Ensuring the Protection of Children's Online Privacy

Raima Ahmed

In an era where children's lives are increasingly digitally mediated, matters of online privacy and security have never been more pressing. While laws like the Children's Online Privacy Protection Act (COPPA) were passed with the intention of shielding children from exploitative uses of data, the rapid evolution of social media, artificial intelligence, and cyber-surveillance have far out-paced that of legislatures. Social media platforms rely on algorithmic targeting, data collection, and manipulative design features that erode children's privacy and expose them to hazardous content as well as potential exploitation. Despite existing legal protections, technology companies prioritize profit over digital safety, keeping children vulnerable to an industry that is predicated on data-driven interaction. While COPPA and other child protection laws provide a foundation for digital privacy laws, they fail to address social media's unchecked data collection, AI-driven surveillance, and exploitation, necessitating greater enforcement measures to safeguard children's digital rights that may be sacrificed for corporate interests.

Existing child protection laws were enacted to secure children's privacy on the internet, but become increasingly ineffective in the face of technological advancements. The Children's Online Privacy Protection Act (COPPA) was enacted into law in 1998 and is still the primary child protection law in the United States to shield minors under 13 years old from unchecked data collection. COPPA requires businesses to obtain permission from parents prior to gathering information from children, making policies regarding privacy clear, and allows parents to view their child's information as well as able to request for its deletion. However, COPPA has some limitations. For one, its protection is only up until the age of 13, leaving adolescents at risk for

data misuse and exploitation. Furthermore, the law is often unevenly enforced; some corporations claim not to "knowingly" collect information from users under the age of 13, shifting the burden of responsibility from companies to parents. Moreover, COPPA does not consider the widespread practice of algorithmic surveillance, which is targeted at children in terms of their online activity and interests without explicitly collecting personally identifiable information. This allows companies to gather in-depth data without COPPA consent requirements. Aside from COPPA, there are additional U.S. laws aiming to protect children's data, but none of them specifically address the scope of current digital threats. The Children's Internet Protection Act (CIPA) was enacted by Congress to limit children's access to harmful content. Through the E-rate program, communication services and products become more affordable to schools and libraries. However, if said schools or libraries do not filter obscene content for minors, they will have limited access to this discount. While this program has proved to be highly effective in filtering harmful content on the internet in an educational setting, it does not tackle the potentially harmful abuse of children's data on internet sites. At the state level, laws like the California Consumer Privacy Act (CCPA) attempt to provide greater protection, including giving consumers the right to access and delete their personal data. The CCPA does not directly deal with children's privacy concerns, however, leaving loopholes in regulation.

Internationally, stricter laws like the European Union's General Data Protection Regulation (GDPR) have evolved by requiring explicit consent to process children's data and granting minors the right to erase their information. The UK's Age-Appropriate Design Code (AADC) goes a step further in ensuring privacy protection by requiring online platforms to set default privacy settings for users under the age of 18. Despite these international efforts, enforcement remains challenging, as tech companies often operate across borders, making it

difficult to ensure compliance with national regulations. Moreover, most current legislation is based on reactive enforcement–focusing on punishment after a violation has been committed–instead of stopping harm in real time. As biometric data collection, artificial intelligence, and algorithmic profiling continue to advance, these laws become increasingly outdated in protecting children from sophisticated methods of data exploitation. Given the rapid evolution of technology, there is a pressing need for stronger, more adaptive regulations to fully address the growing range of digital privacy risks that children face today.

Despite the presence of child protection laws, today's children face more intense online privacy threats than ever before, the majority of which are inadequately addressed by current legislation. One of the most prominent threats that exists involves exposure to explicit content on YouTube, TikTok, and Instagram, where recommendation algorithms expose kids to engaging material that is often void of age-appropriate filtering. While COPPA regulates overt data gathering from children younger than 13, it does not restrict algorithmic targeting, meaning that platforms can still collect behavioral signals and amplify harmful content. Studies have indicated that children are just as susceptible to being influenced by extreme and/or exploitative content that maximize user engagement at the cost of safety. In addition to harmful content exposure, dark patterns–deceptive user interface designs that trick consumers into consenting to more data collection than they realize–are rampant. Dark patterns include but are not limited to pre-checked boxes, confusing word phrasing, and making it deliberately difficult to opt out of data sharing, all of which bypass the parental consent requirement of COPPA and exploit children's digital literacy. In addition, collection and monetization of children's data is common and largely unchecked. Companies have the ability to gather location information, browser history, biometrics, and view behavior, and sell it to data brokers. Though state-level regulations such as

the California Consumer Protection Act (CCPA) give consumers access to and erasure rights of their data, enforcement on specific data from minors is unknown with no proactive protections in place. Adding to these problems is the severe risk of grooming and cyber exploitation. Platforms tend to have moderate measures put in place, but these tend to be reactive as opposed to preventative. Grooming can be done through direct messaging, comment threads, etc, but COPPA does not contain strong requirements for reporting such activity. International efforts like the GDPA place stronger emphasis on data minimization and explicit consent, but even these systems struggle to enforce them, and they do not fully address real-time risks that algorithmic design and predatory behaviors pose. Children's information is continuously harvested online, and can be manipulated and sold. Companies face little regulation in leveraging algorithms and dark patterns.

To effectively protect children in today's rapidly evolving digital era, stronger legal protections are necessary, beginning with a comprehensive expansion of COPPA and the closing of its loopholes. COPPA's age limit of 13 is no longer sufficient, given that teens as old as 17 are targeted by data brokers and social media companies. Expanding the law's coverage to older youth would protect vulnerable users from comprehensive data collection. Also, the vague standard of "unknowingly collecting data" must be replaced with proactive obligations for companies to verify user ages and treat unidentified users as minors by default. In addition to augmenting COPPA, there must be much stronger restrictions on behaviorally targeted marketing and data brokers. Currently, companies exploit ambiguities in law to build deep behavioral profiles on children based on inferred information. Stronger restrictions are needed to prevent the widespread use of this data for manipulation, as well as the selling of sensitive personal data to

third-party advertisers. Effective enforcement of these laws would ensure that platforms comply with policies related to children's online safety and digital privacy.

The prominent counterargument to imposing more controls on children's online privacy is that they would be a hindrance to free speech and innovation. Excessive controls, according to critics, can inhibit technology development, particularly in applications related to artificial intelligence, social networks, and information technologies. Limiting data collection and the use of this data for advertising can also degrade the business model of many freemium offerings, such as social networking services and search providers, that obtain their income from leveraging user information to sustain themselves and provide custom experiences. The critics also cite that excessively burdensome legislation could limit children's access to various resources or conversing with others in beneficial scenarios. However, these concerns must be balanced against the huge risks of unrestricted data collection, exploitation, and privacy violation. The rights of children to privacy and immunity from harm must take precedence, and the law can be drawn up in such a way as to promote innovation while safeguarding children. This balance can be achieved by making transparency and accountability a priority without stifling technological advancement.

The present condition of children's online privacy is inadequate when considering the fast pace in which technology is progressing. Existing laws like COPPA and the Children's Internet Protection Act have set a baseline for protecting children online, but they are insufficient in combating threats like algorithmic targeting, AI-driven surveillance, dark patterns, and data exploitation. Uncontrolled data collection of children by social media platforms and third-party data brokers continues to expose minors to considerable threats, ranging from harmful content to child exploitation online. Expanding the application and closing the loopholes of laws like

COPPA is an essential step that must be taken to protect children's online privacy. While there are potential risks as to how it could impact innovation and free speech, children's safety against child exploitation online should take precedence. Only through proactive, updated, and enforced legislation, can the privacy of children be protected and secured.

Works Cited

Nguyen, Stephanie T. “Children’s Online Privacy Protection Rule (‘coppa’).” Federal Trade Commission, 3 Feb. 2023, www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa.

Nguyen, Stephanie T. “Children’s Privacy.” Federal Trade Commission, 6 Feb. 2025, www.ftc.gov/business-guidance/privacy-security/childrens-privacy.

“Children’s Internet Protection Act (CIPA).” Federal Communications Commission, www.fcc.gov/consumers/guides/childrens-internet-protection-act. Accessed 31 Mar. 2025.

“The Children’s Internet Protection Act (CIPA).” ALA, www.ala.org/advocacy/advleg/federallegislation/cipa. Accessed 31 Mar. 2025.

“California Consumer Privacy Act (CCPA).” State of California - Department of Justice - Office of the Attorney General, 28 Jan. 2025, oag.ca.gov/privacy/ccpa.

Ibm. “What Is the CCPA?” IBM, 19 Dec. 2024, www.ibm.com/think/topics/ccpa-compliance.

Staff, CSO, et al. “California Consumer Privacy Act (CCPA): What You Need to Know to Be Compliant.” CSO Online, 31 Mar. 2025, www.csoonline.com/article/565923/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant.html.

“Protecting Youth from Data Exploitation by Online Technologies and Applications.” NAACP, June 13, 2022. https://naacp.org/resources/protecting-youth-data-exploitation-online-technologies-and-applications.