Articles + Publications | August 5, 2024

Texas and Oregon Data Privacy Laws: Applicability Concerns and Enforcement

Privacy & Cybersecurity Newsletter

WRITTEN BY

Laura L. Ferguson | Alexander R. Cox

RELATED OFFICES

Hartford | Houston

Two state privacy laws that pose unique applicability concerns went into effect July 1, 2024: the Oregon Consumer Privacy Act (the "OCPA") and the Texas Data Privacy and Security Act (the "TDPSA").[1] Generally following the Virginia model, both the Texas and Oregon laws include important nuances that businesses will have to comply with.

U.S. state privacy laws typically take one of three routes of applicability: revenue thresholds, data-processing thresholds, and/or lack of a small-business designation. Texas is the first state relying on the absence of a small-business designation to determine applicability. On top of these applicability thresholds, each state privacy law has limited exemptions for personal information and/or institutions that process personal information, such as employment data, consumer financial information or protected health information. These nuances in the Texas and Oregon laws are discussed below.

Applicability Concerns in Texas

As we discussed in our update from April 2024, Texas' general consumer privacy law went into effect July 1, 2024. The TDPSA casts a wide net, applying to any person that: (1) conducts business in Texas or produces a product or service consumed by Texas residents;[2] (2) processes or engages in the "sale" of personal data;[3] and (3) is not a small business as defined by the United States Small Business Administration. Note, however, that small businesses are not fully exempt from the TDPSA; small businesses are still restricted from selling sensitive data without consumer consent under the TDPSA.

A small business is determined by firm revenue (ranging from $2.25M to $47M) **or** by employment (from 100 to 1,500 employees) depending on the firm's industry. While most firms will find multiple of the North American Classification System Codes (NAICS) applicable, they will have to self-identify which industry is most applicable to them according to the size standard table.[4] Notably, the thresholds for qualifying as a small business are much more restrictive than the $25 million revenue thresholds employed by California and Utah, and so many more businesses will fall under the Texas law than the respective laws in those other states.

The TDPSA, like other state privacy laws, provides important exemptions for financial institutions and data subject to the federal Gramm-Leach-Bliley Act (the "GLBA"); Health Insurance Portability and Accountability Act

("HIPAA") covered entities and business associates; nonprofits; institutions of higher education; state agencies and political subdivisions; and electric utilities, power generation companies, and retail electric providers. Additional data-level exemptions include employment and human resources data, B2B data, HIPAA-protected health information, data subject to the Fair Credit Reporting Act ("FCRA"), and the Family Educational Rights and Privacy Act ("FERPA"). Otherwise, the TDPSA applies to all "personal data," meaning "any information, including sensitive data, that is linked or reasonably linkable to an identified or identifiable individual."

Oregon Applicability Concerns

Oregon's general consumer privacy law, as discussed in our December 2023 update, also went into effect July 1. The OCPA imposes transparency and disclosure requirements on a "controller" (an individual or legal entity who, "alone or jointly with another person, determines the purposes and means for processing personal data") who either: conducts business in Oregon, **or** produces products or services that are targeted at the residents of Oregon; **and** that during a calendar year:

- Controls or processes personal data of not less than 100,000 Oregon residents, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; **or**
- Controls or processes personal data of not less than 25,000 Oregon residents and derives more than 25 percent of its gross revenue from the sale of personal data.

Unlike most other state privacy laws, the OCPA does not have a revenue threshold for entities to be subject to privacy obligations. The OCPA does not exempt small businesses.

Applicability for entities under the Oregon law can be difficult to navigate because of its particularly long list of exemptions. Notably, OCPA has no GLBA entity-level exemption. The OCPA follows the California Consumer Privacy Act (the "CCPA") in exempting only *data* subject to the GLBA. As a result, GLBA regulated financial institutions will need to review the other available exemptions for various categories of financial institutions to determine if another entity-level exemption applies.

