
State Child Privacy Law Update

FEBRUARY 28, 2023

In addition to the numerous comprehensive privacy laws that have been proposed in at least 20 states thus far in 2023, legislative trends demonstrate an emerging focus on regulations that address specific types of information, including the personal information of children. To date, 19 such proposals have emerged across 15 states. Each of these bills imposes new requirements for the processing of children's information, across online services, products, features, and social media platforms. These proposals both emulate and build upon existing requirements. Companies that process the personal information of children in the ordinary course of business (including children under the age of 18) should be aware of these proposals and how they may impact their business operations.

Other than the Children's Online Privacy Protection Act (COPPA, which regulates the collection of personal information of children under the age of 13), there is no uniform approach to regulating the processing of children's data. This is leading to a patchwork of requirements and proposals at the state level. The California Privacy Rights Act (CPRA), for example, creates specific requirements relating to the "selling" or "sharing" of personal information of children under the age of 16. Other states, such as Colorado and Connecticut, are regulating the processing of personal data from a known child as "sensitive" data that is subject to special processing requirements under their comprehensive privacy laws (though both laws also have some form of an exemption for data that is processed pursuant to COPPA).

On September 15, 2022, California became the first state to pass a law that will regulate the online activities of all children under the age of 18. California's [Age Appropriate Design Code](#) (the "Design Act") imposes additional compliance requirements for companies that offer their products and services to children, including data privacy provisions that go beyond those which companies already had to comply with under COPPA and the comprehensive state privacy laws. Specifically, the Design Act requires online services, features, or product operators to proactively consider children's best interest at the design stage of production. The enactment of the Design Act represented an important legislative development and foreshadowed that a "California Effect" may drive other legislative bodies to consider enacting their own legislative scheme (similar to how the California Consumer Privacy Act inspired other states to consider their own privacy legislation).

Further, it signaled to companies covered under the Design Act to consider expanding new compliance structures beyond California residents.

Although most provisions of the Design Act do not go into effect until 2024, the law has already sparked numerous copycat bills in state legislatures across the country. Much like the Design Act, these are standalone bills that regulate specific issues related to children's interactions with online services and social media platforms, including in relation to the processing of personal information. Companies, particularly online service providers and social media platform operators, should be attentive to these emerging standalone regulatory schemes as most impose new requirements for regulatory compliance—such as additional disclosures for child users, data protection impact assessment obligations, and age verification requirements. Further, most bills give rise to monetary liability for violations, including civil penalties, administrative fees, and the potential for class action lawsuits.

In this alert, we offer a few key takeaways at the outset and provide a detailed breakdown of the bills that have been introduced in the 2023 legislative session. We are happy to answer any questions you may have on these issues.

KEY TRENDS AND HIGHLIGHTS

1. **Standalone Bills:** All of these bills are standalone bills focused solely on child privacy issues, most commonly children's use of online services and social media platforms.
2. **Bills Focused on Online Services:** Many of the bills closely mirror the key provisions of California's [Design Act](#), which takes effect on January, 1, 2024—particularly, the following bills: in Maryland, [SB0844](#) and [HB0901](#); in New Jersey, [A4919](#) and [S3493](#); in New Mexico, [SB319](#); and in Oregon, [SB196](#). Common provisions include:
 - Providing protections for children under the age of 18.
 - Key Requirements:
 - Requiring businesses to consider whether their services are “likely to be accessed by children” or whether it is reasonable to expect that the online service would be accessed by children, based on certain indicators.
 - Requiring businesses that provide an online product likely to be accessed by children to complete a data protection impact assessment, which includes documenting any risk of material detriment to children that arises from data management practices; creates a plan to mitigate or eliminate risk; and estimates the age of child users with a reasonable level of certainty appropriate to the risks that arise from the data management practices, among other requirements.

- Requiring configuration of default privacy settings provided to children by an online product to offer a high level of privacy, unless covered entities can demonstrate a compelling reason that a different setting is “in the best interest of children.”
- Requiring businesses to provide monitoring signals to the child, if the online product allows the child’s parent, guardian, or any other consumer to track the child’s location.
- Requiring verifiable age estimation for users of online services. Prohibits the use of any personal information collected to estimate age or age range for any other purpose, retaining the personal information longer than necessary to estimate age, or attempting age assurance in a way that is disproportionate to the risks and data practice of an online product.
- Requires that businesses provide prominent, accessible, and responsive tools to help children or their parents/guardians exercise their privacy rights and report concerns.
- Key Prohibitions:
 - Prohibits a business from using children’s personal information in a manner the business knows or has reason to know is materially detrimental to the physical, mental, or well-being of a child.
 - Prohibits the profiling of a child by default unless appropriate safeguards are in place.
 - Prohibits collecting, selling, sharing, or retaining any personal information that is unnecessary to provide an online product to a child, unless there is a compelling reason that the act is in the best interest of the child.
 - Prohibits collecting, selling, or sharing, precise geolocation without providing an obvious signal and appropriate disclosure to the user.

