Privacy Laws:
An Executive Overview

by Raymond Hutchins and Mitch Tanenbaum
Last update: July 7, 2023

This non-technical report describes the evolution of privacy laws and regulations in the United States and the world. The report provides timely information that business leaders can leverage to correctly protect data, manage risk, and protect company valuation.

AI Statement: This document was written by a human being ***and not AI***. While we may use AI for aspects of our research, we find that AI is (thus far) incapable of writing a document of this kind.

Contents

1.0 Privacy Laws and Regulations

1.1 New Rights for ***Some*** People on Earth

Led by the European Union, liberal democracies are attempting to grant new data and privacy rights to their citizens. Authoritarian governments, led by China, are going in the exact opposite direction, taking away all data and privacy rights of their citizens.

It is an open question as to whether the U.S. Constitution gives people a right to privacy. The Fourth Amendment protects against unreasonable searches, but that was written before the age of the computer and the Internet. U.S. courts (including the Supreme Court) are not quite sure if there is a fundamental right to privacy and personal data ownership.

Possible rights include: (1) the right to obtain a copy of data that a company has collected about you or (2) the right to correct incorrect data that a company has collected or (3) the right to demand that a company delete your data from its IT infrastructure. As we will see later, those rights are separate, and a law might grant one of them without the other/s.

The bottom line is that until around 2016, no laws anywhere in the world addressed these issues, and since they address fundamental (and new) human rights, we will go into a bit of detail.

1.2 International Privacy Laws

According to the United Nations, 137 out of 194 countries have put in place legislation to secure the protection of data and privacy for its citizens.[1] While there may be some formal attempt to put legislation in place, even in developed countries, the state of enforcement is such that no such protections actually exist. And as mentioned earlier, in countries with authoritarian regimes, there is no sign the citizens will ever have these rights.

The European Union's General Data Protection Regulation (GDPR) was adopted in 2016 and went into effect on May 25, 2018. This piece of legislation is the model for legislation occurring in the U.S. and around the world.

1.3 U.S. Federal Privacy Legislation

While some large tech companies and others have supported a U.S. federal privacy law that supersedes those implemented by individual states, thus far, there is no serious movement towards such a law. State legislators and their citizens seem disinclined to forgo the new data privacy rights they have been granted.

American Data Privacy and Protection Act (ADPPA)

The ADPPA is the most recent attempt at nuking state privacy laws via federal legislation. There are many people who do not like California's law (see below), which includes a private right of action to sue in case of a breach. While some people said this new right would cause an avalanche of lawsuits, the reality is quite different. This appears to be because contingency privacy lawsuits are extremely difficult to pursue, and most are thrown out. Thus far, there is little economic incentive for lawyers to pursue such cases.

Given the politics of Washington, we rate the likelihood of the ADPPA passing as low–at least for now.

1.4 U.S. State Privacy Legislation - California Leading the Charge

California led the nation in creating the first cybersecurity law, CA SB 1386 (notice the immediate connection between cybersecurity and privacy–see more below). Passed in 2002, it was considered radical at the time. It said that businesses had a duty to protect consumers' information. It also made an attempt to define what information needed to be protected. It did not give consumers any rights in their data, and it made the Attorney General responsible for enforcement.

Since the AG has a lot of laws to be responsible for and since the law did not give the AG any more money or people to enforce it, only the most egregious violations were ever prosecuted. In the next almost 20 years, every state implemented a law, mostly based on CA SB 1386. The details changed. What data needed to be protected changed. What you had to do in case of a breach changed. But the basis for all these laws was CA SB 1386.

1.5 First-Generation and Second-Generation Privacy Laws

[1] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Most states have had “first-generation” privacy laws on the books for some time. These laws (loosely) don’t offer consumers many protections. Second-generation privacy laws originated in Europe with GDPR and were followed, after several years, by the California Consumer Privacy Act (CCPA). That act is in effect now. CCPA was somewhat of a shotgun wedding to avoid a stronger ballot initiative, but it has gotten watered down by the legislature a bit since it was enacted in 2018. As a result, the California Privacy Rights Act (CPRA) ballot measure was passed in 2020 by California residents. CPRA says (in the law) that the legislature may only modify the law in order to strengthen it.

Now California is leading the nation again–for better or worse. They implemented the first second-generation privacy law, and other states are modeling their second-generation laws on California’s laws. We say *laws* because there are actually two laws that are relevant–CCPA and CPRA.

The benefit of states creating their own privacy laws is that hopefully they are more agile than the feds and they can modify their laws more quickly in case mistakes are made.

