South Carolina AADC-Style Act Comparison Chart

Prepared by: Daniel Hales, Policy Counsel, US Legislation

Overview: On February 5, 2026, South Carolina enacted a novel AADC-style Act (the Act), which includes a new duty of care approach, obligations to provide tools to all users, third party audit requirements, and personal liability for employees. ***Significantly, the Act had an immediate effective date.*** This comparison chart details the scope, business obligations, processing prohibitions, and enforcement provisions in the new South Carolina Act. Given how dynamic the youth privacy and online safety policy landscape is, this chart does not compare the Act to any one state law or model. Rather, the chart identifies the most relevant comparisons from the many other state laws enacted in recent years, drawing on a variety of state comprehensive privacy laws and Age-Appropriate Design Codes.

	South Carolina HB 3431	Comparable Elements from Enacted State Laws	Comparison & Analysis
	Scope		
Applicability	A "covered online service" is any legal entity that owns, operates, controls, or provides an online service that: ● Conducts business in South Carolina; ● Is reasonably likely to be accessed by minors; and, ● Controls personal data processing; And satisfies any of the following: ● > $25 million in annual revenue; ● Buys, receives, sells, or shares the personal data of 50,000+ consumers, households, or devices; and ● Derives > 50% of its annual revenue from selling or sharing data. [§ 39-80-10(4)(a)] The Act exempts government entities, services covered by GLBA, HIPAA, and	[***From Nebraska's AADC:***] **A "covered online service" is any legal entity that owns, operates, controls, or provides an online service that:** ● Conduct business in Nebraska; ● Control personal data processing; ● > $25 million in annual revenue; ● Buy, receive, sell, or share the personal data of 50,000+ consumers, households, or devices; and, ● Derives > 50% of its annual revenue from selling or sharing data. Exemptions for government entities; services covered by GLBA or HIPAA; and information collected as part of a clinical trial subject to existing federal protections.	South Carolina's Act adopts a seemingly broader scope than prior frameworks in the way it defines legal entities and applicability thresholds, potentially bringing more entities within its reach. While these frameworks generally draw from the California Consumer Privacy Act (CCPA) by applying to entities that collect and control personal data and meet specified revenue or processing thresholds, South Carolina departs from the CCPA and Maryland AADC by apparently extending coverage beyond for-profit businesses to ***any legal entity*** that owns, operates, controls, or provides an online service and meets the statutory thresholds. This approach mirrors the scope adopted in Nebraska's AADC, which likewise may apply to non-profit and other non-commercial entities,

	South Carolina HB 3431	Comparable Elements from Enacted State Laws	Comparison & Analysis
	information collected as part of a clinical trial subject to existing federal protections. [§ 39-80-20(D)]	Contains an additional carveout for services with actual knowledge that fewer than 2% of its users are minors. ***[From Maryland's AADC:]*** MD AADC defines "Covered Entity" as a sole proprietorship, partnership, LLC, association, or other legal entity operating for profit in MD that: • Collects individuals' personal data or has individuals' personal data collected on its behalf by a third parties; • Controls personal data processing; **And meets one or more of the following:** • **> $25 million in annual revenue;** • **Buy, receive, sell, or share the personal data of 50,000+ consumers, households, or devices; and,** • **Derives >50% of its annual revenue from selling or sharing data [§14-4601(H)]**	though those laws include narrower applicability thresholds. Although the policy intent is somewhat ambiguous, it is significant for entities–especially non-profit entities or affiliates–to note that South Carolina drops the "for-profit" qualifier. With respect to applicability threshold criteria, South Carolina aligns with the broader model set out in Maryland's AADC, applying to entities that meet any one of the following: (1) $25 million or more in gross annual revenue; (2) the buying, selling, receiving, or sharing of personal data of more than 50,000 individuals (down from 100,000 envisioned in CCPA); or (3) deriving more than 50 percent of annual revenue from the sale or sharing of personal data. Additionally, unlike Nebraska (and Vermont, although it is not included here), South Carolina does not include an additional carveout for services with actual knowledge that a marginal percentage of its users are minors.
Covered Individual	Provides protections for: • "Users," defined as an individual who uses the covered online service and is located in South Carolina [§ 39-80-10(20)]; and, • "Minors" defined as a consumer **under the age of 18** [§ 39-80-10(8)].	**Connecticut Comprehensive Privacy Law:** Minors, meaning individuals under the age of 18. [Conn. Gen. Stat. Sec. 42-515 § 8(7)] (*Note: also includes definition of child (u13) for specific protections).* **Maryland AADC:** Child, meaning individuals under the age of 18. [§14-4601(E)]	South Carolina's Act is consistent with similar frameworks by providing heightened protections for minors under the age of 18.