The OCPA exempts banks and credit unions and their affiliates that are only and directly engaged in financial activities. In addition, the OCPA exempts information collected, processed, sold, or disclosed by a "financial institution, as defined in ORS 706.008, or a financial institution's affiliate or subsidiary that is only and directly engaged in financial activities, as described in 12 U.S.C. 1843(k), as in effect on the effective date of this 2023 Act." "Financial institution" under Oregon law means an insured institution (FDIC insured), an extranational institution, a credit union, a bank, or a list of other banking related entities. The OCPA also exempts insurance producers, insurers, holders of a TPA license, and "information that originates from, or is intermingled so as to be indistinguishable from, information described in [the GLBA and regulations adopted to implement the GLBA] and that a licensee, as defined in ORS 725.010, collects, processes, uses or maintains in the same manner as is required under the laws and regulations specified in [the GLBA]." These Oregon-specific entity exemptions are narrower than exemptions for GLBA-covered entities found in other state privacy laws, as the GLBA often applies to broader categories of financial institutions on top of banks and credit unions, including finders, non-bank and alternative lenders, retailers that extend credit to consumers, money transmitters, tax preparers, mortgage brokers, securities broker-dealers, investment advisors, investment companies, and others. The OCPA, in summary, contains a complicated array of entity-level, data-specific, as well as employment-related, activity-

specific, and processing-related exemptions.

Our comparison chart lines up all these statutes, as a quick guide for comparative analysis. For example, the laws have different definitions of sensitive data; the OCPA includes a unique protection for sensitive data about a consumer's status as transgender or nonbinary and status as a victim of crime. Both the Oregon and Texas laws contain the typical consumer rights that most other state privacy laws have. In terms of controller obligations, both laws require notice to the consumer and include contractual requirements for third parties; neither mandates privacy policies, although (for both OR and TX) required disclosures may be incorporated in privacy policies.

Enforcement Guidance

Enforcement under TDPSA

The Texas Attorney General is granted sole enforcement and investigative authority over consumer privacy data regulation under the TDPSA. The AG is required to: (1) make information available to consumers detailing their rights and controller and processor responsibilities; and (2) establish an online portal by July 1, 2024, for consumers to submit complaints.

If violators do not cure the violation within the cure period and provide the attorney general with evidence of the cure, they can be fined $7,500 per violation. The cure period is 30 days and, unlike other state privacy laws, will not sunset but rather it will continue in perpetuity. The entity must also provide the attorney general with a written statement that they have: (1) cured the violation, (2) notified the consumer their privacy violation was addressed (if their contact information was made available), and (3) made changes to internal policies, if necessary, to ensure the violation won't be repeated.

There is no private right of action under the TDPSA.

Enforcement under OCPA

The OCPA will be enforceable only by the Oregon Attorney General if the Oregon Office of the Attorney General issues notice of a violation to the controller prior to initiating any action. Possible remedies include an injunction and a civil penalty of up to $7,500 per violation. However, the Act provides for a 30-day right to cure period, which will terminate on January 1, 2026, and there is a five-year statute of limitations.

The OCPA does not provide a private right of action.

The Horizon for State Privacy Laws

After Oregon and Texas, up next is Montana's new privacy law, the Montana Consumer Data Privacy Act ("MCDPA"), which will become effective on October 1, 2024. Following Montana, a number of other states have comprehensive privacy laws becoming effective in January of 2025, including Delaware, Iowa, Nebraska, New Hampshire, and New Jersey.

—

[1] Under the TDPSA, businesses will have a slightly longer grace period to comply with the global opt-out technology provision, which takes effect January 1, 2025. In Oregon, the effective date for non-profits (which unlike most other state privacy laws, are not exempt) is delayed until July 1, 2025.

[2] See Theodore Augustinos and Laura Ferguson, Texas Joins the State Privacy Law Landscape on July 1, 2024: The Texas Data Privacy and Security Act, (April 5, 2024) for an analysis of the implications of Texas extending application to persons that produce a product or service consumed by Texas residents ("In contrast to other general consumer privacy laws, which apply to persons "doing business" in the state, the Texas statute extends to persons that produce a product or service consumed by Texas residents, presumably with no other nexus to Texas. . .").

[3] Tex. Bus. & Com. Code § 541.001. The TDPSA defines "sale of personal data" as "the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party. The term does not include: (A) the disclosure of personal data to a processor that processes the personal data on the controller's behalf; (B) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer; (C) the disclosure or transfer of personal data to an affiliate of the controller; (D) the disclosure of information that the consumer: (i) intentionally made available to the general public through a mass media channel; and (ii) did not restrict to a specific audience; or (E) the disclosure or transfer of personal data to a third party as an asset that is part of a merger or

Privacy Rights Act (CPRA) than Virginia's privacy law.

[4] *See* U.S. Small Business Administration, Table of Size Standards, https://www.sba.gov/document/support-table-size-standards.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber