COSMOS
Navigate the Compliance Universe

# CEP Magazine - June 2022
# Are companies prepared for new state-level data privacy bills?

By Bill Tolson


Bill Tolson

**Bill Tolson** (bill.tolson@archive360.com) is Vice President of eDiscovery and Compliance at Archive360.

There was a time when mandates like the General Data Protection Regulation (GDPR), the sweeping data privacy legislation that governs the European Union and European Economic Area, and its California cousin, the California Consumer Privacy Act (CCPA), dominated the headlines. For too long, personally identifiable information (PII) had flown freely between businesses, and been misused and abused along the way. The new regulations were onerous to be sure, but certainly needed to restore even basic privacy. No wonder that there are now many similar laws around the world.

However, ever since GDPR and CCPA went into effect, there's only been a trickle of privacy laws passed in the United States.

That may be about to change. Dozens of data privacy bills have already been forwarded for debate in states around the country, and by 2024, it's likely that almost every state will have its own flavor passed into law. There's surely some overlap, but there are specific provisions that are wildly different.

Preparing for these laws will take significant resources, and forward-thinking enterprises have begun putting the necessary layers in place. But how about the rest—are they as ready as they need to be?

## So just what is PII?

Let's understand the basics. PII is information or attributes that can be used on their own or with other information to identify, contact, or locate a single person or identify an individual in context. This is quite broad: The National Institute of Standards and Technology's PII guide cites attributes such as full name, full face photos, home address, email address, ID number, passport number, vehicle plate number, driver's license, fingerprints or handwriting sample, credit card numbers, date of birth, birthplace, genetic information, biometrics, phone numbers, health plan information, login name or screen name, and geographic information.[1] In the European Union, directive 95/46/EC defines "personal data" as information that can identify a person via an ID number or factors specific to physical, physiological, mental, economic, cultural, or social identity.[2]

Other factors that may not seem obvious are what the government labels as quasi- or pseudo-identifiers that can be used in combination with other quasi-identifiers. Here's one scary stat that should bring this vagueness home: According to a government study, 87% of the US population can be identified with just a combination of gender, ZIP code, and date of birth. Just think of the number of websites that ask for only this info. Other research indicates that consumers believe PII protection is each vendor's responsibility—if there's a breach, most will take their business elsewhere.

This makes for a potent combo—consumers want more protection, and state governments are putting pressure

on businesses to ensure that protection.

## The state of state-level privacy mandates

At this point, despite ongoing speculation, the prospect of a federal mandate that supersedes state laws is remote at best. That may be why, at the state level, we're seeing a lot of action. In fact, states have been introducing new privacy bills at a remarkably rapid rate.

In the first two months of 2022, 27 states introduced new privacy bills.[3] This is on top of the three state-level privacy laws that have already become law: California's aforementioned CCPA (soon to be succeeded by the more targeted California Privacy Rights Act), Virginia's Consumer Data Protection Act, and the Colorado Privacy Act. How many of the latest bills will be passed into law, and with what stipulations, is anyone's guess. However, there's no doubt that we're going to soon see many new laws.

There are three significant challenges:

1. Many state privacy bills borrow content from each other, but they differ in particular rights, definitions, exemptions/exclusions, and time frames; those differences are crucial.
2. These new laws will regulate state data-subject PII *no matter where the company collecting the data is located*.
3. Many of the new laws will be slightly different from each other, meaning companies will not be able to create a high-water mark privacy policy and expect to comply with all relevant laws. For example, just because an organization is compliant with GDPR does not mean it's also compliant with CCPA/California Privacy Rights Act.

So how will this new regulatory landscape affect companies as they oversee and manage this sudden expansion of data-subject information rights?

My own ongoing conversations with state legislators who have authored recent privacy laws, and others looking to do the same in their state, reveal that they're adopting common provisions at the fundamental level. These include granting consumers:

- The right to access their personal data.
- The right to correct their personal data.
- The right to delete their personal data (i.e., the right to be forgotten).
- The right to obtain a copy of their personal data.
- The right to opt out of the processing of personal data for targeted advertising purposes.