	South Carolina HB 3431	Comparable Elements from Enacted State Laws	Comparison & Analysis
		Nebraska AADC: Minors are individuals under the age of 18. (*Note: also includes definition of child (u13) for specific protections)* **Vermont AADC:** Minors are individuals under the age of 18. [§ 2449a(12)]	
Knowledge Standard	The South Carolina Act only applies to online services, products, or features that are **reasonably likely to be accessed by a minor**. The Act includes two factors for consideration: ● The individual is known to the covered online service to be a minor (as defined in § 39-80-10(7)); or, ● The covered online service is directed to children as defined under COPPA (and implementing regulations). [39-80-10(17)(a)] "Known to be a minor" means actual knowledge that the user is a child or minor. However, within this definition, actual knowledge "includes all information and ***inferences*** known to the covered online service relating to the age of the individual including, but not limited to, self-identified age, and including any age the covered online service has attributed or associated with the individual for any purpose, including marketing, advertising, or product development." [39-80-10(7)]	**[*From Vermont's AADC:*]** The Vermont AADC only applies to online services, products, or features that are **reasonably likely to be accessed by a minor**. The bill includes four factors for consideration: ● The service, product, or feature is directed to children as defined by COPPA and its implementing rules; ● The service, product, or feature is determined—based on competent and reliable evidence regarding audience composition—to be routinely accessed by an audience that is composed of at least 2% minors aged 2-17; ● The audience is determined, based on internal company research, to be composed of at least 2% of minors aged 2-17; ● The business knew or should have known that at least 2% of the audience includes minors aged 2-17, provided that, in making this assessment, the business shall not collect or process any personal data that is not reasonably necessary to	South Carolina utilizes a "reasonably likely to be accessed by a minor" standard that diverges from how AADCs have defined it, and represents a blend of components included in Nebraska's and Vermont's AADC. South Carolina's standard is comparable to Vermont's but it is more narrowly crafted. Vermont's AADC includes four factors to consider if an online service, product or feature is reasonably likely to be accessed by a minor, while South Carolina only includes two factors for consideration. One overlapping consideration included in both South Carolina's and Vermont's standard is that a covered online service is "directed to children" as defined under COPPA. South Carolina's second factor for consideration is that a covered entity has actual knowledge that a user is a minor, and the Act's definition of actual knowledge mirrors that included in Nebraska.

	South Carolina HB 3431	Comparable Elements from Enacted State Laws	Comparison & Analysis
		provide an online service, product, or feature with *[**From** Nebraska's AADC:]* The Nebraska AADC applies when covered online services know a user is a minor. Knows to be a child or minor means actual knowledge that the user is a child or minor. "Actual knowledge" is defined as "all information and ***inferences*** known to the covered online service relating to the age of the individual, including, but not limited to, self-identified age, and any age the covered online service has attributed or associated with the individual for any purpose, including marketing, advertising, or product development." However, age classifications for marketing ***take precedence*** over self-declared age. [Sec. 2(1) & (7)]	
Requirements			
Duty of Care	A covered online service shall exercise reasonable care in the use of a minor's personal data and the design and operation of the covered online service, including, but not limited to, covered design features, to prevent the following harm to minors: ● Compulsive Usage; ● Severe psychological harm including, but not limited to, anxiety, depression, self-harm or suicidal ideations;	*[**From** Vermont's AADC:]* Vermont requires covered businesses processing minor data in any capacity to exercise a "minimum duty of care," meaning the use of a minor's personal data and the design of an online service, product, or feature will not result in: ● Reasonably foreseeable emotional distress;	The duty of care in South Carolina's Act appears to blend elements of the duties seen in Vermont's AADC and the Connecticut/Colorado-style heightened protections for minors in comprehensive privacy frameworks. Similar to Vermont's duty of care, South Carolina's duty is not limited to requirements around processing minor's personal data. The duty also extends to harms related to the design of the service, product or

