Published on *The National Law Review* https://natlawreview.com

2023: The Year of New Privacy Laws

Article By:

Briana Kelly

Jack Pringle, CIPP/US

Mallory Acheson, CIPM

It is shaping up to be the year of U.S. privacy laws! In addition to the Washington My Health My Data Act (see our previous article regarding the widespread implications of this enacted law), we have seen six (6) comprehensive privacy laws signed into law: Florida's Digital Bill of Rights (SB 262) (**FDBR**); Iowa's Act Relating to Consumer Data Protection (SF 262) (**ICDPA**); Indiana's Consumer Data Protection Act (SB 5) (**INCDPA**); Montana's Consumer Data Privacy Act (SB 384) (**MTCDPA**); Texas' Data Privacy and Security Act (HB 4) (**TDPSA**); and Tennessee's Information Protection Act (HB 1181) (**TIPA**).

Each state's consumer privacy law has many similarities and a few key differences in comparison with the other existing state consumer privacy laws (i.e., California's CCPA, Colorado's CPA, Connecticut's CTDPA, Virginia's VCDPA, and Utah's UCPA) (collectively, **Existing Comprehensive Privacy Laws**). In comparison to these Existing Comprehensive Privacy Laws, the **ICDPA** (effective on Jan. 1, 2025) is substantively similar to the UCPA; the **FDBR** (effective July 1, 2024), the **INCDPA** (effective Jan. 1, 2026), the TIPA (effective Jan. 1, 2025), and the **TDPSA** (effective July 1, 2024) largely track to the **VCDPA** with some limited variations; and the **MTCDPA** (effective Oct. 1, 2024) is structured similarly to the CTDPA. Thus, businesses that are already in compliance with the Existing Comprehensive Privacy Laws, should be familiar with many obligations of the **FDBR, ICDPA, INCDPA, MTCDPA, TIPA,** and **TDPSA.**

Below we provide an overview and comparison of some of the key aspects of the **FDBR, ICDPA, INCDPA, MTCDPA, TIPA,** and **TDPSA.**

Scope and Exemptions

The scope of the new privacy laws (excluding Florida) largely tracks with many of the Existing Comprehensive Privacy Laws applicability thresholds. The below chart details the scope of all currently enacted comprehensive privacy laws:

State	Business	Monetary	Numbers of	Sell/Share	Technology	Platform
California	Conducts business in the State of California, and that satisfies one or more of the following thresholds:	$25,000,000	100,000 consumers or households	Derives 50% or more of annual revenues from selling or sharing consumers' personal information		
Colorado	Conducts business or produce commercial products or services that are intentionally targeted to Colorado residents and that meet one of the following thresholds:	-	100,000 consumers	Derives revenue or receives a discount on the price of goods or services from the sale of personal data + processes or controls the personal data of 25,000 or more consumers		
Connecticut	Conducts business in Connecticut or persons that produce products or services that are targeted to residents of Connecticut and that during the preceding calendar year meet one of the following thresholds:	-	100,000 consumers	Derives more than 25% of gross revenue from sale of personal data + control or process personal data of not less than 25,000 consumers		
Florida	Conducts business in Florida or produces a product or	$1,000,000,000		Derives 50% or more of its global gross annual revenues	Operates a consumer smart speaker and voice	Operates an app store or a digital distribution platform that

State	Business	Monetary	Numbers of	Sell/Share	Technology	Platform
	service used by residents of Florida and satisfies at least one of the following:			from the sale of advertisements online, including providing targeted advertising or the sale of ads online	command component service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation	offers at least 250,000 different software applications for consumers to download and install
Indiana	Conducts business in Indiana or targets Indiana residents and during a calendar year meets one of the thresholds	-	100,000 consumers	Derives over 50% of gross revenue from sale of personal data + control or process personal data of at least 25,000 consumers		
Iowa	Conducts business in Iowa or produces products or services that are targeted to residents of Iowa, and during a calendar year meets one of the following thresholds:	-	100,000 consumers	Derives over 50% of gross revenue from sale of personal data + controls or processes personal data of 25,000 or more consumers		
Montana	Conducts business in Montana or produce products or services targeted to residents of Montana and meet one of	-	50,000 consumers	Derives over 25% gross revenue from sale of personal data + controls of processes personal data of 25,000 consumers		

State	Business	Monetary	Numbers of	Sell/Share	Technology	Platform
	the following thresholds:					
Tennessee	Conducts business in Tennessee or target products or services to Tennessee consumers, meet the revenue threshold and one other threshold:	$25,000,000 (+ another category)	175,000 consumers	Derives over 50% of gross revenue from sale of personal data + controls or processes personal data of 25,000 or more consumers		
Texas	Conducts business in Texas or produces a product or service consumed by residents of Texas	-		Processes or engages in the sale of personal data		
Utah	Conducts business in Utah or produces a product or service that is targeted to consumers who are residents of Utah	$25,000,000 (+ another category)	100,000 consumers	Derives over 50% of gross revenue from sale of personal data + controls or processes personal data of 25,000 or more consumers		
Virginia	Conducts business in the Common wealth or produce products or services that are targeted to residents of the Comm onwealth and that (i) during a calendar	-	100,000 consumers	Derives over 50% of gross revenue from sale of personal data + control or process personal data of at least 25,000 consumers		

