PAUL HASTINGS

Stay Current

October 2023

Follow @Paul_Hastings

Preparing for New State Privacy Laws in 2024

By Brianne Powers & Aaron Charfoos

Introduction

As we enter into the final few months of the year, it is important for companies operating in the United States to not only assess the implementation of the compliance requirements for the four new comprehensive state privacy laws (the California Privacy Rights Act, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, and the Connecticut Data Privacy Act) that have already gone into effect this year, but also to prepare for those state privacy laws that will go into effect over the next 12 months.

One More New Privacy Law This Year!

Utah Consumer Privacy Act: The Utah Consumer Privacy Act goes into effect on **December 31, 2023**. Like the other state privacy laws, there is a certain threshold that must be met: $25 million in annual gross revenue and processes data of at least 100,000 consumers; or processes data of at least 25,000 consumers and derives at least 50% of gross revenues from selling personal data. The Utah Consumer Privacy Act does carve out exceptions for entities subject to HIPAA and GLBA. It also does not apply to employee data or business-to-business data. Unlike the other state privacy laws effective to date, the Utah Consumer Privacy Act does not provide consumers the right to correction nor does it require companies to complete privacy assessments.

What else should companies prepare for in 2024?

Five more state privacy laws will go into effect in 2024, including those in Washington, Oregon, Texas, Florida, and Montana.

State of Washington My Health My Data Act: Washington's privacy law is targeted specifically to the collection, storage and transfer of health data, especially that health data related to reproductive health care, and goes into effect for covered entities on **March 31, 2024** (with an extension for small businesses until June 30, 2024). Please see our Client Alert for additional details.

Oregon Consumer Privacy Act: The Oregon law, which will go into effect on **July 1, 2024**, applies to any person that conducts business in the state or that provides products or services to residents of the state, and that during a calendar year, controls or processes: (1) the personal data of 100,000 or more consumers, other than personal data controlled or processed solely for the purpose of completing a payment transaction; or (2) the personal data of 25,000 or more consumers, while deriving 25% or more of the person's annual gross revenue from selling personal data. Like the other comprehensive state privacy laws, the Oregon law provides for certain exemptions based upon the type of business,

offers consumers data privacy rights, and imposes certain notice obligations on businesses. Please see our Client Alert for additional details.

Texas Data Privacy and Security Act: The Texas law also mostly takes effect on **July 1, 2024** (there are some exceptions for global opt-out requirements extending the compliance deadline to January 1, 2025), and is similar to other state privacy laws. Of note, however, the Texas law includes a carve-out for "small businesses" defined under the Small Business Administration and is otherwise quite broad in application. The Texas law applies to persons that (1) conduct business in Texas or produce a product or service consumed by residents of Texas; (2) process or engage in the sale of personal data; and (3) are not defined as a small business.

Florida Digital Bill of Rights: The Florida law will also take effect on July 1, 2024, and has requirements similar to the other state privacy laws, but has a significantly higher threshold for applicability. Businesses must operate in Florida, collect personal data from consumers, make in excess of $1 billion in global gross annual revenue and satisfy at least one of the following – (1) derive 50% or more of its global gross annual revenues from the sale of advertisements online, including providing targeted advertising or the sale of ads online; (2) operate a consumer smart speak and voice command component service with an integrated virtual assistance connected to a cloud computing service that uses hands-free verbal activation; or (3) operate an app store or digital distribution platform that offers at least 250,000 different software applications for consumers to download and install.

Montana Consumer Data Privacy Act: Finally, on **October 1, 2024**, the Montana Consumer Data Privacy Act will take effect. The Montana law applies to businesses that operate in Montana or businesses that produce products or services that are targeted to residents of Montana and (1) control or process the personal data of not less than 50,000 consumers (excluding personal data controlled or processed for the purpose of completing a payment transaction); or (2) control or process the personal data of not less than 25,000 consumers and derive more than 25% of gross revenue from the sale of personal data. Like other state privacy laws, the Montana law does not apply to personal data covered by Gramm-Leach-Bliley Act ("GLBA"), entities covered under the Health Insurance Portability and Accountability Act ("HIPAA"), administrative bodies, nonprofit organizations, institutes of higher education, financial institutions, and other similar exclusions. Please see our Client Alert for more details.

	Utah	Washington	Oregon	Texas	Florida	Montana
Consumer Rights	Yes, but No Right to Correction	Yes, with an Absolute Right to Delete All Personal Information	Yes	Yes	Yes	Yes
Right to Opt-Out	Yes, for Targeted Advertising and Sale of Personal Information	Opt-In Consent Requirements: ±	Yes, for Targeted Advertising; Sale of Personal Information; and Profiling Consent Necessary to Process Sensitive Personal Information	Yes, for Targeted Advertising; Sale of Personal Information; and Profiling Consent Necessary to Process Sensitive Personal Information	Yes, for Processing of Personal Information for Purposes of Targeted Advertising; Sale of Personal Information; and Profiling Opt-Out of Collection or Processing of Sensitive Personal Information	Yes, for Sale of Personal Information for Purposes of Targeted Advertising and Profiling Opt-In Required for Sale of Personal Information of Consumers between 13 - 16
Applies to Employees	No	No	No	No	No	No
Applies to B2B Data	No	No	No	No	No	No
Do HIPAA Exemptions Apply?	Entities subject to HIPAA are exempted	Information subject to HIPAA is exempted	Information subject to HIPAA is exempted	Entities and Information subject to HIPAA are exempted	Entities subject to HIPAA are exempted	Entities subject to HIPAA are exempted
Do GLBA Exemptions Apply?	Entities subject to GLBA are exempted	Information subject to GLBA is exempted	Information subject to GLBA is exempted	Entities subject to GLBA are exempted	Entities subject to GLBA are exempted	Entities subject to GLBA are exempted

Private Right of Action	No	Yes, under Washington's Consumer Protection Act	No	No	No	No
Privacy Assessments Required	No	No	Yes	Yes	Yes	Yes
Other Considerations	N/A	No Threshold for Applicability – Applies to All Businesses that Fall Under Definition of "Regulated Entity" Prohibition on "Geofencing"	Applies to Non-Profit Entities Beginning July 1, 2025	Global Opt-Out Mechanism Recognized January 1, 2025 Privacy Notice Language Requirements	Applicability Threshold of $1 Billion Annual Global Revenue	Universal Opt-Out Mechanisms Recognized
± Consent Necessary for Collection and Sharing of Consumer Health Data When Collected or Shared for Purposes Other than to Provide a Requested Product or Service; Consent Necessary for Sale of Consumer Health Data (Must include Description of Data to be Sold, Name and Contact Information of Purchaser, and Description of How Data is to be Used) – Consent is Only Valid for 1 Year						

How can companies be prepared?

As with the state privacy laws that went into effect this year, there are a number of actions companies can take to ensure they are prepared for these new laws.

1. ***Determine What Laws Apply:*** Each of these state privacy laws has different thresholds of applicability so companies will need to carefully assess how they apply to business operations.

2. ***Update Privacy Policies:*** Each of these state privacy laws requires some form of privacy notice. While a current notice may already sufficiently outline the data privacy practices, collection, use, and sharing of personal information, it is important to update such privacy notices to include details about the data privacy rights for individuals within each of these states. In some circumstances, it may make sense to provide data privacy rights to all customers rather than attempt to differentiate between state residency.

3. ***Update Data Privacy Rights Processes:*** While the processes may already be in place, companies will need to consider how to incorporate the requirements of these new states and train teams on how to handle such requests.

4. ***Reduce Collection of Personal Data:*** Given the heightened emphasis on the protection of personal data, companies may want to consider minimizing data collection in general by

determining what types of personal data are actually needed and used as part of the company's operations. This may be an appropriate time to redo privacy compliance assessments and data mapping exercises and to consider other enhancements to company data protection assessment processes.

5. ***Review processes and protections for the collection, use and sharing of sensitive personal data and consumer health data:*** Like the other state privacy laws, sensitive personal data is formally defined and granted certain rights related to the collection and use, thereof, including the right to opt-in to such collection. Companies will need to expand the use of opt-in mechanisms to meet such requirements. Similarly, companies that collect consumer health data (e.g., "personal information that is linked or reasonably linkable to a consumer and that identifies a consumer's past, present, or future physical or mental health") in Washington will need to implement mechanisms to collect consent to the sharing of such information with third parties under the "My Health My Data Act."

6. ***Review and Update Vendor Agreements:*** In addition to assessing their own compliance with these new state privacy laws, companies should also assess how their vendors and other third parties that operate in these jurisdictions comply with these laws. Data processing agreements should be updated accordingly.

7. ***Review and enhance data security safeguards:*** As with all new privacy laws, this is an opportunity to review, test and enhance the physical, technical, and administrative safeguards in place to secure company information, including personal data.

8. ***Provide Training to Employees:*** Finally, employees throughout the company will need to be aware of how these new state privacy laws apply to their roles and responsibilities from the legal and compliance teams, to HR, marketing, customer service and information security.

✧ ✧ ✧

Our Data Privacy and Cybersecurity practice regularly advises companies on how to meet the requirements of new privacy and cybersecurity laws. If you have any questions concerning any laws outlined here, please do not hesitate to contact either member of our team:

Chicago

Aaron Charfoos
1.312.499.6016
aaroncharfoos@paulhastings.com

Washington, D.C.

Brianne B. Powers
1.202.551.1237
briannepowers@paulhastings.com