CCPA: What You Need to Know about California's New Privacy Regulations

By Yetunde Abass

Compliance

May 30, 2019

CCPA: What You Need to Know about California's New Privacy Regulations

Digital privacy rights have been a growing point of activism among consumers, legislators, and civil liberties experts. In recent years, protests and petitions have morphed into actual laws. In 2016, the European Union passed the General Data Privacy Regulation (GDPR)—the first major law addressing data protection and privacy. It went into effect in May 2018.

While there is no federal equivalent of GDPR in the United States, a growing number of states and municipalities are passing their own laws that address data privacy and security in some fashion. So far, only California has passed legislation that could be considered on a par with GDPR.

The sweeping law, known as the California Consumer Privacy Act (CCPA), passed in September 2018 and will go into effect on January 1, 2020. Although CCPA theoretically only covers residents of the state of California, it is likely that its effects will be felt nationwide.

Only in California?

It seems fitting that the first state to regulate data collection is also the same state where our modern technology landscape developed. In addition, although the final law was a bill passed by the California State Legislature, it started out in a very California way—as a state ballot initiative.

The individual who spearheaded the initiative was Alastair Mactaggart, a San Francisco real estate developer who was becoming increasingly wary of the amount of data being collected about him, his family, and his inability to access any of it. He assumed correctly that many other Californians felt similarly. In a keynote at Privacy. Security. Risk. 2018, Mactaggart said that his proposed law was based on three pillars:

Transparency – Consumers should be able to access the data collected on them.

Control – Consumers should be able to stop companies from selling their personal data.

Accountability – Companies should keep consumer data safe.

The purpose of the voter initiative and the subsequent bill (AB-375) was to regulate the third-party data resale market. Although not as all-encompassing as GDPR (the main point of division being an opt-in vs opt-out system), California's law may be the example for other states and possible federal regulation.

Breaking down CCPA

CCPA has three major components. Consumers have a right to:

1. **Knowledge** – California residents have a right to know what personal data is being collected about them; they also have the right to access this data. In addition, they have a right to know if their personal data is being resold, and to whom.
2. **Control** – Consumers can say no to their personal data being sold.
3. **Recourse** – Consumers can directly sue companies if their personal data is compromised or stolen.

According to the law, companies under the jurisdiction of CCPA must do business in California or with California residents and meet at least one of the following three requirements:

- Have annual revenue of at least $25 million.
- Use, buy, or sell the personal data of at least 50,000 consumers, households, or devices.
- Derive more than half of annual revenue from the selling of personal data.

Although CCPA does not cover all companies, many US-based and multinational corporations will fall under its jurisdiction. In addition, while this is a California state law, it will most likely affect all United States residents. Similar to how California's stringent emissions standards changed the cars that automakers sold across the US, CCPA may change data privacy standards for all of a company's customers—not just those who happen to live in California.

What to expect

Compliance

Compliance with CCPA will require companies to simultaneously guard personal data, while also making it accessible to any individual who wants to know what information is being collected about them. The ability of individual consumers to sue for damages as a result of a data breach poses an issue that many companies have never experienced before. They will be directly accountable to consumers instead of a state attorney general of a government regulator.

Damages range from $100 to $750, per person per breach or the actual consumer cost, whichever is higher. If the suit is brought by the attorney general, the damages can be much higher. While $100 to $750 seems like a small price to pay for data exposure, we know that a data breach rarely if ever only involves one consumer (for reference, of the 70 million US Facebook users affected by the Cambridge Analytica breach, 6.7 million were California residents).

via GIPHY

Becoming compliant with CCPA will require not only a change in mindset about consumer data privacy, but also a change in the technology used to access and protect it. One place companies can start is with is minimizing the use of third-party data processors. Organizations can reduce the risk of consumer data exposure by keeping as much information in house as possible—more on this later.

According to a recent TrustArc survey about CCPA compliance, new technology is a major component of CCPA preparation. Seventy-two percent of the 250 companies surveyed said that “technology and tools” would be an investment area for CCPA compliance. This exceeded every other category including consultants and legal expertise. The survey also found that companies are putting in significant financial resources to come into compliance by January 2020:

71% expect to spend at least $100,000

39% expect to spend at least $500,000

19% expect to spend at least $1 million

In the grand scheme of things, these are small investments to ensure data privacy and protect an organization from the costs of a data breach.

New Business Models

For internet companies that depend on advertising revenue, CCPA presents a challenge and an opportunity. For more than a decade, collecting data through web and mobile applications has been a cheap way to create targeted and personalized advertising programs. Under a new system where consumers can essentially opt out of tracking altogether, companies will need to convince consumers that this practice is still valuable. Maybe we will see fewer ads for the sake of ads and more solutions that solve consumer problems.

Future of data privacy laws

Not waiting to see how the California law will turn out, several other states including Hawaii, Massachusetts, and Maryland have drafted legislation similar to CCPA. There is currently no federal law that addresses privacy to the extent that CCPA does, but the growing number of proposed state laws may spur Congress into action. In late 2018, the Data Care Act was introduced in the Senate. Its aim is to hold organizations accountable for security breaches and allow consumers to control the sale of their personal data. This bill, however, has not been brought up during the current congressional session.

Interestingly, we are in a moment where corporations themselves see a need for federal data privacy regulations and oversight. Citing the "patchwork" of data breach and security laws, the Internet Association (the internet industry's largest trade group), is calling for federal legislation that would preempt any state or municipal law. In a November 2018 the organization published a policy statement recommending that the Federal Trade Commission (FTC) oversee and enforce a national data privacy framework.

What does CCPA have to do with MetaRouter?

As mentioned earlier, data privacy laws are nudging businesses away from dependance on 3rd party tools to be compliant. Naturally, the more risk an organization has surrounding data practices, the more control they would like to maintain over their infrastructure.

MetaRouter Enterprise helps to assuage these fears by allowing customers to bring our data engine onto their own stack through secure deployment in their private cloud. Furthermore, Enterprise enables security through features such as encryption, data conditioning (e.g. dropping PII in payloads), and robust monitoring. Interested? Learn more!

MetaRouter is a data engineering company with a mission to realize the robust and sustainable systems of the future. We create data routing solutions for all sizes, from our private cloud enterprise edition to our accessible hosted cloud offering. Sign-up for Cloud Edition or contact us about Enterprise Edition or with questions at support@metarouter.io.

CCPA compliance data regulation

Yetunde Abass / About Author

› More posts by Yetunde Abass

Related Posts

Five Key Takeaways from the

14 Mar 2019

GET STARTED

Cloud

ABOUT

PRICING

SIGNUP

LOGIN