PAUL HASTINGS

Stay Current

October 2022

Follow @Paul_Hastings

New Comprehensive U.S. State Privacy Laws Are Coming – Is Your Company Ready?

By Aaron Charfoos, Jacqueline Cooney, Dave Coogan & Brianne Powers

Over the last two years, many states have taken cues from California and the EU by adopting sweeping privacy laws. These laws, passed in Virginia, Colorado, Connecticut and Utah, as well as updates to the already enacted California Consumer Privacy Act ("CCPA"), are focused on providing consumers (and soon employees in some states) better information about how their data is used, more control over their data and imposing additional requirements on companies to protect consumer personal information.

Similarities and Differences in the New Laws

While each law should be reviewed to understand their specific requirements, each has similar provisions related to requiring companies to:

- Implement reasonable security measures;
- Share data with third parties only when those third parties are subject to specific contractual requirements limiting their own uses of the data; and
- Provide clear privacy notices that must include details of the collection and use of data.

Most of the new laws also give state regulators broad authority to pursue enforcements for violations of the law.

It is important to note that even though there are similarities, the laws also have important, and often nuanced, differences that companies must understand in order to comply with the laws' requirements. Below, are some of the more significant differences:

	CA	VA	CO	CT	UT
Consumer Rights[1]	Yes, but right to confirm processing is not explicitly included	Yes	Yes	Yes	Yes, but no right to correction
Right to opt out of certain processing	Sale of PI Sharing for contextual advertising	Targeted advertising Sale of PI Profiling	Targeted advertising Sale of PI Profiling	Targeted advertising Sale of PI Profiling	Targeted advertising Sale of PI

	CA	VA	CO	CT	UT
Applies to Employees	Yes	No	No	No	No
Applies to B2B Data	Yes	No	No	No	No
Do HIPAA Exemptions Apply?	Yes, but only HIPAA data is exempted	Entities subject to HIPAA exempted	Entities subject to HIPAA exempted	Entities subject to HIPAA exempted	Entities subject to HIPAA exempted
Do GLBA Exemptions Apply?	Yes, but only GLBA data is exempted	Entities subject to GLBA exempted	Entities subject to GLBA exempted	Entities subject to GLBA exempted	Entities subject to GLBA exempted
Private Right of Action	Yes, but only for data breaches	No	No	No	No
Privacy Assessments	Yes	Yes	Yes	Yes	No

Effective Dates

The laws will come into effect throughout 2023. In particular, the laws become effective on:

- The California Privacy Rights Act — January 1, 2023.
- The Virginia Consumer Data Protection Act — January 1, 2023.
- The Colorado Privacy Act — July 1, 2023.
- The Connecticut Data Privacy Act — July 1, 2023.
- The Utah Consumer Privacy Act — December 31, 2023.

What Companies Should Be Doing to Prepare

As an initial matter, companies that are subject to these laws must assess their current practices to determine whether they meet the law's specific requirements. Where there are gaps, companies should focus first on California and Virginia requirements (which come into force first) and should work to remediate those gaps before the end of this year.

We recommend that companies focus on the following:

1. ***Determine whether these laws apply to your company.***

   The following are the thresholds for each state:

   - **California**: $25 million in annual gross revenue in the preceding calendar year; or processes data of at least 100,000 consumers; or derives at least 50% of gross revenues from selling or sharing data.
   - **Virginia**: 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 data.

- **Colorado**: Processes data of at least 100,000 consumers; or processes data of at least 25,000 consumers and derives revenue or receives a discount on goods or services from selling personal data.
- **Connecticut**: Processes data of at least 100,000 consumers (excluding purely payment transactions); or processes data of at least 25,000 consumers and derives at least 50% of gross revenues from selling personal data.
- **Utah**: $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.

2. ***Review and update privacy notices and privacy rights links***. Companies should review and update, as needed, their privacy notices (including website privacy policies, internal privacy policies, and other just-in-time collection notices) to reflect the new state law requirements.

3. ***Review your online advertising practices***. Companies that process personal data from website visitors for the purposes of targeted advertising should also review the state requirements that allow visitors to opt-out via a universal opt-out mechanism or global privacy control.

4. ***Review your uses of sensitive data***. While companies may be familiar with the requirements for special categories of personal data as defined under the GDPR, several of the new state privacy laws also provide specific requirements for the use and disclosure of "sensitive personal information."

5. ***Implement privacy assessments***. California, Virginia, Colorado and Connecticut require a data protection assessment for certain activities, including those that involve the use of sensitive personal information or other "high-risk" data.

6. ***Review consumer privacy rights requests procedures***. Companies will need to update their internal consumer privacy rights requests processes to address the new state privacy rights, including in California to address employee and business-to-business contact rights requests.

7. ***Review and update vendor agreements***. Companies should review and update their vendor agreements involving personal data to ensure they meet the requirements of the new state privacy laws and to ensure vendors are also bound to such requirements.

8. ***Provide training to employees***. Employees from compliance, HR, and marketing, as well as those who implement the technical business requirements for privacy compliance need to be trained on the new state privacy laws.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Chicago

Aaron Charfoos
1.312.499.6016
aaroncharfoos@paulhastings.com

Dave Coogan
1.312.499.6059
davidcoogan@paulhastings.com

Washington, D.C.

Jacqueline W. Cooney
1.202.551.1236
jacquelinecooney@paulhastings.com

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Brianne B. Powers
1.202.551.1237
briannepowers@paulhastings.com

Sherrese M. Smith
1.202.551.1965
sherresesmith@paulhastings.com

[1] Except where otherwise indicated in this chart, the following consumer rights are included in these laws: confirm processing, access, portability, correction, deletion, and equal services and price.