How to Prepare Your Business for Privacy Laws Taking Effect in 2023

Legal Alert

November 29, 2022

Mariel Giletto, Krishna Jani

In 2023, five new state privacy laws will become effective. How will these new laws affect your business?

Currently, privacy laws in the United States include a patchwork of state laws as well as some industry- or issue-specific federal laws, such as the Health Insurance Portability and Accountability Act (HIPAA) for protected health information and the Gramm-Leach-Bliley Act (GLBA) for the financial services industry. There is no comprehensive federal privacy law in effect in the United States at this time.

Below you will find a brief overview of the new state privacy laws going into effect, their commonalities, their differences, and what you need to know to prepare your company for compliance.

If you have any questions related to your company's compliance with these laws, please contact Mariel Giletto or Krishna Jani.

If you have any questions, please contact Mariel Giletto or Krishna Jani.

NEW LAWS BY STATE

California

Effective: January 1, 2023

The California Privacy Rights Act (CPRA) amends and extends the California Consumer Privacy Act (CCPA). CPRA is a new law with more stringent requirements than the current law and creates a new regulatory agency (California Privacy Protection Agency (CPPA). To date, only draft regulations have been released. Final form regulations have not been published.

California's new, more stringent law is significant because state attorneys general are tasked with enforcing data privacy laws and this new legislation signals a ramp up in enforcement, thereby bringing the U.S closer to Europe's General Data Protection Regulation (GDPR).

One crucial piece of the proposed CPRA regulations is the right of a consumer to opt-out to both the sale and sharing of personal information. This is relevant for data brokers, and companies that contract with data brokers.

Separately, California passed a new bill called the California Age-Appropriate Design Code Act about two months ago. It is an online safety bill containing unique privacy requirements to protect minors 18 and under.

Virginia

Effective: January 1, 2023

Under the Virginia Consumer Data Protection Act, consumers have the right to opt-out of the processing of personal data for purposes of targeted advertising, sale of personal data, or profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.

Colorado

Effective: July 1, 2023

The Colorado Privacy Act (CPA) gives the Colorado attorney general authority to adopt rules governing privacy. It also requires that, by July 1, 2023, the Colorado attorney general must adopt rules detail the technical specifications for one or more universal opt-out mechanisms that clearly communicate a consumer's affirmative, freely given, and unambiguous choice to opt-out of the processing of personal data for purposes of targeted advertising or the sale of personal data.

Both **Connecticut** and **Utah** have also passed privacy laws that are set to take effect on July 1, 2023 and December 31, 2023 respectively.

COMMONALITIES

Each state law:

- Attempts to balance the risk to individuals in sharing certain data against benefits to the corporation in collecting such data.
- Has thresholds of applicability, including the types and size of companies (based on revenue and/or employee count) to which it they apply.

For example, the CCPA, as amended by the CPRA, applies to any company that does business in California, no matter where it is based, if it meets any of the following criteria:

  - It has an annual revenue of $25 million or higher.
  - It shares, sells, or acquires the personal data of 100,000 or more customers or households.
  - It makes at least half of its yearly income from selling or exchanging personal information about customers (regardless of total revenue).
- Has data subject rights (right to know what data is collected, the fact that the company has the data, the right to access the data, right to correct inaccurate data (except Utah), right to be forgotten (right to delete the data), right to opt out of sale, and the right to take data somewhere else—or data portability).
- Contain exceptions for public information (including government records and records that consumers make publicly available (*g.*, a social media post made online).

- Attempt to regulate profiling (automated use of personal data for the purpose of analysis/predicting usage).

SIGNIFICANT DIFFERENCES

The significant differences of each state law include:

- Different revenue, size, and other thresholds may apply across different states.
- The State of California also defines sales to include "anything of value" to include more than just cash. This means that Service Providers could be viewed a "purchasing data."
- The State of California also uses a global opt out tool, meaning that the consumer can opt-out of all use of personal data.
  - A business can do this in one of a few ways including creating a clear and conspicuous link on the business's internet home page entitled "Do Not Sell or Share My Personal Information" to a webpage that enables a consumer to opt-out of the sale or sharing of the consumer's personal information.
  - Businesses only need an "opt-in" from a consumer who is a minor between 13-16 years old.
- Significantly, California's law contains a private right of action for breach for failure to use adequate security measures.

HOW TO PREPARE

Below are some helpful considerations for your company to begin their analysis of compliance with the new state laws:

- Procure cyber insurance with a sufficient policy limit for potential data breach costs.
- Develop a data privacy incident response plan and train your staff accordingly Ideally, this should be reviewed and updated every year, as necessary.
- Cross off any laws that include revenue thresholds, which do not apply to your company.
- Utilize data mapping to your advantage – understand the process of gathering and using the data
- Review service provider contracts to confirm that transfer of data is not considered a "sale" in California given the definition of a "sale" under California's new law. Consider limitations of service providers' use of data.
- Create a retention policy, make sure to train your employees on it, conduct annual audits on your system, as necessary, and delete any stale data in accordance with applicable law(s) and retention policies.
- Stale data is a liability. So, to the extent the above tips are implemented, it can help to reduce liability in the event of a cyberattack.

WHAT ELSE TO EXPECT

Another draft of a federal privacy law has been introduced – the American Data Privacy and Protection Act.

- Draft federal legislation has been introduced almost every year for the past few years but has not progressed.

- Passage of this particular law is not likely because the draft legislation proposes to pre-empt state law and a number of state Attorneys General oppose federal pre-emption of their state's privacy laws. Most state Attorneys General want a federal baseline privacy law, meaning the federal law is the minimum that businesses would have to comply with, and each state is free to enact stricter privacy laws.
- The federal law would apply to medium to large businesses and has a partial state preemption (Illinois is exempted as there is a huge amount of class-actions surrounding Illinois privacy laws) (California is excluded). Small businesses are exempt, as well
- The proposed legislation seems to be targeted to large tech companies called Large Data Holders (LDHs). LDHs would have to annually certify compliance, designate a privacy officer who reports to a higher officer of the company, and if they use an algorithm, then they must minimize biases.

If you have any questions about the new data privacy laws and how it could affect your business, please contact Mariel Giletto or Krishna Jani.

ATTORNEYS MENTIONED

Mariel Giletto