THOMPSON HINE

Privacy & Cybersecurity Update

June 2023

Significant Changes to Florida's Privacy, Breach Notification, and Telemarketing Laws

In recent weeks, Florida Governor Ron DeSantis signed various data protection bills into law that will have a significant impact on organizations conducting business in the state. These laws create a comprehensive data privacy framework for Florida consumers, bolster privacy protections for children using online games and platforms, amend Florida's data breach notification requirements, and update the state's telemarketing law.

Florida Digital Bill of Rights

On June 6, Governor DeSantis signed Senate Bill 262 to create the Florida Digital Bill of Rights (FDBR). The law is scheduled to go into effect on July 1, 2024. Although the FDBR resembles other newly enacted state privacy laws, it has several unique aspects that add additional levels of analysis in determining multi-state privacy compliance.

Controller. To qualify as a data "controller" under the FDBR, an organization must have $1 billion in global gross revenue and satisfy one of the following:

- Derive 50% of its global gross revenue from the sale of advertisements online,
- Operate a consumer smart speaker and voice command service, or
- Operate an app store or digital distribution platform with at least 250,000 different software applications.

Based on these requirements, it is clear that the FDBR is targeting large technology and advertising companies. However, the terms "processor" and "third-party" do not include these same threshold criteria as a data controller, so there are still compliance implications for businesses that process data on behalf of data controllers, as well as those who receive personal data in a third-party capacity, but do not otherwise satisfy the data controller threshold.

Like other data privacy laws, the FDBR provides exemptions to various entities regulated by federal law (e.g., HIPAA, GLBA, FCRA) and does not apply to individuals who are acting in a commercial or employment capacity.

Consumer data privacy rights. The FDBR provides consumers residing in Florida with the following data privacy rights:

- Access rights, including a right to confirm whether the controller is processing any data at all,
- Correction rights,
- Deletion rights (concerning the data provided by or about the consumer),
- Data portability rights,
- Opt-out rights related to the sale of personal information, targeted marketing, and profiling,
- Opt-out rights related to the collection of sensitive data, and
- Opt-out of the collection of personal data through voice recognition features.

The FDBR sets forth specific processes for how data controllers must receive, process, and respond to individuals who exercise their privacy rights, including establishing a privacy rights appeals process.

Consent and Sensitive Data. The FDBR provides that a data controller must obtain a consumer's consent before they: (i) use the consumer's personal data for a purpose that is neither reasonably necessary nor compatible with the

purpose for which the personal data is processed, as disclosed to the consumer, (ii) process sensitive personal data of a consumer, and (iii) enroll the consumer in certain financial incentive programs. Like other privacy laws, the FDBR specifically prohibits using "dark patterns." Though the FDBR does not define dark patterns, it does state that consent cannot be obtained through acceptance of general or broad terms of use, or hovering over, muting, pausing, or closing a given piece of content.

The FDBR also creates obligations for organizations that are not otherwise deemed a data controller. Specifically, all for-profit entities that conduct business in Florida and collect personal data (and not just those entities that satisfy the data controller threshold) are prohibited from selling a consumer's sensitive data without first obtaining the consumer's consent or parental consent, where appropriate.

Surveillance. The FDBR also is distinct in its approach to regulating devices that involve voice or face recognition or have video or audio recording features. A device that has video recording, audio recording, facial recognition, voice recognition, or other electronic capability features and engages in "surveillance" may not use those features when not in active use by the consumer unless "expressly authorized" by the consumer. However, the FDBR does not define "surveillance" or "expressly authorized," and it appears the latter term is meant to be different than how the FDBR defines consent or how a consumer expressly authorizes the continued use of those features.

Controller and processor obligations. In addition to the typical obligations on controllers and processors seen in other states' laws, such as responding to data subject requests and requiring appropriate data processing contracts between controllers and processors, the FDBR creates a unique obligation on controllers and processors by limiting the retention of personal data. Controllers or processors may (subject to certain exceptions) only retain personal data until (i) the initial purpose for the collection was satisfied, (ii) the contract for which the data was collected or obtained is expired or terminated, or (iii) two years after the consumer's last interaction with the regulated business.

Privacy notices. The FDBR requires a controller to post a privacy notice, which must be updated annually. In addition to the notices regarding the website selling sensitive or biometric data mentioned above, if the controller operates a search engine, it is also required to disclose the parameters in ranking results. Specifically, the search engines must disclose the prioritization or deprioritization of political partisan or political ideology in search results.

Data protection assessments. Pursuant to the FDBR, controllers are required to undertake data impact assessments before engaging in several different processing activities, including: (i) processing for targeted advertising, (ii) sale of personal data, (iii) processing of personal data for profiling if the profiling presents a reasonably foreseeable risk of legal, deceptive, discriminatory, financial, reputational or physical harm, (iv) processing sensitive data, and (v) a catch-all category of any processing that presents a heightened risk of harm to consumers. The Florida attorney general is granted the authority to request such assessments at any time.