These bills/laws lay out basic definitions, such as who is considered a "data collector" and who is a "data processor," what is considered PII, what is consent, opt-in versus opt-out, and who is viewed as a consumer. They also include exclusions/exemptions such as which types of organizations are governed under the law, the organization revenue threshold, the industry, and whether there is an existing data retention regulation such as 17 C.F.R. §§ 240.17a-3 and 240.17a-4 or Gramm–Leach–Bliley.

State privacy laws have a broad jurisdiction. Many company executives don't realize a basic but far-reaching fact about individual state privacy bills and laws: They reach *across state lines and countries.* This means a company in

Florida that collects PII from individuals in Colorado is subject to the requirements/responsibilities of the Colorado Privacy Act. This holds true for all state privacy laws, meaning organizations worldwide will need to track all of these laws and new amendments to ensure they can identify individual PII attributes and the state the data subject lives in and react to data-subjects requests specified in the individual state law.

All bills/laws include the right of a data subject to request information about their PII that a company may hold with specific but sometimes differing response times.

For the record, a data subject access request (DSAR) is addressed to an organization that may hold an individual's PII. It gives individuals the right to get a report about their PII and access and review that personal information and know how the organization is using their PII. The DSAR report should include a confirmation that their data is held, describe how it's being used, whether it's been sold and to whom, the source of the PII, and whether artificial intelligence/machine learning is being used to make automated decisions, including profiling. Individuals are not even required to provide a reason for the DSAR.

Complying with these requests is complex, time consuming, and expensive. Most of the existing laws, along with the new privacy bills moving forward in state legislatures, provide only a limited time to respond to a DSAR. California's CCPA and Virginia's new law (just like European Union's GDPR) require that a request either be rejected (with very good reason) or the information provided in 30 to 45 days. Failure to comply can be costly—up to $7,500 with CCPA and Virginia's Consumer Data Protection Act, and up to $20,000 for particular violations of the Colorado Privacy Act.

But there's another factor that deserves much more attention: Ensuring compliance isn't easy or cheap. There are estimates that the average company getting hit with 142 DSARs a month in 2021 was spending on average $1,400 to respond to each request. That adds up to $200,00 per month—and DSARs are still an outlier.

## Conclusion

Some of these bills will be passed, some will not, but certain realities need to be accepted. Compliance will not be a choice. Consumers will continue to expect PII protection and won't have much sympathy for companies that don't comply.

We're in a new era of data privacy. The coming torrent of state-level laws will strengthen PII protection, and that's a good thing. State governments are doing exactly what their constituents want them to do.

Companies should consider how best to stay apprised of this rapidly evolving legal landscape and how they can strengthen their compliance programs to meet these new demands. Whether it is appointing a chief privacy officer, modifying training and policies, or developing new procedures and practices, there is a lot of work to be done to ensure compliance with the new privacy laws coming down the pike.

## Takeaways

- With the potential for new data privacy laws across the country, the issue deserves more attention than ever.
- Dozens of state-level data privacy bills are moving forward nationwide; by 2024, almost every state will have its own flavor passed into law.
- Many of these privacy laws have common provisions, but there are sometimes key differences—and these include potential landmines.

- While there are hefty fines for failing to comply, ensuring compliance—such as with DSAR statutes—can also be costly and time consuming.
- State-level privacy laws reach across state and country lines.

**1** Erika McCallister, Timothy Grance, and Karen A. Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, Special Publication (NIST SP) - 800-122, April 6, 2010, https://www.nist.gov/publications/guide-protecting-confidentiality-personally-identifiable-information-pii.
**2** Council Directive 95/46, 1995, O.J. (L. 281) (EC).
**3** Tanya Forsheit, Jessica B. Lee, and Shely Berry, "State-Proposed Comprehensive Privacy Legislation in 2022," Loeb & Loeb, February 2022, https://www.loeb.com/en/insights/publications/2022/02/state-proposed-comprehensive-privacy-legislation-in-2022.