AN A.S. PRATT PUBLICATION
OCTOBER 2024
VOL. 10 NO. 8

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 10 **NUMBER 8** **October 2024**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... (908) 673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2024–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

New State Data Protection Laws Will Impact Business Nationwide: What You Need to Know

By Mary J. Hildebrand*

In this article, the author reviews the key elements of new data protection laws in Texas, Florida, and Oregon.

Currently, 19 states have comprehensive data protection laws scheduled to become effective through 2026. Since adoption of the California Consumer Privacy Act of 2018 (CCPA), the pace of adoption has continued to accelerate. New laws in Texas, Florida, and Oregon have potentially significant implications for companies that conduct business there.

THE TEXAS ACT

The Texas Data Privacy and Security Act (Texas Act) approved by the Texas legislature and signed by Governor Abbott, catapults Texas into uncharted territory. By establishing an exceptionally low jurisdictional threshold, the Texas Act ensures coverage of companies that are not (or not yet) required to comply with any other state data protection law. The Texas Act is not just one among many: it demands specific attention.

To date, all state data protection laws, including the Texas Act, regulate entities that "conduct business" in the state, and/or produce "products or services" targeted to or consumed by residents of the state; and do not require regulated entities to maintain a place of business or have employees in the state. To assert jurisdiction, 17 state data protection laws also require that an entity meet some combination of the following factors. They must

- Buy, sell, share, and/or process the personal information of a minimum number of state residents;
- Derive a specific percentage of annual revenue from the sale of personal information; and/or
- Meet an annual revenue threshold.

The Texas Act (along with the Nebraska Data Privacy Act, which becomes effective on January 1, 2025) is an outlier because jurisdiction does not depend on any of these elements.

---

* The author, a partner in Lowenstein Sandler LLP, may be contacted at mhildebrand@lowenstein.com.

The Texas Act applies to any entity that meets the following conditions:

- Conducts business in Texas or produces products or services that Texas residents consume;
- Processes any volume of personal data or engages in the sale of personal data;

  and

- Does not qualify as a small business, as defined by the U.S. Small Business Administration (the SBA).

The potential impact of the Texas Act should not be underestimated. As the second most populous state after California and the largest in size after Alaska, Texas has a burgeoning economy. According to the U.S. Department of Commerce's Bureau of Economic Analysis, the real gross domestic process for Texas in the third quarter of 2023 was $2.5 trillion in goods and services/year.

There are undoubtedly many thousands of organizations that conduct business in Texas or produce products or services consumed by Texas residents. Further, it is reasonable to assume that a significant percentage of them also process the personal data of state residents (broadly defined as performing an operation or set of operations on personal data such as collection, usage, storage, disclosure, analysis, deletion, or modification). A relatively smaller number of these organizations will sell the personal data (i.e., share, disclose, or transfer personal data to a third party for monetary or other valuable consideration), making them also subject to regulation. Small businesses qualified by the SBA are exempt, except for one important obligation: the business must obtain consumers' prior consent to "sell" sensitive personal data.

The Texas Act imposes a full range of obligations on regulated entities, such as the timely honoring of consumer requests to exercise a broad array of rights, including the right to delete personal data and opt out of targeted advertising, requiring its service providers and contractors to comply with the Texas Act, conduct data protection assessments, practice data minimization, monitor compliance, provide training, and many others. Unlike the CCPA, which also regulates personal data related to employees, independent contractors, job applicants, and business-to-business business contact data processed by the regulated entity, the Texas Act only applies to personal data when a state resident acts in an individual or household context. The Texas Act includes coverage exclusions and exemptions common to other state data protection laws, such as excluding entities and/or data regulated by certain sector-specific laws (e.g., Health Insurance Portability and Accountability Act of 1996; Gramm-Leach-Bliley Act).

The Texas Attorney General has exclusive enforcement authority under the Texas Act, and consumers are prohibited from pursuing private causes of action. On June 4, 2024, Texas Attorney General Paxton announced the launch of "a major data privacy and

security initiative to protect Texans' sensitive data from illegal exploitation by Tech, AI and other companies." Housed in the Consumer Protection Division of the OAG, the new team will focus on "aggressive enforcement of Texas Privacy Laws . . . and is poised to become among the largest in the country. . . ."