Enforcement. FDBR grants the Department of Legal Affairs the exclusive authority to enforce FDBR, and a violation of the FDBR is deemed an unfair and deceptive trade practice. The FDBR authorizes civil penalties of up to $50,000 per violation but does not create a private right of action. The FDBR includes a 45-day "cure period" that the Department of Legal Affairs, at its discretion, may provide before initiating an enforcement action.

Data Breach Notification Amendments

It is important to note that the FDBR amends the state's data breach notification law. As background, Florida's data breach statute previously identified the following categories of data as "personal information" that, if compromised, could potentially trigger a data breach notification requirement: government identifiers (e.g., Social Security number, a driver license or identification card number, a passport number, military identification number); certain financial account numbers and access codes; medical data and health insurance policy numbers; and certain usernames or e-mail addresses in conjunction with their passwords, provided any of the foregoing are in connection

to an individual's first name or first initial and last. The FDBR expanded this list of protected personal data to include an individual's biometric data and any information regarding an individual's geolocation, provided they are still connected to an individual's name.

This amendment is especially important for organizations that use cookies, pixels, and tags on their website to identify an individual, such as through their social media account, and track their location, as such data may be subject to data breach notification requirements. To be clear, the FDBR's definition of "geolocation," for purposes of its breach notification law, does not correspond to the definition of "precise geolocation data" used elsewhere in the law and likely is broader in scope.

Online Platforms and Children's Privacy

Protection of children in online spaces. The FDBR expanded the recently enacted Florida Student Online Personal Information Protection Act and provides additional privacy protections to children. This section of the FDBR applies only to online platforms, including social media platforms and online gaming platforms. Though online gaming platforms are undefined, the FDBR defines social medial platforms as "a form of electronic communication through which users create online communities or groups to share information, ideas, personal messages, and other content." The provision defines a child as any person under 18 years of age and applies to spaces predominantly likely to be accessed by children.

This section of the FDBR creates two prohibitions for such applicable platforms. First, they may not process any personal information belonging to children if they have actual knowledge or willfully disregard that processing such information may result in "substantial harm or privacy risk to children." This FDBR section explicitly defines "substantial harm or privacy risk" to include mental health disorders; addictive behaviors; physical violence, online bullying and harassment; sexual exploitation; the promotion and marketing of tobacco, gambling, alcohol, or narcotic drugs; and predatory, unfair, or deceptive marketing practices or other financial harms.

Second, applicable platforms are prohibited from "profiling" children, which is defined as "any form of automated processing performed on personal information to evaluate, analyze, or predict personal aspects relating to the economic situation, health, personal preferences, interests, reliability, behavior, location, or movements of a child." An applicable platform must demonstrate a compelling reason that profiling does not "pose a substantial harm or privacy risk to children" to be granted an exemption from this prohibition.

Telemarking Amendments

On May 25, 2023, Governor DeSantis signed into law House Bill (HB) 761, which amends (and consequently narrows the applicability) the Florida Telephone Solicitation Act (FTSA). The changes to the FTSA go into effect immediately, including with respect to certain putative class actions not yet certified as of May 25. This timing is especially important because privacy advocates have relied on the FTSA as the basis to bring a significant amount of class action lawsuits against organizations through the statute's "private right of action" framework.

HB 761 amended the FTSA to now only require a telemarketer to obtain consent from a consumer when they are contacting them (for telemarking purposes) through the use of an "automated system for the selection *and* dialing of telephone numbers," among other areas. The FTSA previously applied to such automated systems that could be used for the selection or dialing of telephone numbers.

In addition, HB 761 makes it easier for telemarketers to obtain the "signature" of consumers (which is a threshold needed to perform certain telemarketing activities under the law). The law, as previously written, allowed for such signature to be communicated to the telemarketer via electric or digital signature. HB 761 expanded this provision to allow such "signature" to be communicated to the telemarketer via an "act that demonstrates express consent," including by "checking a box indicating consent or responding affirmatively to receiving text messages, to an advertising campaign, or to an e-mail solicitation."

Pursuant to HB 761, before an individual is permitted to commence a legal action under the FTSA with respect to receiving text message solicitations in violation of the law, the called party "must notify the telephone solicitor that [they do] not wish to receive text messages from the telephone solicitor by replying 'STOP' to the number from which the called party received text messages from the telephone solicitor." Thereafter, within 15 days after receipt of such notice, the telemarketer must cease sending text messages, except for certain "confirmation" messages. Under HB 761, an individual may only bring a lawsuit against a telemarketer under the FTSA if they continue to receive telemarketing messages after this 15-day timeframe. This particular amendment will give businesses the opportunity to cure any of their non-compliant practices prior to a consumer being able to bring a legal action for such activities.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Brenna Fasko
216.566.5642
Brenna.Fasko@ThompsonHine.com

Marla M. Izbicky
312.998.4253
Marla.Izbicky@ThompsonHine.com