aidentified

Business Tips for Navigating U.S. Data Privacy Laws

JANUARY 28, 2022

Data Privacy is a hot topic - with many new laws being passed all over the world - but what can we expect in the U.S. and how might it affect your business?

In this article, we will cover the current state of data privacy laws in the U.S. and tips to help your business be ready for 2022 and beyond.

Overview of Data Privacy Laws in the U.S.

In the U.S. an overlapping web of individual laws and regulations govern how we handle personal information. Some of these laws are federal, in which case they are typically sector-specific, e.g., the health sector's Health Insurance Portability and Accountability Act ("**HIPAA**"), or the financial sector's Gramm Leach Bliley Act ("**GLBA**") and some are on the state level, e.g., the California Consumer Privacy Act ("**CCPA**"). Our privacy laws are constantly changing and it is often hard to keep up with these changes.

So, where are we with comprehensive state laws on data privacy? What about a comprehensive federal law and what does this all mean for businesses trying to do the right thing?

State Data Privacy Laws

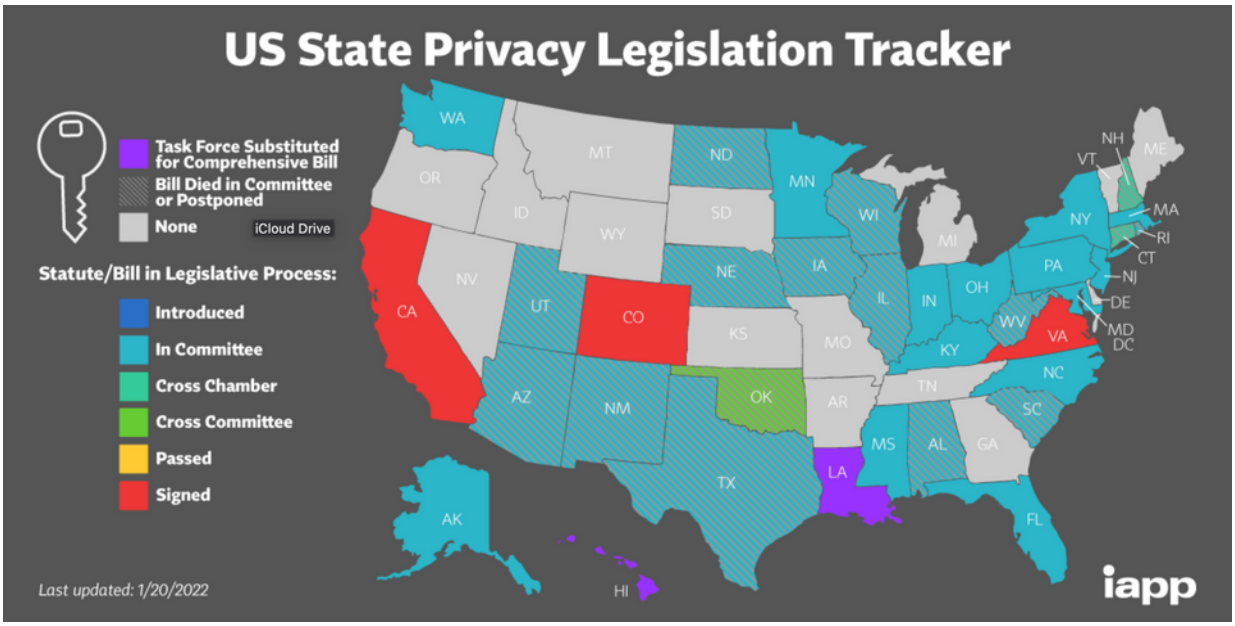
There are currently only three states that have comprehensive privacy laws that were past in the last few years:

- ✓ California
- ✓ Colorado
- ✓ Virginia

There are also states that have previously enacted privacy laws that give some privacy or data security protection, such as the Massachusetts Safeguards Regulation (which requires businesses that own or license personal information of Massachusetts residents to have a Written Information Security Plan in place to secure such information).

However, there were twenty-three states that introduced comprehensive privacy legislation in 2021 and there are many states where such legislation is presently in committee such as New York, North Carolina and Pennsylvania or that have task forces that are looking into privacy legislation like Louisiana and Hawaii. There will definitely be more states that pass comprehensive data privacy laws in 2022.

The International Association for Privacy Professionals (IAPP) publishes this great map to help you track U.S. state privacy legislation.



CCPA and CPRA

Most people have heard about the California Consumer Privacy Act ("CCPA") since it was passed in 2018 and went into effect in 2020 and has required many organizations to make changes to their processes surrounding the collection, usage and processing of California consumers' information.

In addition, the California Privacy Rights Enforcement Act (the "CPRA") goes into effect in January 2023, further expanding California consumers' privacy rights.

VCDPA and CPA

The most recently passed state data privacy laws are the Virginia Consumer Data Protection Act ("VCDPA"), which goes into effect on January 1, 2023 and the Colorado Privacy Act ("CPA"), which goes into effect on July 1, 2023.

Distinctions between CCPA/CPRA and the VCDPA and CPA

The Virginia and Colorado laws are similar to the CCPA and CPRA but not identical.

