CEP Magazine - March 2021
Steer clear of US consumer data privacy law misconduct

By Itzhak Assaraf

Itzhak Assaraf is Chief Technology Officer and cofounder of 1touch.io, based in New York City.

Data privacy laws started trending with the European Union's General Data Protection Regulation (GDPR) and continued with the California Consumer Privacy Act[1] (CCPA)—which will eventually become the California Privacy Rights Act (CPRA) in 2023—and has expanded worldwide. All-encompassing consumer data privacy laws are now in the works, or have recently been passed, in India, Indonesia, South Africa, New Zealand, Malaysia, Tanzania, and many more countries across the globe.

In the US, there has also been a shift toward consumer data privacy, with the implementation of several state laws now underway. And though CCPA gets the lion's share of the press due to its depth and breadth of applications, it is not the only state-level consumer data privacy regulation on the books. Maine and Nevada have also recently enacted state-level laws that put the brakes on consumer data-sharing practices. Though both are far more limited in scope than the far-reaching CCPA, this represents commendable momentum in the shift toward a privacy-by-design approach to how consumer data are handled.

There are only three laws currently on the books, and another 10–12 are in some stage of the legislative process. We can expect this number to rise as additional states begin to recognize that consumers across the country now expect businesses to correct data privacy sins of the past and become transparent in their collection and sharing practices. This means that, within a few years, we can reasonably expect to see upwards of 10–15 state-level regulations on the books.

That is a whole lot of laws to adhere to simultaneously. Here we will outline the current and proposed consumer data privacy laws to understand where they overlap and where they diverge. By seeing what they have in common, we can get a baseline understanding of the most important elements of any consumer data privacy initiative.

Laws already on the books

The following are state laws that are already in force.

California

Let's start with the state that started it all. The CCPA went into effect in the state of California on January 1, 2020. The rights granted in CCPA apply to all California residents (i.e., individuals in the state for a nontemporary purpose and individuals who live in the state but are outside for temporary purposes).[2] Considering that this group makes up around 12% of the entire US population,[3] this makes CCPA compliance a "must" for any organization that collects personally identifiable information on either of the above categories of individuals.

The goal of the CCPA is to reestablish customers as the owner of their data and to provide them with five fundamental rights regarding the data they share with organizations:

1. The right to know what is being collected;
2. The right to know if and with whom their data are being shared, and the right to opt out;
3. The right to get access to the data that have been collected;
4. The right to deletion; and
5. The right to equal treatment if they do exercise their rights.[4]

Companies in violation of the law will be subject to fines of up to $2,500 for unintentional violations and $7,500 for intentional violations.[5] Individuals may seek damages up to $750 per individual per violation. The CCPA has become the model for all consumer data privacy regulations across the US.

Though CCPA has obviously been groundbreaking, in November 2020, Proposition 24, or the CPRA, was passed and will replace CCPA on January 1, 2023. This new law expands upon CCPA and will place additional fines and requirements on businesses. It will also oversee the establishment of the California Privacy Protection Agency as an independent watchdog agency to supervise the enforcement of the new data privacy law.[6] These changes, among many others, will align the state law much more closely with GDPR.

Nevada: Senate Bill 220

The Nevada Privacy of Information Collected on the Internet from Consumers Act went into effect in 2017. In October 2019, it was amended with Senate Bill (SB) 220, which requires website operators and online businesses to enable consumers to opt out of allowing their data to be sold.[7]

Businesses must establish a specific email or physical address for consumer opt-out requests, and requests must be fulfilled within 60 days (or up to 90 days if they have informed the consumer of the delay).[8] Anyone who owns a for-profit online business and collects data on Nevada residents must comply with SB220.[9] The law is much smaller in scope than CCPA, but there is still a $5,000 price tag for violations.[10]

Maine: An Act to Protect the Privacy of Online Customer Information

The Pine Tree State's newly enacted consumer data privacy law is concerned with internet service providers' data.[11] The law went into effect in July 2020 and stated that providers "may not use, disclose, sell, or permit access to customer personal information" unless specific consent has been granted.[12] Though this is clearly more narrow in scope than the CCPA, it is viewed by privacy experts as a significant win, as internet service providers, or broadband internet access providers, "know when we're sleeping, they know when we're awake… They may know more about us than we know about ourselves," according to lawmakers.