Enforcement of Calif. Data Privacy Law Begins
Women's Wear Daily
July 1, 2020
Adriana Lee
[Link]

As consumers look ahead to the Independence Day weekend, businesses mark another milestone today: On Wednesday, enforcement of the California Consumer Privacy Act begins to rein in companies from playing fast and loose with consumer data.

Some businesses had hoped Gov. Gavin Newsom would hold off on the regulation, a first of its kind in the U.S., in light of the coronavirus crisis and its resurgence in the Golden State.

No such luck. Now businesses from Silicon Valley to L.A., as well as others, must audit their business practices, policies and vendor relationships to ensure they don't run afoul of the act, which was signed into law two years ago and went into effect as of January.

That the rules cover more than tech-makers should be apparent. Today, practically every organization may be considered a tech company, whether due to running over a digital platform, offering services online or using back-end tools like artificial intelligence and machine learning to improve preference predictions.

The CCPA protections also go beyond the state's borders.

"Retailers, or any online company that does business with California residents, need to be aware of the risks of CCPA enforcement," said Julie O'Neill, partner in Morrison & Foerster's global privacy and data security group. "The risk of not complying with CCPA arises regardless of where the company is headquartered or operates, and may extend to brands' mobile apps as well."

Like Europe's General Data Protection Regulation, the CCPA focuses on data privacy rights, offering consumers more transparency and control over their personal information.

But they are not identical, Jennifer Rathburn, a partner at Foley & Lardner LLP, told WWD. The firm has been instrumental in developing Foley's Custom Made Counseling for the Fashion Industry in partnership with the Beacon Council, Miami International University of Art & Design, and The Fashion Group International. The collaboration of professionals provides advice on manufacturing, business, design and technology matters to the fashion, apparel and design industries.

When it comes to CCPA compliance, Rathburn said that a company that already conforms to the GDPR could be "at least 70 percent of the way there…the GDPR can be even more stringent in many ways. But there are differences." She brought up the example of someone requesting or needing to know their information-access rights, as they hold different exemptions.

"There's a whole big thing under GDPR about the rights to erasure or deletion. The CCPA actually has many exceptions to this that are different than GDPR," she added. Those details matter, especially for any brands or retailers partnering with tech vendors that tout GDPR compliance.

Some of the nuances in the baseline grounding of the law may need to be clarified as well. Per the CCPA, California consumers have a right to know, the right to delete, and the right to opt out of any sale of their personal information that businesses collect.

Some of that hinges on what constitutes a sale of personal data.

"The CCPA defines a 'sale' broadly to mean the disclosure of personal information for monetary or other valuable consideration, and it requires that a business provide California residents a way to opt out of any sale, or to opt in, with respect to minors under age 16," said Morrison & Foerster's O'Neill.

An e-commerce site that uses cookies — or small bits of data used to track users' online activity — may not use the information externally, but what about its tech service provider?

"The use of cookies for certain types of interest-based advertising — such as where a user is tracked across multiple web sites — may be deemed a sale because, for example, each of the participating web sites essentially makes information about its users available to the other web sites, so that each can better tailor the ads it serves," she added.

But O'Neill also pointed out that whether or not the use of cookies involves a sale depends a lot on the particular case-by-case details, including whether companies allow pop-up opt-out notices for cookies.

"If the vendors you use take data and do something else with it, other than on your behalf, then it becomes a quote-unquote 'sale of data,'" clarified Foley & Lardner's Rathburn. "So I think the question is not so much how you're internally using it, but if you're using third-party vendors to assist you with your data modeling, you have to be really careful how those vendors are using your data."

According to the law, service providers are allowed internal use of the information to create or improve their quality of services, "provided that the use does not include building or modifying household or consumer profiles, or cleaning or augmenting data acquired from another source."

So the complication, Rathburn said, "is really that aggregation of data across multiple businesses." That may not affect cases where data is anonymized — for instance, to gain insights into broader fashion or shopping trends. But in others, where personal information is pegged to specific shoppers, businesses may need to tread carefully.

Consider loyalty programs.

The CCPA comes with certain obligations on financial incentives, "if they restrict consumers' data rights," O'Neill noted, so "loyalty programs should be carefully reviewed to determine whether they constitute a 'financial incentive.'" If they do, then it's subject to particular CCPA rules. Notice and consent obligations would have to apply, and the benefit for the consumer would have to relate directly to the value provided to the business by this personal information.

Whether loyalty programs fall into this category depends on a variety of factors, including whether consumers have the option to delete their personal information, among others.

Retailers often hire loyalty program providers to handle their club memberships or other initiatives, which could add another layer to their compliance efforts. Although much of the CCPA conversation revolves around direct-to-consumer companies, businesses that serve other businesses and, say, handle their shopping data should definitely scrutinize their practices.

At a bare minimum, any companies that partner with them should know how they handle the information.

The rules can vary, depending on the sector and the case-by-case details, but the CCPA isn't yet totally comprehensive. It leaves plenty of open privacy questions — including how companies should regard employee data. That issue takes on new relevance now, as it meets contact tracing efforts through the pandemic.

Either way, brands and retailers shouldn't procrastinate to evaluate their practices. Ideally, as the law went into effect at the beginning of the year, they've already created a data map outlining how they're

collecting information and to whom they're disclosing it. If not, then they must act quickly. Legislative attention is not likely to go away. In fact, it's poised to ramp up — regardless of where companies do business.

"The interesting part is that this is really the most broad-based privacy law that we have seen, and other states are picking up on it," said Rathburn. "So I really do think that whether it's tomorrow or within the next couple of years, many states…are going to adopt similar concepts around the sale of data and consumer rights."

According to Rathburn, it may only be a matter of time before such measures become prevalent. At some point, she said, "we may even see a federal law."