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.