Committee on Commerce and Tourism

CS/CS/SB 262 — Technology Transparency

by Rules Committee; Commerce and Tourism Committee; and Senator Bradley

Prohibition on Government-Directed Content Moderation of Social Media Platforms

The bill creates s. 112.23, F.S., to prohibit employees of a governmental entity from using their position or any state resources to communicate with a social media platform to request that it remove content or accounts. Additionally, a governmental entity cannot initiate or maintain any agreements with a social media platform for the purpose of content moderation. These prohibitions do not apply to routine account maintenance, attempts to remove accounts or content pertaining to the commission of a crime, or efforts to prevent imminent bodily harm, loss of life, or property damage. These provisions are effective July 1, 2023.

Protections for Children Online

The bill creates s. 501.1735, F.S., to establish protections for children in online spaces. The bill prohibits an online platform that provides an online service, product, game, or feature likely to be predominantly accessed by children from processing or collecting the personal information of children in the following ways:

- Processing the personal information of any 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;
- Profiling a child unless certain criteria are met;
- Collecting, selling, sharing, or retaining any personal information that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged unless the online platform can demonstrate a compelling reason that does not pose a substantial harm or privacy risk;
- Using personal information of a child for any reason other than the reason for which the personal information was collected, unless the online platform can demonstrate a compelling reason that does not pose a substantial harm or privacy risk;
- Collecting, selling, or sharing any precise geolocation data of children unless the collection of the precise geolocation data is strictly necessary and then only for the limited time that the collection of the precise geolocation data is necessary;
- Collecting any precise geolocation data of a child without providing an obvious sign to the child for the duration of the collection that the precise geolocation data is being collected;
- Using dark patterns to lead or encourage children to provide personal information beyond what is reasonably expected to be provided for that online service, product, game, or feature;
- Forgoing privacy protections;
- Taking any action that the online platform has actual knowledge of or willfully disregards that may result in substantial harm or privacy risk to children; and

- Using any personal information collected to estimate age or age range for any other purpose or retain that personal information longer than necessary to estimate age.

The bill provides that a violation of s. 501.1735, F.S., is an unfair and deceptive trade practice actionable under part II of ch. 501, F.S., to be enforced by the Department of Legal Affairs. Additionally, the bill provides that the new provisions in s. 501.1735, F.S., do not establish a private cause of action.

The Florida Digital Bill of Rights

The bill creates ch. 501, part V, F.S., to provide a unified scheme to allow Florida's consumers to control the digital flow of their personal data. Specifically, it gives consumers the right to:

- Confirm and access their personal data;
- Delete, correct, or obtain a copy of that personal data;
- Opt out of the processing of personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of a decision that produces a legal or similarly significant effect concerning a consumer;
- Opt out of the collection or processing of sensitive data, including precise geolocation data; and
- Opt out of the collection of personal data collected through the operation of a voice recognition or facial recognition feature.

The bill defines "targeted advertising" as displaying to a consumer an advertisement selected based on personal data obtained from that consumer's activities over time across affiliated or unaffiliated websites and online applications used to predict the consumer's preferences or interests. However, the term does not include an advertisement that is based on the context of a consumer's current search query on the controller's own website or online application, or an advertisement that is directed to a consumer search query on the controller's own website or online application in response to the consumer's request for information or feedback.

The bill provides that a device that has a voice recognition feature, a facial recognition feature, a video recording feature, an 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 when such features are not in active use by the consumer, unless otherwise expressly authorized by the consumer.

The data privacy provisions of the bill generally apply to "controllers," businesses that collect Florida consumers' personal data, make in excess of $1 billion in global gross annual revenues, and meet one of the following thresholds:

- Derives 50 percent or more if its global gross annual revenues from the online sale of advertisements, including from providing targeted advertising or the sale of ads online;
- 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 activation; or

- Operates an app store or digital distribution platform that offers at least 250,000 different software applications for consumers to download and install.

The bill requires a controller who operates an online search engine to make available an up-to date plain language description of the main parameters that are most significant in determining ranking and the relative importance of those main parameters, including the prioritization or deprioritization of political partisanship or political ideology in search results. A controller must also conduct and document a data protection assessment of certain processing activities involving personal data. Additionally, the bill requires a controller to provide consumers with a reasonably accessible and clear privacy notice, updated at least annually.

The bill requires a controller in possession of deidentified data to do the following:
- Take reasonable measures to ensure that the data cannot be associated with an individual;
- Maintain and use the data in deidentified form;
- Contractually obligate any recipient of the deidentified data to comply with the data privacy provision of the bill; and
- Implement business processes to prevent inadvertent release of deidentified data.

The bill provides that a business organized or operated for the profit or financial benefit of its shareholders or owners, conducting business in Florida, and collecting personal data about consumers, or is the entity on behalf of which such information is collected, may not engage in the sale of personal data that is sensitive data without receiving prior consent from the consumer, or if the sensitive data is of a known child, without processing that data with the affirmative authorization for such processing. Additionally, a person who engages in the sale of personal data that is sensitive data must provide a notice on its website of such potential sale.

The bill provides exemptions for the use of certain data, and provides that certain restrictions on the collection and retention of data for particular purposes is prohibited.

The bill provides that a violation of ch. 501, part V, F.S is an unfair and deceptive trade practice actionable under ch. 501, part II, F.S., to be enforced by the Department of Legal Affairs (DLA). The DLA may provide a right to cure a violation of ch. 501, part V, F.S., by providing written notice of the violation and then allowing a 45-day period to cure the alleged violation. The bill also requires the DLA to make a report publicly available by February 1 each year on the DLA's website that describes any actions it has undertaken to enforce the bill. The bill provides that ch. 501, part V, F.S., does not establish a private cause of action.

The bill amends s. 16.53, F.S., to require all money recovered by the Attorney General for attorney fees, costs, and penalties in an action for a violation of this bill must be deposited in the Legal Affairs Revolving Trust Fund.

Florida Information Protection Act

The bill amends s. 501.171, F.S., to include an individual's biometric data and any information regarding an individual's geolocation in the Florida Information Protection Act's definition of "personal information," so that covered entities are required to notify the affected individual, the Department of Legal Affairs, and credit reporting agencies of a breach of biometric information or geolocation paired with an individual's first name or first initial and last name.

If approved by the Governor, or allowed to become law without the Governor's signature, these provisions take effect July 1, 2024.
Vote: Senate 40-0; House 110-2