Insight

COPPA 2.0: The Costs of Layering on Liability

JOSHUA LEVINE | MAY 18, 2023

Executive Summary

- As part of a legislative package of children's online protection bills, the Senate reintroduced the Children and Teens' Online Privacy Protection Act (COPPA 2.0), which would broaden the scope of regulated websites and expand the existing law's applicability to all minors under age 17.
- The proposed changes would significantly expand websites' potential liability by requiring them to comply with additional regulations related to data collection, storage, and deletion, as well as age verification and hosting content under the threat of federal and state litigation.
- Because COPPA 2.0 could harm competition and innovation in digital markets, user privacy, and online speech, lawmakers should consider alternative measures to protect children online such as enacting a federal data privacy standard, improving existing efforts promoting digital literacy and internet skills for children, and empowering parents to help their children safely navigate online interactions.

Introduction

Senators Ed Markey (D-MA) and Dr. Bill Cassidy (R-LA) re-introduced the Children and Teens' Online Privacy Protection Act (COPPA 2.0), which would update and expand the regulations outlined in the Children's Online Privacy Protection Act (COPPA) to any internet user under age 17. COPPA passed in 1998 with the goal of empowering parents to control what types of information websites collect about their children, but only protected users under age 13. Lawmakers and regulators have been largely unsuccessful in previous attempts to expand COPPA's requirements through legislation and rulemaking.

Much like other recent legislative attempts to improve children's online safety, COPPA 2.0 is unlikely to achieve its intended purpose and could introduce additional harms to internet users of all ages. COPPA 2.0's proposed changes would expand potential liability and regulatory burdens for any website that could be used or is "reasonably likely to be used" by minors. These requirements will impact how websites collect, store, use, and delete data; how they verify the identity and age of users; and what types of content they host. Failure to comply with the law's requirements could also leave firms vulnerable to litigation from the Federal Trade Commission (FTC) under its unfair and deceptive acts or practices authority as well as civil action from state attorneys general (AG) if they have reason to believe residents have been "adversely affected" by a firm's practices. COPPA 2.0's expansion of regulatory compliance and threat of litigation could negatively impact competition in digital markets, user privacy, and online speech.

Protecting children online is a worthwhile and important goal, but lawmakers should consider alternative approaches that would enhance protections for minors while minimizing potential harm to the online experience. One option is to adopt a federal privacy law that would apply to all users and provide minors and adults alike greater control of how their data is collected, stored, and used. Another option is to evaluate existing programs and resources dedicated to improving digital literacy and providing children with the skills to understand how their data is used and ways to safely navigate the internet. Further, if lawmakers are set on reforming COPPA, they could focus on empowering parents to manage their children's internet usage rather than requiring firms to collect, store, and catalogue more sensitive user information from minors.

What COPPA Does and COPPA 2.0's Update

COPPA

COPPA directs the FTC to promulgate and enforce rules to restrict websites and other interactive computer services from collecting certain kinds of data on users under age 13. Primarily, the law requires that before any website collects data on a child younger than 13 it must receive "verifiable parental consent" and provide information on what types of data the site collects, how the data is used, retained, and deleted, and allow parents to prevent certain uses of their child's data. COPPA's requirements only apply to websites that are "targeted towards children," or have "actual knowledge" of collecting data from covered users or other websites targeted toward children. While the onus is on websites to follow procedures related to parental notification and consent and data governance, the rules attempt to empower parents to decide who collects data on their children, what data is collected, and how it is used.

The FTC first promulgated rules for COPPA in 1999, and while there have been a few updates and rule expansions, larger changes have not materialized. In 2005, the FTC promulgated a rule to allow for the use of email combined with other methods to verify parental consent, and in 2013, expanded the definition of personal information to identifiers such as cookies, geolocation information, and photos of children under age 13. Since 2000, the FTC has brought 34 COPPA cases and collected more than $190 million in civil penalties. The agency has attempted however, to update and expand rules to cover more websites and data practices, but has not succeeded.

Beyond the work of the FTC, legislators have attempted to expand COPPA's protections and scope in response to concerns that the current framework falls short of protecting children's data. State and federal lawmakers have previously introduced legislation to expand COPPA's protections to all minors, broaden the scope of websites covered by regulations, and increase the amount of information sites collect and store to ensure compliance. Supporters of increased protections claim that current regulations fall short in protecting children, who are online more than ever. While previous attempts to increase COPPA's protections have stalled, concerns about the relationship between social media, children's mental health, and large technology companies' data collection practices have reinvigorated proponents of updating COPPA.

COPPA 2.0

COPPA 2.0 would extend COPPA's protections to any user under age 17, broaden the scope of websites and firms covered by the law, add regulatory compliance related to data collection and management, and expand enforcement authority to state AGs.

In line with COPPA, covered firms would have to notify and receive consent from a minor's parent before collecting any personal information, but COPPA 2.0 expands the definition of covered websites and services to include platforms "used or reasonably likely to be used by children or minors." This new designation can be avoided if firms that serve a "mixed audience," adults and minors, verifies the age of every user and receives appropriate consent to collect user data. Along with expanding this definition, the rules would also cover online applications, mobile applications, or a "connected device," such as an Apple Watch or video game console that connects to the internet.

The bill would also require firms to comply with "Fair Information Practices Principles." These principles include rules governing long-term data retention and collection, requirements that firms re-affirm parental consent whenever a policy related to data collection changes, and conditions that a minor or a parent of a minor may request any personal information be deleted at any time. Complementing these rules, the bill creates a

"Digital Marketing Bill of Rights for Minors," which prohibits any data collection from minors that could be used for targeted advertising and requires minors to consent to receive targeted advertising.