1.6 Elements of Second-Generation State Privacy Laws

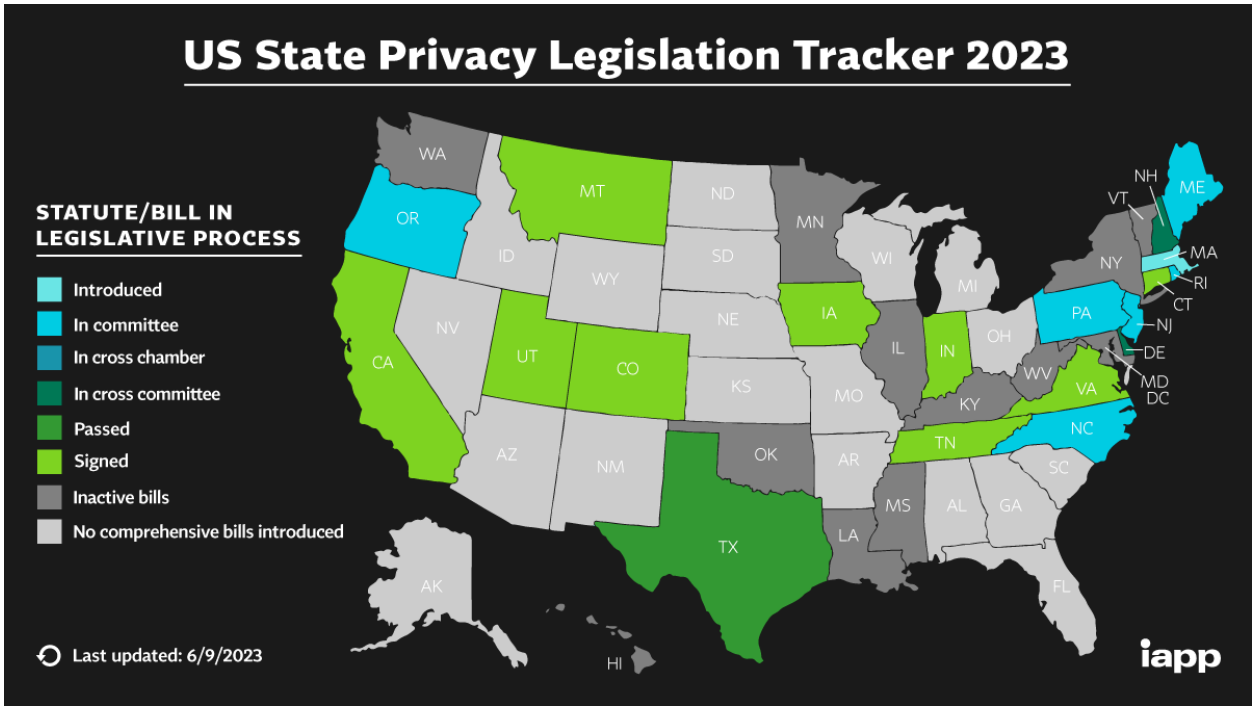
Like GDPR in Europe, second-generation (U.S.) privacy laws create privacy “rights.” This is because there is no agreed-to right-to-privacy in the U.S. Constitution, unlike in the E.U. Constitution. Given that the Constitution was created long before the Internet, the founders didn’t consider privacy to be a problem. While the rights vary from state to state and hence why businesses would prefer a single federal law that preempts state laws, here are some of the rights offered by state privacy laws:

- The consumer’s right to obtain a copy of his/her data (free of charge with some restrictions).
- The right to correct the data that was collected.
- The right to have that data deleted (again, with some restrictions).
- The right to stop anyone from sharing that data (loosely, selling it) with others (again, with some restrictions).

Business responsibilities in second-gen laws:

- A simple-language, publicly-posted, privacy policy.
- Businesses must disclose for what purpose(s) they will be using the data collected.
- They must disclose the classes of (and in some cases) the names of the people with whom they are sharing that data.
- They must provide one or more methods for people to take advantage of these rights.
- In some cases, this includes data that is collected in brick-and-mortar locations.
- They must respond quickly to a consumer request (typically no more than 30 days).
- In many cases, these consumer rights trickle down to third parties with whom the consumer’s data is shared.

Currently, there are twelve states that have passed state privacy laws, with seven more working on laws. The graphic below, outlines the current state law situation. This is a very rapidly changing landscape. Even though this IAPP graphic was recently updated, it is already out of date.



Note that the velocity of privacy law passage has increased greatly. At the rate we are going now, all 50 states will have laws within 5-10 years.

Several states' laws, including California, Colorado, Connecticut and Virginia are already in effect as of July 1, 2023; the remaining laws become effective in 2024 and 2025. Note that California has two new second-generation laws, both of which are in effect now. Also note that on June 30, 2023 a California judge delayed enforcement of the CA CPRA until March 29, 2024. This continue to change fast.

In order to help decision makers understand this fast changing situation, We work to keep the chart below updated. This chart documents the details of each of these laws. Here is a snapshot of what those charts look like.