State	Business	Monetary	Numbers of	Sell/Share	Technology	Platform
	year meet one of the following thresholds:					

Exemptions

The **FDBR, ICDPA, INCDPA, MTCDPA, TIPA, and TDPSA** provide protections to consumers acting only in an individual or household context, and explicitly exclude consumers acting in a commercial or employment context. Each law also expressly exempts financial institutions, affiliates of financial institutions, data subject to the Gramm Leach Bliley Act (GLBA), data regulated by the Family Educational Rights and Privacy Act (FERPA), persons who are subject to the Health Insurance Portability and Accountability Act (HIPAA), nonprofits, and higher education institutions. Of note, the **INCDPA** also exempts from applicability public utilities and affiliated service companies, and licensed riverboat casino owners operating facial recognition programs approved by the Indiana gaming commission.

Consumer Rights

Consumer Rights	California	Colorado	Connecticut	Florida	Indiana	Iowa	Montana	Tennessee	Texas	Utah	Virginia
Know	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Access	Yes	Yes	Yes	Yes	Partial	Yes	Yes	Yes	Yes	Yes	Yes
Data Portability	Yes	Yes	Yes	Yes	Partial	Partial	Yes	Yes	Yes	Partial	Yes
Deletion	Partial	Yes	Yes	Yes	Yes	Partial	Yes	Yes	Yes	Partial	Yes
Correction	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes
Non-discrimination	Yes	Yes	Yes	Yes	Yes	Partial	Yes	Yes	Yes	Partial	Yes
Opt-out of Sale	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Partial	Yes
Opt-out of Targeted Advertising/Shari	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Partial	Yes

Consumer Rights	California	Colorado	Connecticut	Florida	Indiana	Iowa	Montana	Tennessee	Texas	Utah	Virginia
ng											
Opt-out of Profiling	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes
Opt-out of Sensitive Data	No	No	No	Yes	No	No	No	No	No	No	No
Opt-out of Collection Collected Through Voice or Facial Recognition	No	No	No	Yes	No	No	No	No	No	No	No
Appeals	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes

Obligations and Restrictions

General Obligations

As with Existing Comprehensive Privacy Laws, businesses subject to the FDBR, ICDPA, INCDPA, MTCDPA, TIPA, and TDPSA must:

1. Adopt and implement reasonable administrative, technical, and physical data security practices.
2. Be transparent in their accessible and meaningful privacy notice.
3. Avoid unlawful discrimination against consumers exercising their consumer rights.
4. Ensure contracts control relationships with third parties.
5. Obtain consent from a consumer prior to processing their sensitive data.

DPIA

Similar to Colorado, Connecticut, and Virginia, the **FDBR, INCDPA, MTCDPA, TIPA,** and **TDPSA** require annual data protection impact assessments (DPIAs).

DPIAs are required under the **FDBR, INCDPA, TIPA,** and **TDPSA** (activities created or generated after July 1, 2023, for the FDBR and after July 1, 2024, for INCDPA and TIPA) for the following activities: (a) processing of data for purposes of targeted advertising; (b) the sale of personal data; (c) the processing of data for purposes of profiling if certain risk factors are met; (d) the processing of

sensitive data; and (e) any processing activities that present a heightened risk of harm.

Businesses subject to the **MTCDPA** must have compliant DPIAs by Jan. 1, 2025, if they engage in the following: (a) targeted advertising; (b) the sale of personal data); (c) the processing of personal data for the purposes of profiling in which the profiling presents certain reasonably foreseeable risks; and (d) the processing of sensitive data.

Tennessee Affirmative Defense

Unlike any other state's privacy law, the **TIPA** establishes a first of its kind affirmative defense against enforcement for businesses that reasonably conform to the NIST Privacy Framework or other documented policies, standards, and procedures designed to safeguard consumer privacy. However, it is presently unclear what 'reasonably conformity' entails or how invoking this affirmative defense would impact litigation.

Children in Montana and Florida

The **MTCPDA** expands privacy rights for children between the ages of 13 and 16 like California and Connecticut. Businesses are prohibited from processing personal data for the purpose of targeted marketing or the sale of data without consent if the business has actual knowledge that the consumer is between 13 and 16 years of age.

The **FDBR** adds online protections for children similar to California's Age-Appropriate Design Code Act (**CAADCA**, A.B. 2273) (see our previous article regarding the implications of the **CAADCA**). The **FDBR** prohibits social media platforms and online game or gaming platforms (online platform) that provide online services, products, games, or features likely to be predominately accessed by children from processing the personal data of any child if the online platform has actual knowledge of or willfully disregards that such processing may result in substantial harm or privacy risk to children. Under the **FDBR**, substantial harm or privacy risk to children means processing personal information in such a way that it may result in "any reasonably foreseeable substantial physical injury, economic injury, or offensive intrusion into the privacy expectations of a reasonable child under the circumstances," including mental health disorders, patterns of use that indicate or encourage addictive behaviors, violence, sexual exploitation, promotion of drugs, predatory practices, and financial harm.

Online platforms are also prohibited from profiling children unless all of the following are met: (1) the online platform can demonstrate it has appropriate safeguards in place to protect children; (2) profiling is necessary to provide the online service, product, or feature requested with which children are actively and knowingly engaged; and (3) the online platform can demonstrate a compelling reason that profiling does not pose a substantial harm or privacy risk to children. The **FDBR** also restricts the use of children's geolocation data and the use of dark patterns to lead, or encourage, a child to take certain actions, similar to the **CAADCA**. Subject businesses will likely have to conduct a privacy assessment to determine if their online platform creates risks to children and to ensure that any children's personal data will not be used beyond what is minimally necessary.

Global Privacy Signals

Both the **MTCDPA** and **TDPSA** will require subject businesses to recognize global browser privacy signals by Jan. 1, 2025.

Selling Data in Texas and Florida

The **TDPSA** and **FDBR** require subject businesses to notify consumers if they are selling sensitive and/or biometric data. The **TDPSA** requires the following specific language within privacy notices if the subject business sells such data: “NOTICE: We may sell your sensitive personal data” and/or “NOTICE: We may sell your biometric data.” Similarly, the **FDBR** requires subject businesses to have the following similar language in privacy notices: “NOTICE: This website may sell your sensitive personal data” and/or “NOTICE: This website may sell your biometric personal data.”

Florida’s Unique Requirements – Additional Opt-Out Rights, Consumer Consent, Voice and Facial Recognition, Retention, and Government Influence

In addition to the right to opt-out of targeted advertising, the sale of personal data, and certain types of profiling, **FDBR** also provides consumers with the right to opt-out of the collection or processing of sensitive data and the collection of personal data through voice recognition or facial recognition features. **FDBR** also requires consumer consent for the processing and sale of sensitive data. Additionally, any device that has voice and/or facial recognition, video and/or audio recording, or any other electronic, visual, thermal, or olfactory feature that collects data may not use such features for surveillance when such features are not in active use by the consumer, unless otherwise authorized by the consumer.

Subject businesses are prohibited from using or retaining personal data after the expiration or termination of a contract or two (2) years after the consumer’s last interaction with the subject business. However, the **FDBR** provides four exemptions to its retention requirements: (1) provide a good or service requested by the consumer, or reasonably anticipate the request within the context of an ongoing business relationship; (2) debug to identify and repair errors; (3) enable solely internal uses that are reasonably aligned with the expectations of the consumer; and (4) the subject business processes personal data pursuant to exemptions for certain uses of consumer personal data.

Unlike any other state privacy laws, the **FDBR** limits government employees and officers’ interaction with social media platforms. Under the **FDBR**, government employees and officers are prohibited from using their positions or state resources to request social media platforms remove content or accounts and from initiating or maintaining any agreements or working relationships with social platforms for the purpose of content moderation.

Enforcement

The **FDBR, ICDPA, INCDPA, MTCDPA, TIPA,** and **TDPSA** do not provide a private right of action, thus each state’s Attorney General has exclusive authority to enforce each privacy law. Each law’s cure period varies:

- **ICDPA** provides a non-sunsetting right to cure violations within 90 days of receiving notice of a violation.
- **TIPA** provides a non-sunsetting 60 days right to cure period.
- **MTCDPA** provides a sunsetting 60-day cure period, which sunsets after April 1, 2026.
- **FDBR** provides a non-sunsetting 45-day cure period.
- **ICDPA** provides a non-sunsetting 30-day cure period.
- **TDPSA** provides a non-sunsetting 30-day cure period.

Businesses that are found to violate the **ICDPA, INCDPA, TIPA,** and **TDPSA** will be subject to monetary penalties of up to $7,500 per violation. The FDBR authorizes civil penalties of up to $50,000 per violation and grants the Florida Department of Legal Affairs rulemaking authority to assist in the implementation of FDBR. Under the TIPA, a court may also award treble damages for any willful or knowing violations. Of note, the **MTCDPA** does not specify any specific penalties or capped damage amounts.

Next Steps

As noted above, many of the obligations these new privacy laws impose on businesses are not new obligations, rather extensions of Existing Comprehensive Privacy Laws obligations to new states. A good initial step and a continuous step for those already complying with Existing Comprehensive Privacy Laws is to ensure its data mapping is regularly updated. Knowing your businesses data flows can help ensure you have proper procedures are in place for notice, consent, and consumer request requirements.

There are over a dozen other states, including Oregon, Washington, Hawaii, and New Hampshire, with pending consumer privacy legislation.

National Law Review, Volume XIII, Number 206