

[17] Sherlock, M., & Wagstaff, D. L. (2019). Exploring the relationship between frequency of Instagram use, exposure to idealized images, and psychological well-being in women. Psychology of Popular Media Culture, 8(4), 482–490.

that Instagram made body image issues worse for one in three teen girls.[18] Another Facebook study found that 40 percent of teen boys also experienced negative social comparison due to Instagram.[19] The mental health crisis our nation's children are facing has become so dire that earlier this year, U.S. Surgeon General Vivek Murthy issued a mental health advisory.[20]

The longer we wait to pass strong privacy laws, the longer children will be harmed. The lack of legislation to protect all children online is unacceptable given all that we now know about how children are being harmed online, largely because of the excessive amount of data companies have accumulated and can use to exploit them.

Maryland has an important opportunity to be a leader in children's online privacy and should pass a strong state privacy law that protects all consumers, while giving children's data the specific additional protections it deserves. This would not only offer Maryland children unique protections, but it would encourage other states to follow suit, creating a safer online environment for more kids.

II. Maryland Should Adopt Specific Privacy Protections That Will Reduce Online Harms Against Children

Children's online privacy law must go beyond the "notice and consent" model to correct the power imbalance between parents and companies. Parents should not bear the burden of keeping their children and their personal information safe online. Instead, state legislatures should adopt data minimization principles, a targeted ad ban, deletion rights, and a knowledge standard that reflects the reality of companies' data practices today. These provisions will lay the groundwork for a safer online environment for kids to play, explore, and learn in.

A. Data Minimization Requirements

The most effective way to limit privacy harms is to first limit the amount and type of data that companies collect from consumers in the first place. Data minimization principles should be implemented for everyone, but at least for children who are still developing their critical thinking abilities and do not understand the implications of sharing their information online.

Passing a strong data privacy law with data minimization provisions would help to alleviate the burden on parents and children by pushing some of the responsibility onto the companies themselves to engage in responsible data practices. Data collection and sharing should be

[18] Wells, G., Horwitz, J., & Seetharaman, D., Facebook Knows Instagram is Toxic for Teen Girls, Company Documents Show, Wall Street Journal (Sept. 14, 2021), https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739.
[19] *Id.*
[20] *Protecting Youth Mental Health: The Surgeon General's Advisory*. (2021), 9.

limited to what is reasonably necessary to provide the product or service requested by the consumer.

Maryland should also require companies to abide by two other data minimization principles. First, under purpose specifications, companies should be required to disclose the purpose for which personal information is collected to the parent or minor no later than at the time of collection. Companies should only use the data for that specific purpose. Second, companies should only retain data for as long as is necessary to fulfill a transaction or provide a requested service. Such default prohibitions and restrictions on data sharing is far preferable to a regime in which individuals can opt-out of data sharing because individuals will not have to hunt down and navigate different opt-out processes for potentially thousands of different companies, and try to understand long, convoluted privacy policies and terms of service statements.

Additionally, from a cybersecurity concern, any data that is collected can be breached, which is particularly concerning for sensitive information, such as data of a child. By stopping unnecessary data collection practices, there will be less data that can be breached by bad actors.

B. Targeted Ad Ban

The internet is now dominated by targeted advertising in which companies can collect data from individuals, such as about their web browsing behavior, and use that information to make inferences and serve them customized ads to increase chances of engagement and profits. The large number of harms this type of advertising can impose on vulnerable children and teens makes banning them for this group an obvious and necessary solution.

I have previously testified and submitted written testimony to the Senate Finance Committee detailing the harms of targeted, or surveillance advertising, to children.[21] To summarize:

- **Kids and teens are largely defenseless against advanced advertising techniques.** Only 24 percent of 8- to 11-year-olds can distinguish between ads and content, or understand the persuasive intent behind ads.[22] Most children do not know ads can be customized to each individual either, and researchers have concluded that children are not equipped to identify targeted ads that exploit their tracked activity data from traditional advertising.[23] This makes it easy for marketers to manipulate and fine-tune sales pitches

[21] *Maryland Online Consumer Protection and Child Safety Act, SB 11 Before the Maryland Senate Finance Committee* (2022) (statement of Irene Ly, Common Sense Media), https://www.commonsensemedia.org/sites/default/files/featured-content/files/sb0011_irene_ly_common_sense_media_fav_written_testimony.pdf.
[22] Ofcom, Children and Parents: Media Use and Attitudes Report 86 (Nov. 2016), https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf.
[23] Kaiwen Sun, Carlo Sugatan, Tanisha Afnan, Hayley Simon, Susan A. Gelman, Jenny Radesky, and Florian Schaub. 2021. "They See You're a Girl if You Pick a Pink Robot with a Skirt": A Qualitative Study of How Children Conceptualize Data Processing and Digital Privacy Risks. In Proceedings of the 2021 CHI Conference on

to this vulnerable group, often without them even realizing, or being able to resist them.

- **The profiling of targeted advertising can harm kids' and teens' development and constrain and shape their choices and autonomy.** Instead of exploring different interests, targeted advertising can profile kids and target them with ads that encourage more of the same behaviors.[24] When kids know they are being monitored by surveillance technology, they are also less likely to engage in critical thinking, political activity, or questioning of authority.[25]

- **Targeted advertising can perpetuate discrimination toward kids, teens, and adults alike.** Companies can utilize coercive techniques that only show them certain opportunities, such as educational opportunities, and algorithmic profiling that builds in bias in decision making.[26]

At a minimum, companies should be prohibited from engaging in targeted advertising to children. Companies can instead use alternative modes of advertising such as contextual advertising that do not require data collection and tracking of individuals, and can even be more profitable than targeted advertising.[27] With the harms that can come from targeting kids, the benefits of targeted advertising are significantly outweighed by the risks.

C. Deletion Rights

The unique vulnerabilities of children also necessitates giving parents deletion rights over their children's personal information. Children develop and mature over time, and the information they share as a young child should not have to haunt them for the rest of their life. This is especially true while there is still little transparency behind exactly what data companies are collecting from our children, who it is being shared with, and for what reasons.

Human Factors in Computing Systems (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 687, 1–34. DOI:https://doi.org/10.1145/3411764.3445333; Zhao, J., Wang, G., Dally, C., Slovak, P., Childs, J. E., Van Kleek, M., & Shadbolt, N. (May 2019). "I make up a silly name": Understanding children's perception of privacy risks online. CHI Conference on Human Factorsin Computing Systems Proceedings 2019, p. 2.

[24] Common Sense Media, AdTech and Kids: Behavioral Ads Need a Time Out (May 13, 2021).

[25] Brown, D. H., & Pecora, N. (2014). Online data privacy as a children's media right: Toward global policy principles. Journal of Children and Media, 8(2), 201–207.

[26] Rashida Richardson and Marci Lerner Miller, Slate, The Higher Education Industry is Embracing Predatory and Discriminatory Student Data Practices (Jan. 13, 2021), https://slate.com/technology/2021/01/higher-education-algorithms-student-data-discrimination.html; Todd Feathers, College prep software Naviance is selling advertising access to millions of students, The Markup (Jan. 13, 2022), https://themarkup.org/machine-learning/2022/01/13/college-prep-software-naviance-is-selling-advertising-access-to-millions-of-students.

[27] Keach Hagey, Behavioral ad targeting not paying for publishers, study suggests, Wall Street Journal (May 29, 2019), https://www.wsj.com/articles/behavioral-ad-targeting-not-paying-off-for-publishers-study-suggests-11559167195.

Deletion rights do not necessarily cause an undue burden on companies. They do not have to comply with a consumer's request to delete the consumer's personal information if it is reasonably necessary to maintain the consumer's personal information, such as to complete a requested transaction, or to comply with a legal obligation. Existing state privacy laws like CCPA outline specific circumstances in which a company does not have to comply with a deletion request.[28] When compliance is not possible, a company should then issue to the consumer an explanation of why the request could not be filled within a reasonable time.

D. Strengthened Knowledge Standard

The effectiveness of any children's privacy protections rests largely on the knowledge standard that determines which companies must comply with those provisions. Unfortunately, there is a large loophole in COPPA that allows companies to evade compliance.

COPPA's obligations apply to websites and online services that are directed to children, or where the operator has "actual knowledge" that a user on its platform is a child. This knowledge standard enables bad actors to bury their heads in the sand and claim their services are directed to a general audience, often while touting to advertisers that they can target kids. This is what YouTube did, in the most prominent example of how a company can exploit this loophole. In 2019, YouTube settled with the Federal Trade Commission for collecting data from children in violation of COPPA.[29] The Commission had to waste time and money to get evidence confirming the obvious: YouTube knew kids were on its platform and collected information from them in violation of COPPA anyway.

The YouTube settlement also illustrates how the current actual knowledge standard is difficult for the Commission and state Attorney Generals to effectively enforce. Although the Commission ultimately penalized YouTube for its COPPA violations under the actual knowledge standard, it is just one of the thousands of companies collecting data from children in violation of COPPA. A 2018 study showed that more than half of the 5,855 Android apps the researchers examined that target children violate COPPA.[30] Of the apps on the Apple App Store and Google Play Store, about 423,000 apps are likely child-directed and subject to COPPA.[31] This does not

[28] CCPA §1798.105(d).
[29] Press Release, Federal Trade Commission, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law (Sept. 4, 2019), https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law.
[30] Reyes, I., Wijesekera, P., Reardon, J., On, A. E. B., Razaghpanah, A., Vallina-Rodriguez, N., & Egelman, S. (2018)."Won't somebody think of the children?" examining COPPA compliance at scale. Proceedings on Privacy Enhancing Technologies, 2018(3), 63-83. *See also* Kelly, G., Graham, J., Bronfman, J., & Garton, S. (2021). *2021 State of Kids' Privacy*. San Francisco, CA: Common Sense Media (detailing privacy trends found in hundreds of popular kids' apps).
[31] Nine percent of Apple App Store apps (152,000) and eight percent of Google Play Store apps (271,000) are likely child-directed. Trishla Ostwal, Advertisers at Risk of Unknowingly Collecting Children's Data, Violating COPPA Laws, Ad Week (Aug. 25, 2022), https://www.adweek.com/programmatic/advertisers-at-risk-collecting-childrens-data/.

even count the companies that may be subject to COPPA because they have actual knowledge. Yet the Commission has limited resources, dedicating only approximately 9 to 11 full-time employees to the COPPA program annually.[32] With such limited resources, the FTC has opened only 80 COPPA investigations in the last five years.[33] As long as the Commission and state AGs are understaffed and underfunded, they cannot be expected to gather the amount of evidence required for a successful enforcement action under the "actual knowledge" standard. They only have capacity to investigate select companies, which will likely be the largest, most well-known companies, when smaller entities can cause similar levels of harm from wrongful data privacy practices.

The knowledge standard must be updated to reflect today's reality: companies already collect large amounts of data, and some of this data can be used to infer the age of users. Companies tout their detailed data on children in their marketing material to advertisers but hide behind the actual knowledge standard in their legal department. We must move to a knowledge standard where a company must comply with children's protection provisions such as those discussed above if they know or should have known children are on the platform.

This does not have to be burdensome for companies either. Such a knowledge standard would *not* require businesses to collect any additional information or implement age verification or age gating tools. Rather, it would ensure that companies have to look at the data they already have, and cannot turn a blind eye when they already know children are on their site.

Changing the knowledge standard is instrumental to truly protecting children online. Without a strong knowledge standard, the substantive protections I have discussed above would not be effective because companies can continue evading compliance.

III. Conclusion

Children are increasingly online and are being harmed by the way online platforms are designed and operated. It would be irresponsible for the state of Maryland, with all that we know about online platforms and the experiences of minors, not to pass its own privacy law, and one that contains strong childrens' privacy protections. Study after study spells out all the different ways children are harmed online. With so much uncertainty around pending federal legislation, states like Maryland must forge ahead and pass their own legislation in this field. Maryland can and should set a strong precedent for others to follow suit and ensure its residents enjoy the privacy rights they want and expect.

[32] Federal Trade Commission, Federal Trade Commission Report to Congress on COPPA Staffing, Enforcement, and Remedies (Aug. 2022), https://www.ftc.gov/reports/federal-trade-commission-report-congress-coppa-staffing-enforcement-remedies.
[33] *Id.*