Finally, COPPA 2.0 would expand enforcement to the state level, giving states' AGs the ability to enforce compliance if a resident of their state has been "adversely affected" by the actions of a covered firm.

Potential Costs Associated with COPPA 2.0

COPPA 2.0's proposed changes would increase the potential liability online firms and service providers face. While the goal of improving protections for children's data is commendable, legislators should consider the potential harms to digital commerce and competition, user privacy, and speech and information online.

Expanded liability related to user access and data for online services would increase economic costs for all firms participating in digital markets and could stunt competition and innovation. COPPA 2.0's expanded definition for covered services, which moves away from an actual knowledge standard, coupled with raising the age of covered users to include minors under age 17, would mean any websites that could be visited by a minor must comply with COPPA 2.0. Cost estimates from one study on COPPA compliance in 2000 ranged from $115,000–$290,000 per year for a "mid-sized children's website," while other sources estimated a single site's compliance costs at $60,000–$100,000 per year. Additional research estimated that COPPA's 2013 updates would increase costs by $6,200 per year for existing firms and $18,670 per year for new entrants. These compliance costs already present a significant barrier, especially for small businesses and startups, whose average annual revenue can range from $46,978–$387,000 depending on size. Eighty-one percent of small businesses have no employees, and on average accrue less than $50,000 in revenue per year. Additional regulations would increase compliance costs, raising barriers to entry and insulating incumbents from competition.

COPPA 2.0's requirements would also expand the amount of data firms must collect, store, catalogue, and potentially delete, cutting against the privacy goals of the bill. COPPA 2.0 builds on existing law by requiring sites to collect more user data and to store and provide information on what data has been collected on a user if requested by a minor's parent. Requiring firms to retain such information makes sites appealing targets for cybercriminals to hack, a problem that is growing exponentially. Building on the potential harms of additional data collection, COPPA 2.0's requirements would not apply to platforms that serve a "mixed audience," serving both minors and adults, if the site verifies the age and receives consent from every user before collecting their data. This creates a binary choice:

comply with all of COPPA 2.0's rules or gate service using age verification, which would likely require a user to provide government-issued or biometric identification. Large majorities of Americans are uncomfortable providing their own or their child's identification to use social media or other services. Research has shown technical problems related to using biometric tools to age gate services, especially for teens, as well as high implementation costs and other concerns related to the security and accessibility of biometric identification.

In addition to potential harms to user privacy and security, the difficult binary choice between compliance and age verification could have adverse impacts on free speech and online content. Putting services behind age verification will effectively eliminate online anonymity, which is key to preserving the right to speak anonymously and free expression online generally. Further, in response to COPPA 2.0's expanded age range and scope of covered websites, firms may remove certain content that could be appealing to minors to avoid designation as a covered site. This could have an adverse effect on the diversity of information online, specifically for minors looking to learn from and explore online content that interests them. Alternatively, firms will age gate their sites to prevent non-compliance, which will also reduce the amount of information available online for all users. COPPA 2.0's expanded rules could incentivize firms to gate their services by requiring age verification, which could have adverse consequences for free speech and access to information online for users of all ages.

Alternative Measures to Protect Minors' Data and Promote Safe Internet Use

If Congress wants to address how minors' data is collected, stored, and shared, then enacting a federal privacy law would be a move in the right direction. As there is currently no federal privacy law, states are increasingly filling the void, creating a patchwork of regulatory regimes across the country. Creating a uniform standard for how firms treat users' data would ensure consumers of all ages are protected online and allow firms to focus on one framework and simplify compliance, which could help lower barriers to entry and promote trust between users and firms.

Another path to promote online safety and responsible online habits is improving digital literacy efforts. Research has shown that digital literacy education can have a positive impact on children's online habits, decrease the likelihood they divulge sensitive information to strangers, and help them avoid malicious actors online. There already exist federal, state, and local programs promoting digital literacy and better online habits. As digital skills become more important and digital services continue to proliferate, lawmakers should ensure future generations can reap the benefits of digital commerce and information while preparing them to deal with potential harms.

Lawmakers could consider changes that would further COPPA's original intent, empowering parents to help their children manage their data online. COPPA intended to provide parents' a degree of control over the data websites collected on their children. COPPA 2.0 does encourage parental oversight, but the legislation also requires firms to collect and store additional information on users and refocuses the law toward increased regulation for internet platforms rather than empowering parents to protect their children. Incentivizing the use of tools and education to help parents and children understand and manage online interactions may better serve constituents. Many large technology firms and international organizations have features designed to empower parents, some of which are open-source, and available to smaller firms. To improve COPPA 2.0, lawmakers could focus on incentivizing firms to provide parents more tools and options to manage what data websites collect on their children and how it is used rather than forcing companies to collect and store more personal information for undetermined amounts of time.

Conclusion

COPPA 2.0 is part of a larger push by federal and state lawmakers to address concerns about online harms to children. COPPA 2.0 would add to existing law that requires websites receive verified parental consent to collect data on users under age 13 by raising the age threshold to include all users under age 17, expanding the scope of covered websites and services, and increasing regulatory compliance related to data collection and use for minors. Protecting children from unscrupulous data practices is a worthy goal. Yet the proposed changes would impose significant costs on the digital economy for users of all ages, including children. Compliance costs for COPPA are already significant and COPPA 2.0 would increase these costs, as more sensitive data would be collected and stored. This also presents real risks related to cybersecurity and privacy. If lawmakers want to protect children's data and promote a safer online experience, they could enact a uniform federal data privacy standard, promote and improve programs related to digital literacy, and consider how to focus regulations to support the law's original intent of empowering parents as it relates to the collection and use of their child's data.