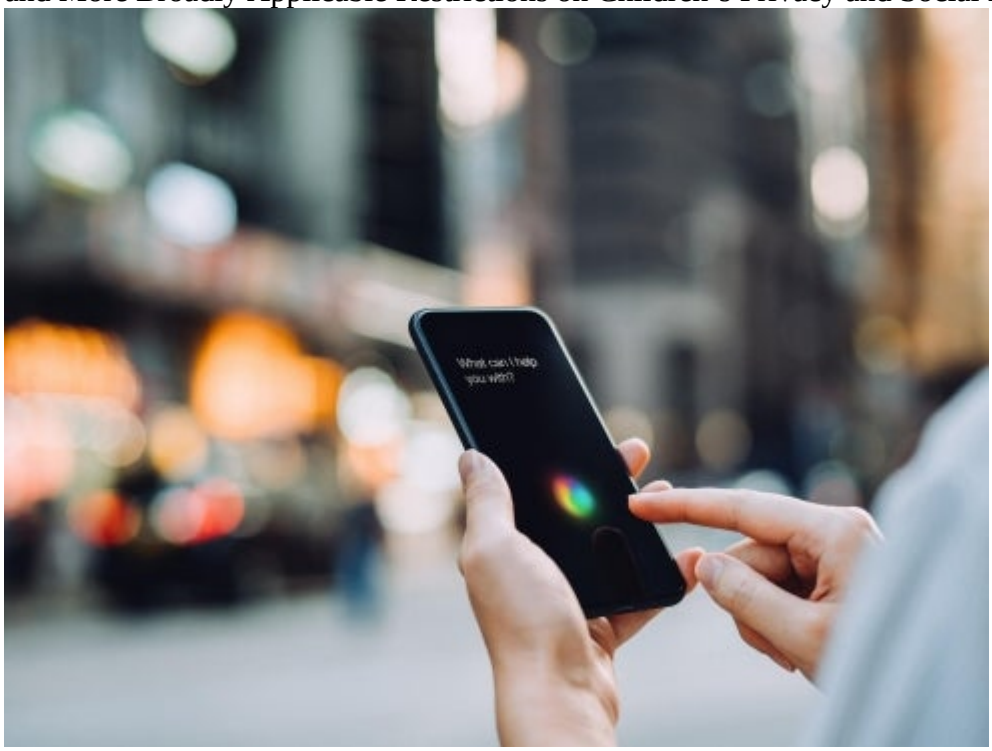
Blogs
July 14, 2023
Florida Enacts “Digital Bill of Rights” Combining Narrowly Applicable “Comprehensive” Privacy Provisions and More Broadly Applicable Restrictions on Children’s Privacy and Social Media Restrictions



On June 6, 2023, Florida Governor Ron DeSantis signed Senate Bill 262 into law. SB 262 is a departure from the comprehensive privacy laws enacted by other states for a variety of reasons, including its (1) ban on government-directed moderation of social media, (2) restrictions on online interactions with minors (somewhat akin to the California Age-Appropriate Design Code), and (3) establishment of a "digital bill of rights" that creates general consumer privacy rights similar in many respects to those adopted in other states but, unlike them, Florida's are narrowly applicable. Governor DeSantis has not shied away from saying the new law is directly aimed at "Big Tech," and the targeted application of certain aspects of the law reflects that goal.

The ban on government-directed moderation took effect on July 1, 2023, with the protections for minors and digital bill of rights provisions set to take effect on July 1, 2024.

Government Content Moderation Prohibition

Applicability. The new prohibitions on content moderation apply to a "governmental entity," defined as "any officer or employee of a state, county, district, authority, municipality, department, agency, division, board, bureau, commission, or other separate unit of government created or established by law and include any other public or private entity acting on behalf of such governmental entity."

Key Provisions. Government entities are prohibited from (1) communicating with social media platforms to request the removal of accounts or content; and (2) initiating or maintaining any agreement orworking relationship with social media platforms for the purpose of content moderation.

A social media platform is defined as "a form of electronic communication through which users create online communities or groups to share information, ideas, personal messages, and other content."