	South Carolina HB 3431	Comparable Elements from Enacted State Laws	Comparison & Analysis
	• Severe emotional distress; • Highly offensive intrusions on the minor's reasonable privacy expectations; • Identity theft; • Discrimination against the minor on the basis of race, ethnicity, sex, disability, or national origin; and • Material financial or physical injury. [§ 39-80-20(A)] This Act makes two key disclaimers about the application of this duty of care, including: • "Harm" is limited to those which do not conflict with liability limitation granted by Section 230 (including any future amendments or repeal); and • This duty does not require covered online services to prevent minors from deliberately and independently searching for content related to the mitigation of the described harms. [§ 39-80-20(B) & (C)]	• Reasonably foreseeable compulsive use of the service; or, • Discrimination against a covered minor based on race, ethnicity, sex, disability, sexual orientation, gender identity, gender expression, or national origin. [§ 2449c] The Act makes two disclaimers regarding the duty of care: (1) the ***content*** of what a minor views ***shall not*** establish emotional distress or compulsive usage [§ 2449c(c)]; and (2) the duty of care is not intended to prevent a minor from accessing or viewing any type of media [§ 2449c(d)]. ***[From Colorado's Comprehensive Privacy Law:]*** The Colorado Privacy Act requires controllers to use reasonable care to avoid any heightened risk of harm to minors, where heightened risks of harm include processing minor personal data in a manner that presents any reasonably foreseeable risk of: • Unfair or deceptive treatment of, or any unlawful disparate impact on, minors; • Financial, physical or reputational injury to minors; • Physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of minors if such intrusion would be offensive to a reasonable person; or	feature, including consideration of compulsive usage, emotional distress, and discrimination against the minor. South Carolina's duty of care also goes beyond Vermont's by incorporating additional harms more similar to those seen in Colorado's duty of care, such as harms involving highly offensive intrusions on a minor's reasonable expectation of privacy and identity theft (which is similar but not identical to Colorado's consideration of "any financial, physical or reputational injury to minors"). South Carolina's duty of care diverges from Vermont's and Colorado's in three key ways: (1) Vermont and Colorado qualify the assessment of harm by whether it is "reasonably foreseeable," which South Carolina omits; (2) South Carolina's duty requires services to take steps to ***prevent*** specified harms to minors as opposed to mitigating harms; and (3) South Carolina's duty includes an additional harm–consideration of "severe psychological harm"–which is typically not seen in other laws with a duty of care (but is included within Maryland's best interests of children standard). Furthermore, similar to Vermont, South Carolina's Act specifically states that viewing particular content will not give rise to a violation of the duty of care, presumably to address constitutional concerns involved in California's and Maryland's AADC.

	South Carolina HB 3431	Comparable Elements from Enacted State Laws	Comparison & Analysis
		• Unauthorized disclosure of the personal data of minors as a result of a security breach. [§ 6-1-1308.5]	
User Tools	***All users*** on a covered online service must be provided tools to: • Disable unnecessary design features; • Limit time spent on the platform; • Limit the "financial value" of purchases and transactions on the platform; • Block or disable contact from account holders not already among the ***minor's**** existing connected accounts; • Restrict ***minor account**** visibility to only connected users; • Disable the display of engagement quantification features (e.g. likes, comments, clicks, views, etc.) on items generated by the user; • Disable search engine indexing of a user's account profile; • Prohibit others from viewing a user's connections; • Restrict location visibility to only those a user specifically shares such information, and provide notice when a ***minor's*** precise geolocation information is being tracked or shared; • Opt-outs for personalized recommendation systems except for tailoring based on explicit preferences • Prevent push notifications or alerts during specified times. [§§ 39-80-30(A) & (B); 39-80-40(E)]	***[From Nebraska's AADC:]*** Covered online services must provide a covered minor with "accessible and easy-to-use tools" to: • Limit the ability of other users or visitors to communicate with the minor; • Prevent other individuals from viewing the personal data of the minor; • Control the operation of all design features that are unnecessary for providing the service by allowing a minor to opt out of all unnecessary features or categories of unnecessary covered design features; • Control personalized recommendation systems by allowing a minor to opt into a chronological feed or by preventing categories of content from being recommended; • Control the use of in-game purchases by allowing a minor to opt out of purchases or to place limits on purchases; • Restrict the sharing of precise geolocation of a minor and provide notice regarding tracking precise geolocation information (1,750 feet); and, • Provide minors options to limit the	While the kinds of tools required by South Carolina's Act are generally comparable to those in Nebraska's AADC, a major difference between these two frameworks is that South Carolina requires that these tools are provided to ***all users*** on a covered online service, not just minors. South Carolina goes on to require that these tools/settings are turned on in minor accounts by default (as noted below). Importantly, some of the provisions on required tools in South Carolina's AADC involve the ability to restrict visibility or block unconnected users to ***minor*** accounts, even though these tools apply to all users. The ambiguity around how tools provided to all users should allow for restrictions in minor accounts may cause compliance challenges and confusion. South Carolina also requires that users are provided with a tool that allows them to limit the "financial value" of purchases and transactions on the platform, without clarifying or defining that term, which may cause compliance difficulties. South Carolina's mandatory user tools may add to a growing patchwork of required tools and default settings (and range of users for which these tools/settings must be available), likely resulting in further compliance challenges for any businesses in scope of multiple minor online

