Insights: Publications

5 Key Takeaways | Marketing to Kids: New U.S. Privacy and Social Media Safety Laws Impact Advertising Compliance

October 17, 2024

Written by **Meghan K. Farmer, Tatum Andres**

With increasing scrutiny on how companies handle personal data of children under 18, several new laws are reshaping the legal landscape. Even companies that may not intend to direct their services to children still need to be vigilant. Recent laws, coupled with FTC enforcement actions, as well as new federal and state legislation on the immediate horizon, underscore the importance of securing valid consent and minimizing the collection and processing of minors' data. The authors of this article, together with Prentecia Floyd, recently discussed these issues at a seminar in Atlanta, organized in collaboration with the Georgia Chapter of the Association of Corporate Counsel (ACC), which supports the needs of in-house counsel throughout the state. During the seminar, the panelists engaged in a thoughtful discussion on how recent legislative changes and enforcement actions impact the guidance in-house counsel should provide to their clients about offering services to children and teens. Key takeaways from the seminar are outlined below.

Historically, the federal Children's Online Privacy Protection Rule (COPPA) was the primary regulation governing children's online privacy. However, COPPA's scope is limited in several ways:
• It only applies to children under 13;
• It solely covers information collected online, such as through websites, mobile apps, and internetconnected services; and
• It is focused on information collected by services specifically directed at children.

Because of these limitations, many products and services found it relatively easy to avoid falling under COPPA's requirements. However, the new wave of laws designed to protect children and teens expands beyond COPPA's narrow reach. As these regulations evolve, it is important to reassess data practices and ensure compliance, even if services are not explicitly child directed. The broader scope of these new and pending laws means that services used by minors, even incidentally, could now fall under regulatory oversight, making it essential for companies to proactively implement appropriate safeguards.

1. The Age Threshold for “Child” is Expanding

While COPPA applies to children under the age of 13, many states have enacted comprehensive privacy laws that extend protections to older minors. For example, California requires opt-in consent for children between 13 and 16, while Florida and Maryland have extended similar protections to minors up to the age of 18. In states like Iowa and Utah, companies are required to provide notice of data processing practices, and consumers must

be given the opportunity to opt out of sensitive data processing. Maryland goes further by banning the sale of children's data or the processing of children's data for targeted advertising, with no exceptions. These broader protections create more complex consent requirements, and companies must be aware of varying state-level thresholds to ensure they are compliant across jurisdictions.

2. Broader Protection Against Harmful Content and Advertising

Beyond expanding the age definition, new laws aim to address the harms that children and teens face in the digital space, including how companies collect and use their data. Data collected from children and teens can be used to personalize content, promote engagement, and increase time spent on digital platforms. These practices can result in young users being exposed to harmful content or manipulated into addictive behaviors. These regulations are not merely designed to limit data collection but also to create safer online environments for young users. For example, Maryland's Age-Appropriate Design Code requires companies to conduct data protection impact assessments (DPIAs) for online products likely to be accessed by children. These DPIAs must identify how a product uses children's data and assess whether the product aligns with the best interests of children. Companies are required to take affirmative steps to ensure that their platforms are designed in a way that minimizes risks to minors. As states pass such laws, companies must shift from merely limiting data collection to actively protecting children's well-being in the digital world.

3. Stricter Regulations for Social Media Platforms

Social media platforms (i.e.: website or internet application that allows a person to create an account and communicate with others through posts) are especially under scrutiny as state lawmakers increasingly focus on the addictive nature of these services for minors. New York's Stop Addictive Feeds Exploitation (SAFE) Act prohibits social media platforms from sending notifications to users under 18 between midnight and 6 a.m. unless they have verifiable parental consent. Similarly, California has introduced laws limiting notifications to minors during school hours, unless parental consent has been obtained. Georgia takes a different approach by focusing on limiting how personal data can be used for ad targeting, giving parents control over which features of the platform can be disabled or modified. The common theme across these regulations is clear: social media platforms must limit the exposure of minors to addictive content, restrict the use of personal data for targeting, and ensure parents play an active role in managing their children's digital experiences. As states implement these restrictions, companies must invest in creating robust age verification systems and parental controls to stay compliant with these new requirements.

4. Parental Consent and Data Transparency Are Crucial

Parental consent and transparency remain critical components of both existing and new regulations. Companies must ensure that they not only obtain verifiable parental consent before collecting data from children but also provide clear and transparent information about their data practices. Parents must be informed if a company collects their contact information to seek consent, and they must be given a clear explanation of what data will be collected, how it will be used, and what will happen if consent is not given. Transparency goes beyond mere legal compliance—it establishes trust with parents and ensures that they can make informed decisions about their children's online activity. Companies must review their consent processes to ensure they comply with both COPPA and the new state laws that expand upon COPPA's requirements.

5. Changes Are Still on the Horizon

Despite the wave of new regulations, more changes are still on the horizon. Key pieces of legislation, such as the federal Kids Online Safety Act (KOSA) and an updated version of COPPA (referred to colloquially as

COPPA 2.0), are currently advancing through Congress. KOSA seeks to create additional duties of care for platforms by requiring them to implement the strongest privacy settings for minors, provide parents with tools to report harmful behavior, and take steps to mitigate risks to minors, such as suicide, eating disorders, and substance abuse. Meanwhile, COPPA 2.0 would expand privacy protections to cover minors under the age of 17, prohibit targeted ads for teens, and create an “eraser button” that allows teens to delete their personal data. These proposed laws indicate a growing consensus that the digital world must be a safer place for children and teens. Companies must prepare for even stricter privacy and safety requirements as these legislative efforts gain momentum. Both KOSA and COPPA 2.0 are expected to undergo further negotiations in Congress, with additional developments likely in the coming months.

Therefore, it is important to remain vigilant in adapting to this expanding regulatory landscape. As states continue to pass laws with stricter requirements for handling children's and teens' data, companies need to stay ahead of the curve by proactively implementing comprehensive safeguards, ensuring data transparency, and securing appropriate consent. Failure to do so could result in significant legal and reputational risks, especially as enforcement actions increase under existing laws.

For more information, please contact:
Barry Benjamin, bbenjamin@ktslaw.com
Meghan Farmer, mfarmer@ktslaw.com
Tatum Andres, tandres@ktslaw.com

Related People



Meghan K. Farmer

t 404.541.6816
mfarmer@ktslaw.com



Tatum Andres

t 312.628.7183
tandres@ktslaw.com