The statute exempts from this prohibition routine government entity account management, removal of content or accounts pertaining to the commission of a crime or violation of the state's public records law, and investigations or inquiries related to preventing imminent bodily harm, loss of life, or property damage.

Restrictions on Online Platforms That Are Likely To Be Predominantly Accessed by Minors

The new law also imposes restrictions intended to protect the online privacy and safety of children, meaning those under 18.

Applicability. Florida's child-related restrictions apply to online platforms that provide an online service, product, game, or feature "likely to be predominantly accessed by children." (The heightened revenue-related requirements for the application of the digital bill of rights provisions, discussed below, do *not* apply to the child-related restrictions.)

Key Provisions. Online platforms subject to the child-safety provisions of SB 262 must comply with the following requirements:

- **Avoidance of Harm.** Processing the personal information of a child if "the online platform has actual knowledge of or willfully disregards that the processing may result in substantial harm or privacy risk to children" is prohibited. "Substantial harm or privacy risk to children" is defined as the processing of information in a manner that may result in reasonably foreseeable (1) substantial physical injury, (2) economic injury, or (3) offensive intrusion into the privacy expectations of a reasonable child under the circumstances. Examples of "substantial harm or privacy risk to children" include mental health disorders, including the promotion of self-harm or eating disorders; patterns of use that indicate or encourage addictive behaviors; physical violence, including harassment and bullying; sexual exploitation, including sex trafficking and sexual abuse; promotion of alcohol, gambling, tobacco products, or narcotic drugs; and predatory, unfair, or deceptive marketing practices.
- **Profiling.** Profiling a child is restricted to when (1) the platform can demonstrate it has appropriate safeguards in place to protect children, and (2) the profiling is either necessary to provide the online service, product, or feature that the child is knowingly and actively engaged in, or the platform has a compelling reason such that the profiling will not pose a substantial harm or privacy risk to children.
- **Data Minimization.** Collecting, selling, sharing, or retaining any personal information from a child is restricted to when it is necessary to provide the child with the service, product, or feature in which they are actively and knowingly engaged or when they can demonstrate a compelling reason that such privacy practices do not pose a substantial harm or privacy risk to children. Likewise, using a child's personal information for any reason other than the initial reason the personal information was collected is prohibited unless an online platform gives a compelling reason that there is no substantial harm or privacy risk to children to do so.
- **Geolocation.** Collecting, selling, or sharing any precise geolocation data of children is prohibited unless the collection of precise geolocation data is strictly necessary for the platform to provide the requested service, product, or feature and the collection of precise geolocation data is limited to only the length necessary to provide the service, product, or feature. Moreover, platforms may not collect precise geolocation data without providing the child with an obvious sign for the duration of time the precise geolocation data is collected.
- **Dark Patterns.** "Dark patterns" (defined as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice and includes, but is not limited to, any practice the Federal Trade Commission (FTC) refers to as a dark pattern") are prohibited from being used to lead or encourage children (1) to provide personal information beyond the personal information reasonably expected to be provided for that online service, product, game, or feature, (2) to

forego privacy protections, or (3) to take any action for which the platform has actual knowledge (or willfully disregards such knowledge) that the action may result in substantial harm or privacy risk to children.
- **Limits on Age Estimation Data.** Using personal information collected to estimate age or age range for any other purpose, or retaining it longer than necessary to estimate age, is prohibited.

Digital Bill of Rights Child Provisions. In addition to the specific child-related restrictions, there are portions of the Florida Digital Bill of Rights (described below) that also address children's internet use. For example, parents or guardians may exercise their child's consumer rights on the child's behalf. In addition, processing the sensitive data of a known child requires either (1) affirmative authorization for such processing by a known child who is between 13 and 18 years old or (2) compliance with the notice and consent requirements of the Children's Online Privacy Protection Act (COPPA) for a known child under 13. Further, sensitive data, as defined by the Digital Bill of Rights, includes any personal data collected from a known child.

Florida's Digital Bill of Rights

Finally, SB 262 also includes the Florida Digital Bill of Rights (FDBR), which borrows heavily from recently enacted state consumer privacy laws but differs from them in key respects: the statute's narrow applicability and notable substantive differences, such as mandatory search engine disclosures and provisions governing surveillance by various devices.