	South Carolina HB 3431	Comparable Elements from Enacted State Laws	Comparison & Analysis
		amount of time they spend on the service. [Sec. 4(2)].	protection frameworks.
Parental Tools	Covered online services must provide parents with tools "to help parents protect and support minors" using the service. For users known to be minors, the tools must be enabled by default. These tools include: ● View the child's account settings; ● Change and control privacy and account settings of a child; ● Restrict purchases and financial transactions of a minor; and, ● View total time the child has spent on a service and place reasonable limits, including the ability to restrict use of the service during times of the day specified by parents, including during school hours and at night. [§ 39-80-50] Covered online services must notify a minor when any of the parental tools are in effect and what settings have been applied. [§ 39-80-50(D)]	***[From Nebraska's AADC:]*** Covered online services must provide parents with tools "to help parents protect and support minors" using the service. For users known to be children (under 13), the tools must be enabled by default. [Sec. 6(1)]. Required tools for parents to have available: ● View the child's account settings; ● Change and control privacy and account settings of a child; ● Restrict purchases and financial transactions of a minor; and, ● View total time the child has spent on a service and place reasonable limits, including the ability to restrict use of the service during times of the day specified by parents, including during school hours and at night (Sec. 6(2)). While any tools are in effect, a covered service shall notify a covered minor and describe what settings have been applied. [Sec. 6(3)].	Requirements for parental tools are largely comparable to those established in Nebraska's AADC. While other frameworks sometimes include broad requirements for covered entities to provide tools to help children or parents exercise privacy rights, Nebraska's and South Carolina's obligations to provide parental tools are more robust and prescriptive than other state privacy laws.
Signals to Minors	**Parental Monitoring:** If a covered online service allows parental monitoring, it must provide an obvious notice to the minor when they are being monitored. [§ 39-80-40(H)] **Geolocation:** An obvious notice to the	***[From Nebraska's AADC:]*** **Parental Monitoring:** If a service allows parental monitoring, the service shall provide an obvious signal when a minor is being monitored. [Sec. 5(9)].	Requirements to provide obvious signals to minors related to parental and geolocation monitoring mirror those established in Nebraska's AADC. Except for Maryland's AADC, these requirements are common in other comparable frameworks.