All of these laws allow for residents of the states at issue to access, correct, and delete the personal information held by organizations, which includes rights to understand what personal information a business holds on them and to opt-out of the processing of their personal information for various purposes (such as targeted advertising, profiling or the sale of their personal data).

There are also notable distinctions in the laws: for example, the CPA applies to nonprofit entities that meet certain requirements but the CCPA/CPRA and VCDPA exempt nonprofit organizations.

The Virginia and Colorado laws do not apply to employee or business-to-business data, unlike the CCPA and CPRA. Additionally, there is no private right of action under the CPA or VCDPA but the CCPA and CPRA give a limited private right of action for breach of personal information.

All three state laws differ with respect to the required process for responding to a consumer privacy request and the applicable exceptions for responding to such requests.

Businesses should research and be aware of the changes these data privacy laws bring along with them and develop programs to comply with these laws as they make their compliance plans in 2022. A great resource is the IAPP website.

What about a comprehensive U.S. Federal data privacy law?

Multiple attempts were made in the last years to pass federal data privacy legislation. Notably, since the debate on privacy legislation began in earnest in 2018, members of Congress have released over twenty comprehensive information privacy bills or drafts. Some with recognizable names such as the Data Accountability and Transparency Act and the Consumer Online Privacy Rights Act. In early 2021, the Information Transparency and Personal Data Control Act was introduced, and later in 2021, the Online Privacy Act of 2021, originally introduced in 2019, was reintroduced in Congress. However, so far, no meaningful progress has been made on a federal privacy law.

Federal Data Privacy Legislation Complications

Complicating the need for data privacy legislation in the U.S. is the fact that there does not exist an explicit and general right to privacy in the U.S. Constitution. The concept of privacy rights is inherent in the right to privacy in the First, Third, Fourth, Fifth, and Ninth Amendments. The Bill of Rights created "zones of privacy" into which the government could not intrude.

However, our federal legislators now also recognize that there is a need for the U.S. to craft rules for online data privacy protection to protect consumers and their data that is out there on the internet. Personal data is frequently in the hands of businesses and used (and possibly misused, by businesses and bad actors alike) in a myriad of ways.

There may be inevitable constitutional challenges to federal privacy legislation, especially with respect to First Amendment commercial speech protections or Article III standing questions, but there is hope that we will get a federal law in the near future.

Here are two issues that are highly controversial with respect to a federal data privacy law (the first issue is one that remains controversial for state laws as well):

1. Will there be a private right of action for consumers to bring actions for alleged violations to enforce the law or will it only be enforceable by a government agency, like the Attorney General's office or the Federal Trade Commission?

2.. Will the federal law wholly pre-empt any previously passed state laws or will it just add additional burdens to the morass of state privacy laws already out there?

How realistic is it that a federal law will be passed in 2022? It may be difficult in this mid-term year, and because of the Covid-19 pandemic and other legislative issues currently dominating Congress, the federal government may not view it as much of a priority.

How do businesses do the right thing with respect to data privacy in the U.S.?

U.S. businesses are generally looking to do the right thing when it comes to data privacy since protecting personal information is:

a) required by current laws already in effect
b) good for business
c) spurred on and modeled by new privacy initiatives from Apple, Google and Facebook that are affecting digital marketing and usage of personal information from social media and in mobile apps to help protect data privacy, even if it may not currently be required by federal or state law.

For those who work in businesses that handle personal information, and most of us do in this day and age, whether it is the main focus of your business or whether it is not, these are some of the most important things you should remember as you build products and handle personal information:

1. Incorporate privacy by design

Build data privacy into products and data handling and storage processes with the privacy by design" concept by using Privacy Impact Assessments which will allow you to understand what privacy risks you may be facing and what remediations and controls to put into place to manage those risks.

"Our company strives to always adhere to a "privacy by design" policy. Every new product, feature and enhancement idea goes through a rigorous review to ensure we're meeting all compliance requirements – current and anticipated."

- Juliana Spofford, General Counsel & Chief Privacy Officer, Aidentified

2. Map your data and know the laws that apply to your organization

Know what types of personal information you collect, store or process and what laws apply to your organization and the data sets that you collect, store or process.

3. Secure personal information

Always handle personal information with care and put proper protections in place for personal information (which included your customers' personal information which may be in your care!).

4. Treat individuals' right to privacy with respect

Always provide transparency about personal information and offer a right to opt out of personal information data collection and usage.

5. Ask for help

When in doubt, look to compliance and privacy individuals in your organization, or ask for help from outside privacy experts. It is a good investment in your busines

About Author Juliana Spofford

Juliana is the General Counsel and Chief Privacy Officer for Aidentified and brings decades of legal experience to her pointed in-house legal insights, having worked as counsel for both small data technology start-ups and powerhouse data services companies such as Dow Jones/Factiva and Dun & Bradstreet, where she honed her privacy skills. She enjoys sharing her insights about compliance, privacy and security issues to help organizations do the right thing and understand the importance of these issues for their ultimate business success.

The content of this blog article contains thoughts and opinions of the writer and not an entity and is not meant to be relied on as legal advice. Content from other sites incorporated in this blog have been attributed to their source.