Applicability. A controller is defined as a sole proprietorship, corporation, partnership, LLC, association, or legal entity that: (1) is organized or operated for the profit or financial benefit of its shareholders or owners; (2) conducts business in Florida; (3) collects personal data about consumers, or is the entity on behalf of which such information is collected; (4) determines the purposes and means of processing personal data about consumers alone or jointly with others; (5) makes in excess of **$1 billion** in global gross annual revenues; and falls into one of three other categories.

The other listed categories include: (1) the entity derives 50% or more of its global gross annual revenues from the sale of advertisements online, including targeted advertising or the sale of ads online; (2) the entity operates a consumer smart speaker and voice command component service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal communication, not including a motor vehicle or device associated with or connected to a vehicle operated by a motor vehicle manufacturer or manufacturer's subsidiary or affiliate; **or** (3) the entity operates an app store or digital distribution platform that offers at least 250,000 different software applications for consumers to download and install. If all five definitional requirements are met, and any one of the listed three categories is met, then the entity constitutes a controller under the FDBR. This likely means this portion of the law applies only to a small sliver of tech companies.

Key Provisions. The FDBR's key provisions include the following:

- **Search Engines.** Controllers operating a search engine must make available, in an easily accessible location on the webpage that does not require a consumer to log in or register to read, an up-to-date plain language description of the main parameters—that are individually or collectively the most significant in determining the ranking—and the relative importance of the main parameters, including the prioritization or deprioritization of political partisanship or political ideology in search results. The law provides that algorithms and information that would enable deception or harm, with reasonable certainty, to consumers through manipulation of search results are not required to be disclosed.
- **Surveillance.** The FDBR prohibits certain devices from using data collection features for the "purpose of surveillance." A device—with a voice or facial recognition feature, a video or audio recording feature, or any other electronic, visual, thermal, or olfactory feature that collects data—may not use those features for the purpose of surveillance by the controller, processor, or affiliate when those features are not in active

use by the consumer. Express authorization of the consumer is an exception to this provision.

- **Sensitive Data.** The FDBR defines sensitive information as a category of personal data that includes any of the following: personal data revealing an individual's racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; genetic or biometric data processed for the purpose of uniquely identifying an individual; personal data collected from a known child (see above); and precise geolocation data. Controllers are required to obtain the consumer's consent before processing sensitive data.
- **Consent.** The FDBR defines consent similarly to Europe's General Data Protection Regulation (GDPR) and other state privacy laws; namely, consent must be specific, informed, unambiguous, and freely given. Consent under the FDBR does not include acceptance of broad or general terms of use, consent obtained through dark patterns, or hovering, muting, pausing, or closing a given piece of content.
- **Privacy Notices.** Among other notice requirements, the FDBR has two distinctive notice requirements for controllers. Those engaged in the sale of sensitive data or biometric data must have explicit notices stating: "NOTICE: This website may sell your sensitive personal data" or "NOTICE: This website may sell your biometric data."
- **Consumer Rights.** Like the growing number of states that have passed comprehensive privacy laws, the FDBR establishes consumer rights to access, correct, delete, or obtain a copy of personal data collected by the controller. The FDBR includes the right to opt out of personal data processing for targeted advertising, for the sale of personal data, and for profiling in furtherance of a decision that produces a legal or similarly significant effect concerning a consumer. In addition, the FDBR includes a right to opt out of the collection of sensitive data, including precise geolocation data and personal data collected through the operation of a voice or facial recognition feature.

Rulemaking and Enforcement

SB 262 directs the Florida Attorney General's Office to issue rules creating standards for authenticating consumer requests, enforcement, data security, and authorized persons who may act on a consumer's behalf. The Attorney General may also issue rules implementing the restrictions on processing children's information.

The Attorney General is authorized to enforce violations of the new statute as an unfair or deceptive trade practice. After notice of an alleged violation, there is a discretionary 45-day cure period. The Attorney General can seek a civil penalty up to $50,000 per violation. (Penalties can be trebled in certain circumstances.)

Summer Associate Caitlin Edwards contributed to this blog post.

Authors

Explore more in

Privacy Litigation Privacy & Security