	South Carolina HB 3431	Comparable Elements from Enacted State Laws	Comparison & Analysis
	minor must be provided when precise geolocation information is being collected or used. [§ 39-80-40(D)]	**Geolocation:** Provide an "obvious signal" to minors when precise geolocation is being collected or used. [Sec. 5(5)].	
Default Settings	The required user tools described above must be turned on in minor accounts by default. [§ 39-80-30(C)] Privacy settings related to requirements in § 39-80-40 must be set at the highest level of protection by default. [§ 39-80-40(G)]	***[From Nebraska's AADC:]*** For the tools listed above, a covered service shall set them by default at the option or level that provides the highest level of protection available. [Sec. 4(3)].	South Carolina's obligations mandating default settings and high level protections for minor accounts aligning with the required user tools and processing restrictions is largely comparable with Nebraska. More broadly, South Carolina's requirement to implement user tools as default settings in minor accounts is a different but equivalent means of requiring highly protective settings by default for minors–a common requirement across minor online protection frameworks.
Transparency & Disclosures	Each covered online service that utilizes personalized recommendation systems is required to describe in its terms and conditions, in a clear, conspicuous, and easy-to-understand manner, how the systems are used to provide information to minors and information regarding how minors or their parents can opt out of or control the systems. [§ 39-80-60(D)] Covered online services are required to provide comprehensive, clear, conspicuous, and easy-to-understand information in a prominent location describing the design safety for minors, the privacy protections for minors, and the parental tools that the covered online service has adopted pursuant to this chapter. Such disclosure must also include a clear, conspicuous, and	***[From Vermont's AADC:]*** Covered businesses shall prominently and clearly provide on their website or app: • Privacy information, terms of service, policies, and community standards; • The purpose of each algorithmic recommendation system in use by the business; • Inputs used by the algorithmic recommendation system and how each input is (a) measured or determined, (b) uses a minor's personal data, (c) influences the recommendation, and (d) is weighed relative to the other inputs; and • For every feature of the service that uses a minor's personal data, descriptions of (a) the purpose of the	South Carolina includes transparency requirements that are generally similar to Vermont's transparency requirements in that they both require covered online services to disclose information related to use of personalized or algorithmic recommendation systems and minor data use/privacy protection. However, South Carolina's requirement is written more broadly than Vermont's, potentially allowing covered online services more flexibility in the way they provide this information and avoiding the operational challenges and trade secret questions raised by Vermont's more prescriptive and demanding requirement.

	South Carolina HB 3431	Comparable Elements from Enacted State Laws	Comparison & Analysis
	easy-to-understand explanation of how minors and parents may utilize those design safety measures, privacy protections, and tools. [§ 39-80-60(E)]	feature, (b) the personal data collected by the feature, (c) the personal data used by the feature, (d) how the personal data is used, (e) any personal data transferred to or shared with a processor, and (f) how long the personal data is retained. [§ 2449e(3)]	
Third-Party Audits	Covered online services must annually issue a ***public report*** prepared by an ***independent third-party auditor*** that contains a detailed description of the covered online service as it pertains to minors, including its covered design features, its use of personal data, and its business practices as they pertain to minors. Each report must include: ● The purpose of the covered online service; ● The extent to which the covered online service is likely to be accessed by minors; ● An accounting of the total number and types of reports generated pursuant to Section 39-80-60(A) and assessment of how those reports were handled, if known; ● Whether, how, and for what purpose the covered online service collects or processes minors' personal data and sensitive personal data; ● The design safety for minors, the privacy protections for minors, and the parental tools that the covered online entity has adopted;	***[From Maryland's AADC:]*** A covered entity that provides an online product reasonably likely to be accessed by children must prepare a **Data Protection Impact Assessment (DPIA)** for the online product. [§14-4604]. The DPIA must: ● Identify the purpose of the online product; ● Identify how the online product uses children's data; ● Determine whether the online product is designed in a manner consistent with the best interests of children reasonably likely to access the online product through consideration of [*a list of harms to be assessed, some of which have been omitted here for the sake of space*]; ○ Whether the online product **uses system design features to increase, sustain, or extend the use of the online product, including the automatic playing of media, rewards for time spent,**	Contrasting sharply from Maryland's AADC and other prior state privacy laws, South Carolina takes a novel shift by requiring covered online services to conduct third-party audits for public reporting. These reports must be submitted to the Attorney General, who will publicly post it in a prominent location on the state Attorney General's website. Depending on how detailed the report information must be under these provisions, it's possible that public disclosure of this information may result in operational challenges and trade secret questions for covered online services. However, some of the assessment criteria is still comparable to existing law. Similar to the DPIA assessment criteria in Maryland's AADC, a third-party audit in South Carolina would require covered online services to evaluate minor data management practices, use of certain design features, and certain information about algorithms used by the online service. Although, diverging from Maryland, South Carolina requires more descriptive reporting of service design rather than assessment of likelihood of harm to children resulting from design elements.