3. **Bills That Regulate Social Media Platforms:** Many of the bills focus on children’s interactions with social media platforms. Provisions vary across bills; however, many include provisions such as:

- Conditioning applicability on the number of account holders that a particular social media platform hosts.
- Requiring descriptions of social media platforms’ use of algorithms for content moderation purposes; some bills, such as [Minnesota HB1503](#) and [Texas HB2155](#), go as far as banning the use of algorithms for content moderation when targeting children.

- Requiring descriptions of design features, in particular those that have addictive tendencies. While some require only disclosures (for example, [Florida HB591](#)), others (like the bills being considered in New Jersey, [A5059](#) and [S3608](#)) go as far as banning features with addictive tendencies.
 - Requiring age verification of users.
 - Providing exemptions for platforms that otherwise meet the provided threshold but are primarily news outlets, internet service providers, or covered under Section 230, among other criteria.
4. **Current Status:** Most of the bills remain in the early stages of the legislative process, with many having only, at most, been referred to committees. Five bills have made more notable progress:
- The Maryland Age Appropriate Design Code Act has advanced in both the House and Senate, with committee hearings scheduled for [SB0844](#) on March 8 and [HB0901](#) on March 1.
 - Maryland's [HB0254](#) had a hearing scheduled by the House Economic Matters Committee on February 22.
 - Utah's Social Media Regulation Act: A fiscal note regarding [SB152](#) has been sent to a sponsor in the House Rules Committee, while [HB311](#) has been placed on the Senate calendar for a third reading.
 - Virginia's Consumer Data Protection Act, [HB1688](#), has passed in the House.
 - New Mexico's Age Appropriate Design Code Act has been granted a "Do Pass recommendation" by the Senate Taxation, Business and Transportation Committee.

2023 PROPOSALS

Florida

1. **Bill Title:** [House Bill 591](#)
2. **Current Status:** As of February 27, 2023, HB591 has been referred to the House Regulatory Reform & Economic Development Subcommittee (2/7/2023).
3. **Key Provisions:**
 - Applies to social media platforms and requires them to disclose and describe various practices, including content moderation policies, such as the use of addictive design features; manipulation of photographs or digital images; and clear and concise user policies, protections, and reporting mechanisms related to harmful behaviors such as bullying, harassment, and threats of violence or self-harm. Specifically, requires the

disclosure of the methodology used to consider the best interest of minors when designing, developing, and providing services.

- Requires that social media platforms implement protective measures for use of services by minors, such as providing zip-code-based references to local law enforcement, suicide prevention, and domestic violence prevention services; displaying screen time usage data; incorporating parental settings; and incorporating a preset disclaimer (provided by the legislature) at the time of login that provides notice of addictive qualities, mental health consequences, and data practices, among other disclosures.
- Prohibits schools that accept state funding from requiring students, regardless of age, to register, enroll, or participate in social media platforms as a means to access information, materials, or resources related to school activities.
- Provides the Department of Agriculture and Consumer Services with the authority to create and enforce rules under this act.
- Social media platforms that fail to meet the criteria are prohibited from enrolling minors in their service. The act allows for civil penalties of up to \$10,000 per minor who is registered in violation of the act.
- Would take effect on July 1, 2023, with requirements for social media companies to begin on January 1, 2024.

Illinois

1. *Bill Title:* Minor Online Data Privacy Act ([SB1739](#))
2. *Current Status:* As of February 27, 2023, SB1739 has been referred to the Senate Assignments Committee (2/9/2023).
3. *Key Provisions:*
 - Bill contains only a short title provision.

Kansas

1. *Bill Title:* [Senate Bill 222](#)
2. *Current Status:* As of February 27, 2023, SB222 has been referred to the Committee on Federal and State Affairs (2/9/2023).
3. *Key Provisions:*
 - Provides protections for children under the age of 18.
 - Establishes platform liability: A platform provider is liable for information published by a user of such online platform if such provider knew or should have known such provider used an algorithm to make personalized recommendations to a user of

such online platform, and such posted material contributed to a physical or severe emotional injury to users.

- Requires that wireless communication device vendors configure default settings on a newly purchased device to alert parents that a minor has downloaded an application on the minor's device.
- Would go into effect immediately upon publication in the statute book.

