

BUSINESS INSIDER

As Enforcement of California's Data Privacy Law Kicks in Today, Here's How Experts Say Companies May Face Big Penalties

Business Insider

Jeff Elder

July 1, 2020

[\[Link\]](#)

- Enforcement of California's privacy law begins today, and many questions linger about how the state will handle it.
- The law calls for fines against companies that fail to protect consumers' data, but it's not clear where the attorney general will focus enforcement.
- The attorney general has said of offenders "I will descend on them and make an example of them."
- Experts say companies need to show they're making an effort to comply, and pay particular attention to the rules around selling data and data breaches.

Enforcement of California's privacy law, which is designed to punish companies that fail to protect consumer data, begins Wednesday. The state was still tinkering with the law last month, and many questions linger about its enforcement.

The uncertainty has built up a certain amount of suspense about the California Consumer Privacy Act, especially after the state's attorney general delivered a warning that seems charged with Biblical thunder:

"I will descend on them and make an example of them, to show that if you don't do it the right way, this is what is going to happen to you," Xavier Becerra [said in December](#).

The CCPA was signed into law in 2018 and went into effect January 1. But final revisions to the law have [lingered on](#). So it remains to be seen exactly how consumer advocates will seek to use it, and how Becerra wishes to enforce it. Enforcement of a similar privacy law began in Europe in 2018, and has taken many forms, from [a German police officer](#) being fined for looking up a driver's phone number to [Google being fined \\$57 million](#) by France.

Attorney Miriam Wugmeister of the law firm [Morrison & Foerster](#)'s pre-eminent Global Privacy and Data Security Group, says, "The big question is, where is the attorney general going to focus his attention? It's likely to be the key provision on companies not selling consumer data, and the ability for people to exercise their individual rights. That's what we have to wait and see."

Like Europe's stringent General Data Protection Regulation, the CCPA provides for sanctions against companies that leak, fail to protect, or mishandle consumer's personal information, such as their addresses, Social Security numbers, credit information, and other data. The law also allows consumers to demand access to the data a company has extracted and stored about them.

Dan Clarke, president at [IntraEdge](#), an Arizona technology development company, leads the firm's work on [Truyo](#), a privacy compliance platform built with Intel to help companies provide customers with access to their data. He is not a lawyer, and this is not legal guidance, but here's what Clarke believes will be key areas, based on his study of the state's legislative work on the law.

How fines are applied

Initially the CCPA fines don't seem that steep: Up to \$2,500 per accidental violation, or up to \$7,500 for each "intentional" violation, when a business is aware of the law, but breaks it anyway. But companies can also be subject to a \$750 fine per consumer. In a data breach affecting a million customers, that could amount to three-quarters of a billion dollars.

Who will get hit

Companies that fail to provide consumers with a way to request their data will likely see [complaints filed with the state](#) about them. If a company is complained about multiple times, the state is likely to take action. Companies that suffer a data breach are also likely candidates, Clarke says. "One of the things we saw with GDPR is that enforcement often followed a breach, and I think it's fair to assume that will happen here."

Will companies make an effort

"What's top-of-mind for enforcement in my estimate is having something visible to show that you're really trying to be transparent and do your best to comply with a lot of the CCPA," Clarke says. In the same interview where he threatened to smite scofflaws, Becerra said he would "look kindly" on companies that "demonstrate an effort to comply."

Will privacy policies be everywhere

On their websites and mobile apps, companies should have already posted their privacy policies, which inform consumers about the data the companies collect. [Here is California's guidance](#) on posting privacy policies.

Will companies be prepared to accept data requests

The backbone of the CCPA is that "a consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer" what has been collected. Businesses need to have some mechanism for doing so. "You need to be able to accept an intake request, and it needs to be easy for a consumer to say, 'I want to exercise my rights under this law'," Clarke says. [Here](#) is how the ecommerce platform Shopify helps its merchants get started taking CCPA requests.

Do companies know where the law applies

Companies must comply with CCPA if any of these criteria apply to them:

- Makes an annual revenue of more than \$25 million in total
- Receives personal data from at least 50,000 California residents, devices or households per year
- Obtains 50% or more of its annual revenue from the personal information about California residents

The key: Selling consumers' data

Consumers have a right to know if companies are selling their data to other companies – and have a right to tell them not to. This can be a complex and demanding aspect of [the law](#) for online advertising and marketing firms. [Here is Truyo's guide](#) to this key aspect of the law.

Seeing the big picture

Clarke says the CCPA represents ongoing obligations for companies. "It's not just a one-time notice. You have to be able to serve a consumer who says, 'I want to see my data; I want to delete my data; I want to understand exactly what you're doing with my data.' This law allows a consumer to exercise those ongoing rights."