	South Carolina HB 3431	Comparable Elements from Enacted State Laws	Comparison & Analysis
	• Whether and how the covered online service uses covered designed features; • The covered online service's process for handling data access, deletion, and correction requests for a minor's data; • Age verification or estimation methods used; and, • A description of algorithms used by the covered online service. [§ 39-80-70(A)]	**and notifications that would result in harm to children** ○ Whether, how, and **for what purpose the online product collects or processes personal data of children** and whether those practices **would result in harm to children**; ○ Whether **algorithms used by the online product would result in harms to children** • Include a description of steps that the covered entity has taken and will take to comply with the duty to act in a manner consistent with the best interests of children. ***[From Maryland's Comprehensive Privacy Law:]*** A controller shall conduct and document, on a regular basis, a data protection assessment for each of the controller's processing activities that present a heightened risk of harm to a consumer, including an assessment **for each algorithm that is used**. [§ 14-4610(B)]	Additionally, the requirement that audit reports include a description of algorithms used by the covered online service appears comparable to the Maryland's Online Data Privacy Act's (MODPA) DPIA requirement that controllers assess the likelihood of harm to consumers for each algorithm that is used. Similar to MODPA, South Carolina's requirement may pose compliance difficulties since entities may use many algorithms throughout the service, and South Carolina's requirement is not limited to assessing harms, but instead requires detailed descriptions of service algorithms (without defining "algorithm").
Prohibitions			
Data Minimization	Covered online services shall only collect, use, or share the minimum amount of a minor's personal data necessary to provide the specific elements of the covered online	***[From Nebraska's AADC:]*** Covered services shall only collect and use the minimum amount of a minor's personal	South Carolina's Act includes data minimization requirements seeking to limit unnecessary collection and use of minors' data. Similar to Nebraska, South Carolina restricts processing to

	South Carolina HB 3431	Comparable Elements from Enacted State Laws	Comparison & Analysis
	service with which a minor has knowingly engaged. Such personal data may not be used for reasons other than those for which it was collected [§ 39-80-40(A)]. A covered online service shall only retain a minor's personal data as long as necessary to provide the specific elements of an online service with which a minor has knowingly engaged [§ 39-80-40(B)].	data necessary to provide the specific elements of an online service with which the minor is knowingly engaged. [Sec. 5(1)] A minor's personal data may only be retained as long as necessary to provide the specific elements of the service with which the minor has knowingly engaged. [Sec. 5(3)] ***[From Vermont's AADC:]*** Covered businesses shall not collect, sell, share, or retain any minor's personal data that is not necessary to provide an online service, product, or feature with which the covered minor is ***actively and knowingly engaged.*** Covered businesses shall not use previously collected personal data for any purpose other than the purpose for which the personal data was collected, unless necessary to comply with the Vermont AADC. [§ 2449f(2)].	provide services that minors are **"knowingly"** engaged with, dropping the ambiguous "actively" term used in Vermont and other frameworks.
Dark Patterns	Covered online services are prohibited from using dark patterns. Use of dark patterns by a covered online service shall constitute an unlawful trade practice under Section 39-5-20 of the South Carolina Unfair Trade Practices Act. [§ 39-80-60(C)] "Dark Pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing	***[From Nebraska's AADC:]*** Covered services are prohibited from using dark patterns to subvert or impair covered minor autonomy, decision-making, or choice. [Sec. 8(2)]. "Dark pattern" means a user interface designed or manipulated with the effect of substantially subverting or impairing user	South Carolina's prohibition on dark patterns aligns with Nebraska's approach–both notably appearing to prohibit ***all dark patterns***. This is a major difference from dark patterns prohibitions in prior state privacy laws, which typically prohibit dark patterns in the context of obtaining consent or collecting personal information. As a result, it will be important for compliance teams to assess the impact of South Carolina's