Maryland

1. *Bill Title:* The Maryland Age Appropriate Design Code Act ([SB0844/HB0901](#))
2. *Current Status:* As of February 27, 2023, [SB0844](#) is scheduled for a committee hearing on March 8 (2/7/2023) and [HB0901](#) is scheduled for a committee hearing on March 1 (2/9/2023).
3. *Key Provisions:*
 - Applies to any entity that conducts business in the state of Maryland and has meets one of the following requirements: (1) has annual gross revenues in excess of \$25 million; (2) buys, receives, sells, or shares the personal information of 50,000 or more consumers, households or devices alone or in combination with its affiliates or subsidiaries and for the business commercial purposes; or (3) derives at least 50% of its annual revenues from the sale of consumers' personal information.
 - Exempts various entities and information subject to the Health Insurance Portability and Accountability Act (HIPAA).
 - Defines "likely to be accessed by children" as a reasonable expectation, based on certain criteria, that the online service would be accessed by children, including the reasonable expectation that the online product is directed to children as defined in COPPA; the product, based on reliable evidence regarding audience composition, is found to be routinely accessed by a significant audience of children; elements of the online product are known to be of interest to children, such as games, cartoons, music and celebrities who appeal to children; or the business knows, based on internal research, that a significant amount of the online product's audience is children.
 - Requires businesses that provide an online product likely to be accessed by children to complete a data protection impact assessment that documents any risk of material detriment to children that arises from data management practices; creates a plan to mitigate or eliminate risk; and estimates the age of child users with a reasonable level of certainty appropriate to the risks that arise from the data management practices, among other requirements.
 - Requires businesses to configure default privacy settings provided to children by an online product to offer a high level of privacy, unless covered entities can

demonstrate a compelling reason that a different setting is “in the best interest of children.”

- Requires businesses to provide monitoring signals to the child if the online product allows the child's parent or guardian or any other consumer to track the child's location.
- Requires that businesses provide prominent, accessible, and responsive tools to help children or their parents/guardians exercise their privacy rights and report concerns.
- Prohibits a business from using children's personal information in various ways, including in a manner the business knows, or has reason to know, is materially detrimental to the physical, mental, or well-being of a child; to profile a child by default; to collect, sell, share or retain any personal information that is unnecessary to provide an online product, unless there is a compelling reason that the act is in the best interest of the child; to collect, sell or share precise geolocation or to do so without providing an obvious signal to the child; and to use the personal information of a child for any reason beyond the purpose for which the personal information was collected.
- Prohibits the use of dark patterns.
- Prohibits the use of any personal information collected to estimate age or age range for any other purpose, retain the personal information longer than necessary to estimate age, or attempt age assurance in a way that is disproportionate to the risks and data practice of an online product.
- Does not create a private right of action. Authorizes the state AG to bring a civil action to enforce the act. The state AG may seek civil penalties of up to \$2,500 per affected child for each negligent violation and \$7,500 per affected child for each intentional violation.
- Creates a 90-day cure period for businesses that are in “substantial compliance with requirements.”
- Would take effect on October 1, 2023.

Maryland

1. *Bill Title:* [House Bill 254](#)
2. *Current Status:* As of February 27, 2023, the House Economic Matters Committee held a hearing regarding HB254 on February 22 (2/22/2023).
3. *Key Provisions:*
 - Creates age-tailored protections—designates a child who is 13–18 an “authorized minor” and a child under the age of 13 an “unauthorized minor.”

- Applies to “large social media platforms” that provide a service to the public through an internet website or mobile application that includes features that allow a child in the state to share images, text, or video through the internet with other users of the service whom the child has met, identified, or become aware of solely through the use of the service; and (1) has more than 1 million monthly active users in the United States or (2) generates more than \$500 million in annual gross revenue.
- Exempts specific services and platforms, including platforms primarily used for the sale or provision of professional services or the sale of commercial products; services that do not include the ability for content to be sent by a user directly to a child; or the provision of news or information, as well as large social media platforms that do not prohibit the use of the service by a child in the platform’s terms of use and private social media accounts.
- Creates requirements for large social media platforms, including to identify and remove all public social media accounts created or operated by unauthorized minors and delete all associated user data; to respond to parent requests within 24 hours; to notify children under the age of 13 that they can delete their data; and to allow parents to create a joint social media account with children ages 13–18.
- Large media platforms must submit a biannual report to the state AG outlining their progress in identifying and removing social media accounts created or operated by unauthorized minors. Failure to submit this report could result in a fine of up to \$5 million per violation.
- Creates an opportunity for a parent or guardian to bring an action for injunctive relief against an offending large social media platform. A covered entity can be fined up to \$100,000 per violation. All fines are to be deposited in a “Digital Citizenship Fund.”
- Provides the state AG the power to adopt regulations to carry out this act.
- Would take effect on October 1, 2023.

