Hashed & Salted | A Privacy and Data Security Update
July 2024

New York Governor Signs Legislation to Protect Minors Online

Key Takeaways:

- Two significant kids privacy bills passed the New York Legislature on June 7 and were signed into law by Gov. Kathy Hochul on June 20.
- One law—the Stop Addictive Feeds Exploitation (SAFE) for Kids Act—prohibits operators from offering "addictive feeds" to minors on social media platforms or other online services without obtaining verifiable parental consent.
- The other law—the New York Child Data Protection Act (CDPA)—prohibits operators of online services from processing the personal data of minors ages 13 – 17 without informed consent from the minor, or unless doing so is strictly necessary for the service.
- These laws will likely pose novel compliance challenges for companies, not just individually but also collectively, since the two laws diverge with respect to which party (parent or teen) can provide consent.

Summaries of both laws are below.

Stop Addictive Feeds Exploitation (SAFE) for Kids Act

1. To whom does the SAFE for Kids Act apply?

The SAFE for Kids Act applies to "covered operators" (i.e., any person, business or other legal entity that offers an addictive feed as a significant part of their website, mobile app or other online service to a covered minor). The law does not explain what constitutes a "significant part" of an online service.

A "covered minor" is a user of an online service in New York when the operator has actual knowledge the user is a minor.

A "minor" is an individual under the age of 18.

2. What is an addictive feed?

An "**addictive feed**" is broadly defined as an online service (or portion thereof) where multiple pieces of media generated or shared by users are recommended, selected, or prioritized for display to a user based (in whole or in part) on information associated with the user or the user's device.

However, a feed is not an addictive feed if:

- Media is recommended, prioritized or selected:
  - Based on information that is not persistently associated with the user or the user's device, and does not concern the user's previous interactions with media generated or shared by other users.
  - Based on user-selected privacy or accessibility settings or technical information concerning the user's device.
  - Only in response to a specific search inquiry by the user.
  - Exclusively next in a preexisting sequence from the same author, creator, poster or source.
  - As necessary to comply with the SAFE for Kids Act.

Attorney Advertising

- The user expressly and unambiguously requested certain media to be displayed (e.g., the user subscribed to an author, a page or a group).
- The user expressly and unambiguously requested that certain media, authors or pages be blocked, prioritized or deprioritized.
- The media is direct and private communication (e.g., direct messaging).

3. What does the SAFE for Kids Act require?

Covered operators are prohibited from:

- Providing an addictive feed to a user unless the covered operator has used commercially reasonable and technically feasible methods to determine that the user is not a covered minor or has obtained verifiable parental consent.
- Sending notifications concerning an addictive feed to a covered minor between the hours of midnight and 6 a.m. ET unless the covered operator has obtained verifiable parental consent.

A covered operator can operate under the presumption that a user is not a covered minor if it has used commercially reasonable and technically feasible age determination methods (which are to be set forth by the New York attorney general via rulemaking) and has determined that the user is not a minor. Aside from specifying that the attorney general's regulations must include at least one method that does not rely solely on government-issued identification or that allows a user to maintain anonymity, it is unclear what the age determination methods will look like. The law is very vague in this respect, and likely intentionally so, in light of the First Amendment and other litigation challenges that similar laws have faced (including but not limited to concerns regarding restricting minors' and adults' access to information without adequate justification). However, as noted above, users can still search for specific topics of interest and receive content based on their express requests.

4. What about rulemaking and enforcement authority?

New York's office of attorney general has rulemaking and enforcement authority. Penalties include disgorgement of unlawfully obtained data and other ill-gotten profits or gains, and up to $5,000 in civil penalties per violation.

In particular, the attorney general is tasked with promulgating regulations that identify commercially reasonable and technically feasible methods for covered operators to determine whether a user is a covered minor, as well as identify methods of obtaining verifiable parental consent.

5. When does the SAFE for Kids Act take effect?

It will take effect 180 days after the New York attorney general promulgates rules and regulations necessary to effectuate the provisions of the SAFE for Kids Act.

New York Child Data Protection Act (CDPA)

1. To whom does the CDPA apply?

The CDPA applies to "operators" (i.e., any person who operates or provides a website, mobile app, connected device or other online service that processes the personal data of covered users).

A "covered user" is a user who is actually known by the operator to be a minor, or a user of an online service that is primarily directed to minors (i.e., targeted to minors).

A "minor" is a person under the age of 18.

2. What does the CDPA require?

Operators are prohibited from:

- Processing, or allowing third-party operators to collect, the personal data of covered users under the age of 13 unless such processing is permitted under the Children's Online Privacy Protection Act (COPPA).
- Processing, or allowing third-party operators to collect, the personal data of covered users ages 13 – 17 unless informed consent has been obtained or the processing is strictly necessary for one of the following permissible purposes:
  - Providing or maintaining a specific product or service requested by the covered user.
  - Conducting the operator's internal business operations (defined to exclude marketing, advertising, research and development, providing products or services to third parties, and prompting covered users to use an online service when it is not in use).
  - Identifying and repairing technical errors that impair existing or intended functionality.

- Protecting against malicious, fraudulent or illegal activity.
- Investigating, establishing, exercising, preparing for or defending legal claims.
- Complying with federal, state or local laws, rules or regulations.
- Complying with a civil, criminal or regulatory inquiry, investigation subpoena, or summons by federal, state, local or other governmental authorities.
- Detecting, responding to or preventing security incidents or threats.
- Protecting the vital interests of a natural person.

The law also appears intended to restrict purchasing or selling, or allowing a processor or third-party operator to purchase or sell, the personal data of a covered user, although the language in the statute may leave some room for limited "sales" with informed consent. A "third-party operator" is an operator who is not the operator with whom the user intentionally and directly interacts or that collects personal data from the direct and current interactions with the user.

Operators must:

- Respect age flags—i.e., treat a user as a covered user if the user's device communicates or signals that the user is a minor (including through a browser plug-in or privacy setting, device setting, or other mechanism that complies with regulations promulgated by the attorney general).
- Let third-party operators know, prior to disclosing personal data to such parties, when the operator's online service is primarily directed to minors or when the personal data concerns a covered user.
- Enter into a written, binding agreement with third-party operators (governing the disclosure and processing of personal data) prior to disclosing the personal data of covered users to such parties.
- Enter into a written, binding agreement with processors that requires processors to (1) only process personal data of covered users pursuant to instructions of the operator; (2) assist the operator in meeting the operator's obligations under the CDPA; (3) provide materials to demonstrate CDPA compliance upon the request of the operator; (4) allow operators to evaluate CDPA compliance via reasonable assessments conducted by the operator or the operator's designated assessor; and (5) notify the operator before disclosing personal data of covered users to subprocessors. Processors must also dispose of, destroy or delete personal data at the direction of the operator, and delete or return all personal data at the end of its provision of services (within 30 days of the request).
- Delete personal data within 30 days if the operator learns that such data was improperly collected from a covered user and notify any third-party operators to whom it knows it disclosed personal data of a covered user.

3. How should informed consent be obtained (when it is required)?

Informed consent must be obtained from covered users ages 13 – 17 (where processing is not strictly necessary for permissible purposes set forth in the law) either through a request or through a "device communication or signal" (e.g., through a browser plug-in or privacy or device setting).

- An operator's request for informed consent must (1) be made separately from any other transaction or part of a transaction; (2) be made without the use of dark patterns; (3) state that the processing activity is not strictly necessary and that the user may decline without preventing continued use of the online service; and (4) present an option to refuse to provide consent as the most prominent option.
- An operator must also respect a user's choice to decline or consent to processing as evidenced via device communications/signals (e.g., browser plug-in/privacy setting, device setting or other mechanism that complies with regulations promulgated by the attorney general).

Informed consent, once given, must be freely revocable at any time and at least as easy to revoke as it was to provide.

Notably, upon learning that a user has aged out of being a covered user, an operator still must not process personal data that would otherwise be subject to the CDPA (i.e., data from when the user was under 18), until it receives

informed consent, and it must provide notice to the user that they may no longer be covered by the protections and rights provided under the CDPA.

4. What about rulemaking authority and enforcement?

New York's office of attorney general has rulemaking and enforcement authority. Penalties include disgorgement of unlawfully obtained data and other ill-gotten profits or gains, and up to $5,000 in civil penalties per violation.

5. When does the CDPA take effect?

It takes effect one year after the CDPA becomes law—likely in June 2025.

Related Professional

Chanda Marlowe . . . . . cmarlowe@loeb.com