	South Carolina HB 3431	Comparable Elements from Enacted State Laws	Comparison & Analysis
	user autonomy, decision making, or choice. [§ 39-80-10(5)]	autonomy, decision-making, or choice. Dark pattern includes any practice determined to be a dark pattern by the Federal Trade Commission as of January 1, 2024. [Sec. 2(6)]	broader dark patterns prohibition on covered online services, products, and features, especially in light of the Act's immediate effective date.
Geolocation	Precise geolocation information of minors cannot be collected by default unless necessary to the provision of the covered online service. [§ 39-80-40(D)]	***[From Maryland's AADC:]*** Prohibits processing any precise geolocation information of children by default, unless the collection of that precise geolocation information is strictly necessary for the covered entity to provide the online product requested and then only for the limited time that the collection of precise geolocation information is necessary to provide the service, product, or feature. [§14-4606(A)(5)].	Similar to Maryland's AADC, South Carolina prohibits collecting precise geolocation information of minors by default. However, the two frameworks differ where South Carolina prohibits precise geolocation data collection unless ***necessary*** to the provision of the service, but Maryland requires that such collection is ***strictly necessary***.
Targeted Advertising & Profiling	A covered online service shall not profile an individual the covered online service knows is a minor, unless profiling is necessary to providing the covered online service with which a minor has knowingly requested and is limited to only the aspects of the covered online service with which a minor is ***actively and knowingly engaged.*** [§ 39-80-40(F)] *Note: Profiling means "any form of automated processing of personal data to evaluate, analyze, or predict certain aspects relating to a user including, but not limited to, a user's economic situation, health, personal preferences, interests, reliability, behavior, location, or*	***[From Nebraska's AADC:]*** Covered services shall not profile a minor unless profiling is necessary to provide a service requested by the minor, and only with respect to the aspects of the service with which the covered minor is ***actively and knowingly engaged.*** *Note: Profiling means "any form of automated processing of personal data to evaluate, analyze, or predict certain aspects relating to a covered minor, including . . . economic situation, health, personal preferences, interests, reliability, behavior, location, or movements"* [Sec. 2(15)].	Restrictions on profiling and targeted advertising are comparable to Nebraska. Although similar, it is still worth noting that both South Carolina and Nebraska expressly require ***active and knowing*** engagement rather than just knowing.

	South Carolina HB 3431	Comparable Elements from Enacted State Laws	Comparison & Analysis
	movements." [§ 39-80-10(15)] Covered online services may not facilitate targeted advertising to minors. [§ 39-80-40(C)] *Note: Facilitate is undefined. South Carolina AADC defines targeted advertising as "displaying advertisements to an individual where the advertisement is selected based on personal data obtained or inferred from that individual's activities over time and across nonaffiliated websites or online applications to predict the individual's preferences or interest" and includes exceptions for first-party advertising, contextual advertising, advertisements related to an individual's request for information or feedback, and ad measurement.* [§ 39-80-10(19)]	Covered services shall not "facilitate" targeted advertising to minors. [Sec. 5(4)]. *Note: Facilitate is undefined. Nebraska AADC defines targeted advertising as "displaying advertisements to an individual when the advertisement is selected based on personal data obtained or inferred from that individual's activities over time and across nonaffiliated websites or online applications to predict the individual's preferences or interest" and includes exceptions for first-party advertising, contextual advertising, and ad measurement.* [Sec. 2(17)].	
Penalties & Enforcement			
Enforcement & Liability	The Attorney General is authorized to enforce these provisions, with penalties of treble the financial damages incurred resulting from violations of these provisions. **Officers and employees of the covered online service may be held personally liable for wilful and wanton violations**. [§ 39-80-80] *[FPF Note: Treble financial damages means a court triples the amount of actual damages awarded to the plaintiff, as*	***[From Nebraska's AADC:]*** $50,000 maximum civil penalty for each violation under the Act, recoverable exclusively by the AG. The Act appears to permit individuals to seek injunctive relief under the Nebraska Uniform Deceptive Trade Practices Act. ***[From Vermont's AADC:]*** Vermont ties enforcement to the state's	Unlike other frameworks that typically establish civil penalty caps per violation, South Carolina allows treble financial damages incurred from violations of the Act's provisions. Depending on the amount of actual damages assessed by a court for violations of these provisions, resulting penalties could be quite substantial. **Additionally and significantly, South Carolina is the first to expressly authorize the Attorney General to hold compliance employees personally liable for "wilful and wanton"**

	South Carolina HB 3431	Comparable Elements from Enacted State Laws	Comparison & Analysis
	authorized by law.] Violation of the prohibition against dark patterns is considered a violation of § 39-5-20 of South Carolina's Unfair Trade Practices Act, which includes a PRA for actual damages (and allows for treble damages). [§ 39-80-60(C)(1)]	Unfair or Deceptive Trade Practices Act, which provides for a private right of action of actual damages or $500 per initial violation. For AG enforcement, the maximum civil penalty is $10,000 per violation	**violations under the Act.**