Massachusetts

1. *Bill Title:* Massachusetts Internet Privacy Rights for Children Act ([HD2325](#))
2. *Current Status:* As of February 27, 2023, HD2325 has been introduced in the House (1/19/2023).
3. *Key Provisions:*
 - Provides protections for children under the age of 18.
 - Applies to operators of internet websites, online services, online applications, or mobile applications directed to minors.
 - Prohibits targeted advertisements directed toward children.

- Prohibits disclosure or sharing of children’s personal information with third parties for the purpose of marketing or advertising adult use products or services, including tobacco, and cannabis.
- Creates affirmative rights for minors to obtain information collected and request the removal of information collected, including content posted by the user.
- Requires operators to provide clear instructions on how to exercise rights created under this act and to notify users that exercising the right to remove content does not ensure the complete removal of the content posted.
- Authorizes the state AG to bring a civil action to enforce the act. The state AG may seek a civil penalty of up to \$2,500 per violation.
- Would take effect on January 1, 2024.

Minnesota

1. *Bill Title:* [House Bill 1503](#)
2. *Current Status:* As of February 27, 2023, HB1503 has been referred to the House Commerce Finance & Policy Committee (2/13/2023).
3. *Key Provisions:*
 - Applies to operators as defined by COPPA who operate social media platforms with more than 1 million account holders operating in Minnesota.
 - Prohibits social media platforms from using a social media algorithm to target user-generated content toward an account holder under the age of 18.
 - Requires that social media platforms establish additional requirements for users under the age of 18, such as obtaining permission from a legal guardian prior to allowing activation of an account, or age verification.
 - Creates an exception for a social media algorithm that is intended to block access to inappropriate or harmful content to an account holder who is a minor or a social media platform that provides parental controls that are designed to control what can be accessed by a minor’s account by filtering content. Also exempts user-generated content created by public or private schools.
 - Creates a private right of action. Social media platforms that are in violation are liable to users for any regular or special damages, and a statutory penalty of \$1,000 per violation.
 - Would go into effect immediately upon enactment into law.

New Jersey

1. *Bill Title:* [Assembly Bill 4919](#) and [Senate Bill 3493](#)

2. *Current Status:* As of February 27, 2023, A4919 has been referred to the Assembly Science, Innovation and Technology Committee (12/5/2022), and S3493 has been referred to the Senate Law and Public Safety Committee (1/19/2023).
3. *Key Provisions:*
 - Creates protections for children under the age of 18.
 - Applies to social media platforms that have users in the state of New Jersey.
 - Defines “likely to be accessed by children” as a reasonable expectation, based on certain criteria, that the online service would be accessed by children, including the reasonable expectation that the online product is directed to children; the product, based on reliable evidence regarding audience composition, is found to be routinely accessed by a significant audience of children; the online product includes advertisements marketed to children; elements of the online product are known to be of interest to children, such as games, cartoons, music, and celebrities who appeal to children; or the business knows, based on internal research, that a significant amount of the online product’s audience is children.
 - Requires covered entities to conduct a data protection impact assessment prior to offering an online service, product, or feature which addresses the following: whether the design could harm children; whether the design could lead to children experiencing or being targeted by harmful or potentially harmful conduct; whether the design could allow children to be party to or exploited by contact; whether algorithms used could harm children; whether system design features increase, sustain, or extend use of the social media platform by children; and the method and purpose of collection and processing of children’s information. Data protection impact assessments must be reviewed every two years.
 - Prohibits certain uses of children’s personal information, including in a way that the social media platform knows or has reason to know is materially detrimental to the physical, mental, or well-being of a child; to profile a child by default (exceptions provided); to collect, sell, share or retain any personal information that is not necessary; use and collection of geolocation information of children by default, unless necessary and not without providing an obvious sign to the child; use of deceptive design practices to lead or encourage children to provide more personal information; and use and retention for the purpose of estimating age, beyond the time necessary to estimate age.
 - Does not create a private right of action. Authorizes the state AG to bring a civil action to enforce the act. The state AG may seek a civil penalty of up to \$2,500 per negligent violation or up to \$7,500 per intentional violation.
 - Creates a 90-day cure period for violators before the state AG may bring an enforcement action.

- Creates the New Jersey Children’s Data Protection Commission. The commission will consist of nine members tasked to make recommendations to the state legislature concerning issues such as, best practices for identifying services likely to be accessed by children, as well as assessing and mitigating risks.
- Would take effect 24 months after bill is enacted into law.