THE FLORIDA LAW

Florida's Digital Bill of Rights Law (Florida Law) aims to regulate "Big Tech" by implementing a higher jurisdictional threshold than any other state data protection law to date. It regulates entities that conduct business in Florida, collect personal data from state residents (and determine the purpose or means of processing the personal data), and satisfy the following conditions:

- Has an annual global revenue of more than $1 billion; and
- Meets one of the following criteria:
    - Derives 50 percent of its global gross annual revenue from the sale of advertisements online;
    - Operates a consumer smart speaker and voice command 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 with at least 250,000 different software applications for consumers to download and install.

We do not recommend making quick assumptions that the Florida Law does not apply (and therefore that you need not review the rest of the statute) because at first glance your organization does not seem to meet the revenue threshold. When evaluating the Florida Law, keep the following facts in mind:

- The Florida Law takes an expansive view of "global annual revenue" by combining the revenue of all companies that "control" or are "controlled by" an organization. Control is broadly defined as:
    - (i) Ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security;
    - (ii) Control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or
    - (iii) The power to exercise a controlling influence over the management of a company.

- The Florida Law was adopted along with two accompanying statutes that also merit attention:
    - With limited exceptions, since July 1, 2023, government -directed social media moderation has been prohibited;[1] and
    - Effective July 1, 2024, online platforms face serious restrictions when providing services that children are likely to access.[2]

Relative to other state data protection laws, the Florida Act and the accompanying statutes will apply to a more limited number of entities. When an organization meets the threshold, however, the Florida Law imposes an array of obligations and enforcement penalties. It is worth a closer look.

THE OREGON ACT

The Oregon Consumer Privacy Act (Oregon Act) puts Oregon on the list of states that regulate the data processing activities of for-profit businesses and nonprofit organizations.

Jurisdiction under the Oregon Act is determined by a similar combination of factors as other state data protection laws, although there is no minimum annual revenue requirement. It regulates entities that either "conduct business" in Oregon or "produce products or services that are targeted to state residents"; and, during a calendar year, (i) controls or processes the 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 (ii) controls or processes the 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.

Executives and board members of nonprofits must be attentive to the specific standards of each state law because there is no uniform definition of "nonprofit" and, unlike the Colorado Privacy Act which applies to nonprofits generally, other states may grant various exemptions. For example:

- The Oregon Act, which begins regulating nonprofits that meet the jurisdictional threshold on July 1, 2025, grants narrow exemptions to nonprofits engaged in the detection and prevention of insurance fraud and the noncommercial activity of nonprofits that provide programming to radio or television.
- The Virginia Consumer Data Protection Act excludes nonprofits organized under the Virginia Nonstock Corporation Act and tax-exempt organization under the Internal Revenue Code.[3]

[1] Section 112.23, Fla. Stat.

[2] Section 501.1735, Fla. Stat.

[3] Sections 501(c)(3), 501(c)(6), or 501(c)(12).

- The Utah Consumer Privacy Act and the Tennessee Information Protection Act exclude nonprofits incorporated under their respective state laws.
- Although the CCPA generally excludes "nonprofits," it leaves open the possibility that a nonprofit may become a regulated entity due to affiliate relationships with a regulated business with whom the nonprofit shares branding and personal information.

Consequently, a nonprofit may be regulated by the data protection law in one state but not in others, and two nonprofits in the same jurisdiction may be required to comply with different statutory requirements. As state laws continue to proliferate, so does the scope and complexity of data protection laws applicable to nonprofits, regulating many for the first time.

IN SUMMARY

- The Texas Data Privacy and Security Act has broader jurisdiction than any other state data protection law and will regulate the data processing activities of thousands of companies for the first time.
- Florida's Digital Bill of Rights Law aims to regulate "Big Tech" by implementing a higher jurisdictional threshold than any other state data protection law, but the $1 billion threshold may be deceiving.
- The Oregon Consumer Privacy Act places Oregon on the relatively short list of states that regulate the data processing activities of nonprofit organizations.

CONCLUSION

The Texas, Florida and Oregon laws are notable in their own ways and warrant scrutiny from business leaders and nonprofit executives at organizations of all sizes, even if data protection is a relatively new item on the agenda. Nonprofits have some lead time to prepare for the Oregon Act, but there is no shortage of immediate tasks to prepare for compliance (or to comply with other applicable state data protection laws). To avoid regulatory action, expense, and reputational damage, it is critical to stay ahead of the curve.