	California	Virginia	Colorado	Utah	Connecticut
Scope	Applies to businesses that: Have $25 million in annual gross revenue **-OR-** Process data of at least 100,000 consumers -or- Derive at least 50% of gross revenues from *selling or sharing* data	Applies to businesses that: Process data of at least 100,000 consumers -or- Process data of at least 25,000 consumers and derive at least 50% of gross revenues from *selling* data	Applies to businesses that: Process data of at least 100,000 consumers -or- Process data of at least 25,000 consumers and derive *revenue or receive a discount on goods or services from selling* personal data	Applies to businesses that: Have $25 million in annual gross revenue **-AND-** Process data of at least 100,000 consumers -or- Process data of at least 25,000 consumers and derive at least 50% of gross revenues from *selling* personal data	Applies to businesses that: Process data of at least 100,000 consumers (excluding purely payment transactions) -or- Process data of at least 25,000 consumers and derive at least 50% of gross revenues from *selling* personal data
Effective Date	Jan. 1, 2023	Jan. 1, 2023	July 1, 2023	Dec. 31, 2023	July 1, 2023

The details of each state's law is beyond the scope of this paper, but you can find those details in this shared folder: Shared drives - Google Drive. Note: There are now so many states with privacy laws that we had to break up the document into multiple parts for easy navigation.

Most of the state privacy laws have some minimum business sales volume for compliance, but many of the state cybersecurity laws apply to everyone without exception.

Each state defines which data elements (like a name or driver's license number) are in scope, the definition of sale or sharing of data, what types of organizations are covered, who is exempted (such as health care providers covered by HIPAA), precisely what rights a person has, the responsibilities of covered businesses *and their vendors*, what notices must be provided when, what terms must be written into contracts with service providers, and other items. See the link above to get an idea of these specifics.

In addition, the legislation in some states (for example, Colorado and California) requires clarifying regulations while other states leave the law vague, meaning a greater likelihood of lawsuits since companies don't know how to respond. Each state does this differently. California, for example, set up a separate department, the California Privacy Protection Agency, while Colorado, as another example, has charged the Attorney General with creating the regs. What you can count on is many pages of regulations, all different and some conflicting between states.

1.7 Extraterritoriality

Extraterritoriality is a big word that means "my law applies in your jurisdiction." A well-known example of this is Europe's privacy law, GDPR, which applies to U.S. companies, even to ones that don't have any operations in Europe, but who might possibly have European customers or visitors to their web sites.

In the U.S., states have practiced extraterritoriality since the beginning. State security, breach notification and privacy laws apply to you, whether you have a location in that state or not, if you collect data on a resident of their state. For example, a company located in Texas has to comply with Kansas's cybersecurity and privacy laws, if they collect data on Kansas residents, sell products or services to them, or target them in advertising. Sometimes the nexus is very slight.

1.8 U.S. vs. the European Union

The U.S. and the E.U. have been fighting over adequate privacy for years. The E.U. has an interesting view of the universe wherein the rules the U.S. must play by do not apply to the E.U. As a result, there has been a bit of conflict across the pond. The most recent version of a cross border privacy agreement was struck down by the CJEU, the E.U.'s highest court. European law may allow California to strike a deal with the E.U. regarding adequacy. If they do, then companies based in California, with data stored in California, may be able to transfer data back and forth across the pond freely, while companies elsewhere in the U.S. can't do that. Assuming that happens–and that is a big "if"–then there will be major pressure on the other states and Congress to follow suit so that California companies don't have an unfair advantage over others. This is a big "if," but it could happen.

If you are confused after reading this, you are not alone. Your compliance team has a lot of work ahead of it. Also remember that you must consider that there is a difference between what you are legally required to do and what your customers expect you to do. If your customer, for example, asks for a copy of his or her data and you say, "We are not legally required to provide that" (or some other "get-lost" version of that), odds are that social media will not be your friend. If you need help sorting this out, please contact us.

How Cybersecurity and Privacy Are Merging

Cybersecurity and privacy laws are both about protecting data within various IT infrastructures. Privacy focuses on personal data of citizens, and cybersecurity focuses on all other valuable data assets. In the short period of time that such security has become an issue, cybersecurity and privacy efforts have been driven by different constituencies. However, since we are talking about protecting data, the conversations are merging.

About the Authors

Raymond Hutchins
Managing Partner
rh@cybercecurity.com
303-887-5864

Mitch Tanenbaum
CISO/Partner
mitch@cybercecurity.com
720-891-1663

Ray Hutchins and Mitch Tanenbaum own and operate two cybersecurity companies:

- CyberCecurity, LLC
- Turnkey Cybersecurity and Privacy Solutions, LLC

These are veteran-owned, mission-oriented companies providing defensive governance, strategic and operational guidance, and boots-on-the-ground support to organizations that acknowledge the cyberwar and are ready to actively support and engage in risk reduction and value creation.

Ray's and Mitch's wide range of cyberwar experiences with defending organizations all over the world and their ability to articulate this complex technical environment to leaders has established them as "global cyberwar" authorities. Please learn more about Ray and Mitch here: https://www.cybercecurity.com/about/

Did you find this position paper of value? Here are some of our other papers:

1. The Global Cyberwar and Societal Response
2. IT/Security & Privacy GRC solutions–Time for an Evolution
3. Hiring, Managing and Firing MSPs
4. Caremark and More Propel New Board Risks
5. Why Technologists Fail to Communicate Effectively With Leadership