New Jersey

1. *Bill Title:* [Assembly Bill A5059](#) and [Senate Bill 3608](#)
2. *Current Status:* As of February 27, 2023, A5059 has been referred to the Assembly Judiciary Committee (1/12/2023), and S3608 has been referred to the Senate Health, Human Services and Senior Citizens Committee (2/16/2023).
3. *Key Provisions:*
 - Applies to social media platforms that have users in the state of New Jersey and generated more than \$100 million in gross revenue during the preceding calendar year; and whose service (a) allows users to construct a public or semipublic profile for the purposes of using the platform, populate a list of other users, and post content viewable to other users; and (b) is designed to connect users within the platform to facilitate social interactions.
 - Exempts services that meet certain criteria, or offer specific services, including those that provide email or direct messaging services, services that primarily enable users to play video games, and services that institute and maintain audit programs.
 - Prohibits social media platforms from using any practice, design, feature, or affordance that the platform knew, or by exercise of reasonable care should have known, would cause child users to become addicted to the platform.
 - Creates a carve-out for content that would be covered under Section 230 and the First Amendment.
 - A social media platform shall be liable for a civil penalty of up to \$250,000 per violation to be collected in a civil action by a summary proceeding under the Penalty Enforcement Law of 1999 enforced by the Superior Court and the municipal court.
 - Would take effect three months after the bill is enacted into law.

New Mexico

1. *Bill Title:* Age Appropriate Design Code Act ([SB319](#))
2. *Current Status:* As of February 27, 2023, the Senate Taxation, Business and Transportation Committee has reported SB319 with a Do Pass recommendation (2/24/2023).

3. *Key Provisions:*

- Provides protections for children under the age of 18.
- Applies to controllers or persons who produce services, products or features that are targeted to residents of the state of New Mexico and that during the preceding calendar year (1) controlled or processed the personal data of not less than 100,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or (2) controlled or processed the personal data of not less than 25,000 consumers and derived more than 25% of their gross revenue from the sale of personal data.
- Exempts entities and information subject to HIPAA, as well as telecommunications services.
- Defines “likely to be accessed by children” as a reasonable expectation, based on certain indicators, that the online service would be accessed by children, including the reasonable expectation that the online product is directed to children as defined in COPPA; the product, based on reliable evidence regarding audience composition, is found to be routinely accessed by a significant audience of children; elements of the online product are known to be of interest to children, such as games, cartoons, music and celebrities who appeal to children; and the business knows based on internal research that a significant amount of the online product’s audience is children.
- Requires covered entities to conduct a data protection impact assessment prior to offering an online service product or feature, which addresses the following: whether the design could harm children; whether the design could lead to children experiencing or being targeted by harmful or potentially harmful conduct; whether the design could allow children to be party to or exploited by contact; whether algorithms used could harm children; whether system design features increase, sustain, or extend use of the social media platform by children; and the method and purpose of collection and processing of children’s sensitive information.
- Requires businesses to estimate the age of users with a reasonable level of certainty, and to configure default privacy settings provided to children by an online product to offer a high level of privacy, unless covered entities can demonstrate a compelling reason that a different setting is “in the best interest of children.”
- Requires businesses to provide monitoring signals to the child if the online product allows the child’s parent or guardian or any other consumer to track the child’s location.
- Requires that businesses provide prominent, accessible, and responsive tools to help children or their parents/guardians exercise their privacy rights and report concerns.

- Prohibits a business from using children’s personal information in various ways, including in a manner the business knows, or has reason to know, is materially detrimental to the physical, mental, or well-being of a child; to profile a child by default; to collect, sell, share or retain any personal information that is unnecessary to provide an online product, unless there is a compelling reason that the act is in the best interest of the child; to collect, sell or share precise geolocation or to do so without providing an obvious signal to the child; and to use the personal information of a child for any reason beyond the purpose for which the personal information was collected.
- Prohibits the use of dark patterns.
- Prohibits the use of any personal information collected to estimate age or age range for any other purpose, retain the personal information longer than necessary to estimate age, or attempt age assurance in a way that is disproportionate to the risks and data practice of an online product.
- Does not create a private right of action. Authorizes the state AG to bring a civil action to enforce the act. The state AG may seek civil penalties of up to \$2,500 per affected child for each negligent violation and \$7,500 per affected child for each intentional violation.
- Creates a 90-day cure period for businesses that are in “substantial compliance with requirements.”
- Would go into effect on July 1, 2024.

New York

1. *Bill Title:* New York Child Data Privacy and Protection Act ([S3281](#))
2. *Current Status:* As of February 27, 2023, S3281 has been referred to the Senate Internet and Technology Committee (1/30/2023).
3. *Key Provisions:*
 - Provides protections for children under the age of 18.
 - Applies to all online products that the provider should know are accessible to and used by children, or “targeted towards child users” in the state of New York. The state AG may consider various factors when determining if a product is targeted toward child users, such as internal research about the product’s users, existing evidence of user behavior, and whether advertisements used appeal to children.
 - Requires that covered entities complete a data protection impact assessment that includes various determinations such as the way a child user primarily interacts with the online product; the average amount of time a child user spends using the online product; and the purpose of collection, retention, processing, or sale of covered data.

- Outlines specific requirements for data controllers, such as including in the impact assessment the data sharing relationships the entity has with data processors or other third parties with whom it shares the personal data of child users, including any data addendums or other legal policies put in place between the entity and the party receiving the data.
- Bans collecting, retaining, processing, or selling the personal data of children unless such collection, retention, processing, or sale is necessary to provide such online product, to comply with the law, or for another provided compelling reason.
- Requires covered entities to use certain default settings, such as privacy by default settings, unless the entity can demonstrate a compelling reason to the state AG that an alternative default setting should be used, and to design collection in a manner that proactively alerts children “in a manner likely to be understood” that their personal data is being collected.
- Creates specific requirements for privacy policies and terms of service, including that terms of service and privacy policies must include warnings about potential harms to child users tailored toward the age range targeted by the product and that consent must be received from both child and parent.
- Does not create a private right of action. Authorizes the state AG to bring a civil action to enforce the act. If a finding is made that a person or business knowingly or recklessly violated this article, the court may impose a civil penalty of up to \$20,000 per violation provided that the total amount shall not exceed \$250 million.
- Creates a public awareness campaign to inform covered entities of these provisions prior to the act taking effect. The campaign will be funded by 20% of proceeds collected from violations of this act.
- Creates a 90-day cure period for violators before the state AG may bring an enforcement action.
- Would take effect 180 days after bill is enacted into law.

Oregon

1. *Bill Title:* Age-Appropriate Design Code Act ([SB196](#))
2. *Current Status:* As of February 27, 2023, SB196 has been referred to the Senate Judiciary Committee (1/13/2023).
3. *Key Provisions:*
 - Provides protections to children under 18 years old.
 - Applies to businesses that provide an online product, service, or feature that a child is reasonably likely to access.

- Defines “likely to be accessed by children” as a reasonable expectation, based on certain indicators, that the online service would be accessed by children, including the reasonable expectation that the online product is directed to children; elements of the online product are known to be of interest to children, such as games, cartoons, music and celebrities who appeal to children; the service is substantially similar to an online service, product, or feature children routinely access; advertisements embedded in the online product are directed at children; and the age demographics of users indicates users are under the age of 18.
- Requires covered entities to conduct a data protection impact assessment prior to offering an online service product or feature, which addresses the following: the purpose and use of children’s personal information; the risk of material detriment to the physical or mental health of children who access the service; whether the design of, or an algorithm, could result in access to harmful content, contact with harmful individuals, or viewing of harmful content; whether advertisements embedded in the product could cause harm; whether the design increases, sustains, or extends children’s use of the service; and whether and to what amount the service collects, processes, and retains a child’s personal information.
- Requires businesses to estimate the age of users with a reasonable level of certainty, and to configure default privacy settings provided to children by an online product to offer a high level of privacy, unless covered entities can demonstrate a compelling reason that a different setting is “in the best interest of children.”
- Requires businesses to provide monitoring signals to the child if the online product allows the child’s parent or guardian or any other consumer to track the child’s location.
- Requires that businesses provide prominent, accessible, and responsive tools to help children or their parents/guardians exercise their privacy rights and report concerns.
- Prohibits a business from using children’s personal information in various ways, including in a manner the business knows, or has reason to know, is materially detrimental to the physical, mental, or well-being of a child; to profile a child by default; to collect, sell, share or retain any personal information that is unnecessary to provide an online product, unless there is a compelling reason that the act is in the best interest of the child; to collect, sell or share precise geolocation or to do so without providing an obvious signal to the child; and to use the personal information of a child for any reason beyond the purpose for which the personal information was collected.
- Prohibits the use of dark patterns.
- Prohibits the use of any personal information collected to estimate age or age range for any other purpose, retain the personal information longer than necessary to

estimate age, or attempt age assurance in a way that is disproportionate to the risks and data practice of an online product.

- Does not create a private right of action. Authorizes the state AG to bring a civil action to enforce the act. State AG may seek civil penalties of up to \$2,500 per affected child for each negligent violation and \$7,500 per affected child for each intentional violation.
- Establishes the Task Force on Age-Appropriate Design, which consists of eight members tasked to make recommendations to the state legislature concerning best practices for identifying services likely to be accessed by children, and assessing and mitigating risks, among other focuses.
- Would take effect on July 1, 2024. However, the task force is subject to a sunset clause and will be repealed on January 2, 2025.

South Carolina

1. *Bill Title:* [Senate Bill 404](#)
2. *Current Status:* As of February 27, 2023, S404 has been referred to the Senate Judiciary Committee (1/18/2023).
3. *Key Provisions:*
 - Provides protections for children under the age of 18.
 - Applies to operators of a website, online service, or online or mobile application, including any social media platform.
 - Prohibits operators' use of automated decision systems for content placement, including feeds, posts, advertisements, or product offerings, for users under the age of 18, who are residents of the state.
 - Requires that operators that use automated decision systems for content placement for residents of the state who are 18 years or older conduct age verification of users through an independent service, unless the user creates a profile that provides enough information for the operator to verify age through public records or the user is required to provide government-issued identification.
 - A violation under this act will be considered an unfair or deceptive act or practice under the South Carolina Unfair Trade Practices Act and is enforceable by the state AG, who may seek a civil penalty of up to \$5,000 per violation.
 - Creates a private right of action for users who suffer damages as a result of a violation. If the court finds that the violation was willful, the court will award three times the actual damages sustained and may provide such other relief as it deems necessary or proper.
 - Would take effect immediately upon enactment.

Texas

1. *Bill Title:* [House Bill 896](#)
2. *Current Status:* As of February 27, 2023, HB896 has been introduced in the House (12/7/2022).
3. *Key Provisions:*
 - Prohibits the use of social media platforms by children ages 13 to 18.
 - Applies to social media platforms and creates requirements for social media platforms and users, including that users must have an account and platforms must conduct age verification to ensure users are over the age of 18, including requiring that account holders provide government-issued identification.
 - Incorporates privacy by design principles, such as purpose limitation for the information that is collected for the purpose of conducting age verification.
 - Social media platforms must provide an accessible, verifiable means by which a parent can request the removal of an account and must comply with such request within 10 days of receipt.
 - A violation will occur when a social media platform knowingly allows for a child to use the platform; uses or retains personal information provided in violation of this act; or fails to remove an account after parental request.
 - Does not create a private right of action. The act is enforceable by the state AG.
 - Would take effect on September 1, 2023, while social media platform requirements would not apply until January 1, 2024.

Texas

1. *Bill Title:* [House Bill 2155](#)
2. *Current Status:* As of February 27, 2023, HB2155 has been introduced in the House (2/10/2023).
3. *Key Provisions:*
 - Creates protections for children under the age of 18.
 - Applies to social media platforms or a website application that is open to the public and allows a user to create an account and communicate with other users for the primary purpose of posting information, comments, messages, or images.
 - Exempts internet service providers, electronic mail, and applications that consist primarily of news for which chat, comment, or interactive functions are incidental and directly related to news.

- Creates liability for a social media platform with regard to a user who receives user-generated content through a social media algorithm while the user is a minor if the operator knew or had reason to know that the user was a minor.
- Violators of this act could face actual damages and a civil penalty of up to \$1,000 per violation.
- Would take effect on September 1, 2023.

Utah

1. *Bill Title:* Utah Social Media Regulation Act ([SB152/HB311](#))
2. *Current Status:* As of February 24, 2023, a fiscal note regarding SB152 has been sent to a sponsor in the House Rules Committee (2/22/2023), and HB311 has been placed on the Senate calendar for a third reading (2/16/2023).
3. *Key Provisions:*
 - Provides protections for children under the age of 18 who have not been emancipated.
 - Applies to any social media company or any person or entity that provides a social media platform that (a) has at least 10 million account holders (House Companion Bill HB311 provides a lower threshold of 5 million account holders) and (b) is an interactive computer service.
 - Exempts various services, websites, and applications where the primary function is electronic mail; direct messaging; streaming services that provide only licensed media; news, sports, entertainment, or any content that is not preselected by the provider; or online shopping, among other functions.
 - Requires social media platforms to obtain parental consent prior to providing a minor an account, conduct age verification for new accounts, and enforce age verification requirements by removing access to account if a Utah resident does not comply.
 - Creates restrictions that social media platforms must enforce on minor accounts, including not allowing direct messaging between users who are not friends with minor accounts; displaying of the minor's account in search results; displaying of advertising on the minor's account; collection or use of personal information shared by the minor; targeting the minor account with suggested groups, services, or other accounts, among other forms of targeting; and access to social media accounts by minors between 10:30 p.m. and 6:30 a.m. by default. Social media companies must also provide parents with access to minors' social media accounts, including posts, messages, and responses.
 - Creates a private right of action, and should a court find that a violation occurred, the court can award attorney fees and the greater of \$2,500 per violation or actual

damages for financial, physical, and emotional harm incurred by the person bringing the action.

- The Division of Consumer Protection has the authority to administer and enforce the act and may impose administrative fines of up to \$2,500 per violation, as well as civil penalties of up to \$2,500.
- Creates a 30-day cure period for violators before the division may bring an enforcement action.
- Creates a requirement that the division compile an annual report that details the effectiveness of this act, among other metrics, to the state legislature.
- Would take effect on May 3, 2023; however, most requirements for social media companies, enforcement provisions, and the private right of action do not take effect until March 1, 2024.

Virginia

1. *Bill Title:* Consumer Data Protection Act ([SB1026/HB1688](#))
2. *Current Status:* As of February 27, 2023, HB1688 has passed in the House (2/3/2023), and SB1026 has been passed by indefinitely in the General Laws and Technology Committee (1/25/2023).
3. *Key Provisions:*
 - Applies to operators that conduct business or produce products or services that are targeted to residents of Virginia and (i) during a calendar year, control or process personal data of at least 100,000 consumers or (ii) control or process personal data of at least 25,000 consumers and derive over 50% of gross revenue from the sale of personal data.
 - Exempts various entities and information types, including state government entities, financial institutions and data governed by GLBA, entities and information governed by HIPAA, nonprofit organizations, institutions of higher education, information governed by FCRA, information governed by FERPA, and certain employment-related information.
 - Operators must obtain verifiable parental consent prior to registering a child to use a service, or collecting, using, or disclosing to a third party such child's personal data. Verifiable parental consent can be obtained via a signed consent form, the use of a payment method by a primary card holder, or the provision of a form of government identification.
 - Operators must provide consumers with an accessible privacy notice that describes the categories of data collected, purpose for collection, how consumers may exercise their rights, categories of data shared with third parties and the identity of those third parties.

- Incorporates privacy by design principles, such as purpose limitation and reasonable security practices.
- Does not create a private right of action. Authorizes the state AG to bring a civil action to enforce the act. The state AG may seek a civil penalty of up to \$7,500 per violation.
- Creates a 30-day cure period for violators before the state AG may bring an enforcement action.
- Would take effect immediately after its enactment.

West Virginia

1. *Bill Title:* [House Bill 2964](#)
2. *Current Status:* As of February 27, 2023, HB2964 has been referred to the House Judiciary Committee (1/24/2023).
3. *Key Provisions:*
 - Provides protections for children under the age of 18.
 - Applies to any person or entity that owns an internet website, online service, online application, or mobile application directed toward minors.
 - Exempts any third party that operates, hosts, or manages, but does not own, an Internet website, online service, online application, or mobile application on the owner's behalf or processes information on the owner's behalf.
 - Prohibits marketing or advertising adult use products, such as alcohol, tobacco products, cannabis, or cannabis products, to minors.
 - Requires operators to comply with requests for obtaining and removing content or information posted by a minor, provide notice to a minor of their rights to obtain removal of content, provide clear instructions on how to exercise their rights, and provide notice of instances where their information may not be completely removed.
 - Incorporated into West Virginia Code Chapter 61. Crimes and Their Punishment. Although it does not provide specific provisions regarding enforcement, its inclusion under this article indicates that a violation under this act would constitute a crime.
 - Would take effect immediately after its enactment.

West Virginia

1. *Bill Title:* [House Bill 2460](#)
2. *Current Status:* As of February 27, 2023, HB2460 has been referred to the House Judiciary Committee (1/11/2023).
3. *Key Provisions:*

- Provides protections to children under the age of 18.
- Applies to any person who in the state of West Virginia: (1) operates a website located on the internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or (2) any entity on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service.
- Establishes various requirements for operators, including to provide notice on the website of information collected; to obtain verifiable parental consent for the collection, use, or disclosure of children's personal information; to provide upon request of a parent a description of specific types of child's personal information collected; to provide the opportunity to refuse to permit the operator's further use or maintenance of information; and to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information.
- Prohibits conditioning a child's participation in a game, offering of a prize, or other activity on the child disclosing more personal information.
- Does not require verifiable parental consent when a child's contact information is used for limited purposes such as to respond on a one-time basis directly to a specific request from the child; for the sole purpose of obtaining parental consent; to protect the child's safety; to protect the integrity of the website; or for legal purposes.
- Provides a Safe Harbor Rule for covered entities that incentivizes operators to follow a set of self-regulatory guidelines that are issued by representatives of the marketing or online industries or other guidelines approved by the state AG.
- Authorizes the state AG to enforce this act as a violation under the West Virginia Consumer Credit and Protection Act.
- Requires the AG to propose rules for legislative approval under this act no later than March 1, 2023.

Contributors



Kirk J. Nahra
PARTNER

kirk.nahra@wilmerhale.com

+1 202 663 6128



Ali A. Jessani
SENIOR ASSOCIATE

ali.jessani@wilmerhale.com

+1 202 663 6105



Genesis Ruano
ASSOCIATE

genesis.ruano@wilmerhale.com

+1 202 663 6154
