Comment: California privacy agency's ambitious regulations aim to restore consumer control of data

6 Jun 2022 | 23:07 GMT | **Comment**
By Mike Swift and Amy Miller

California's new privacy regulator has set out its first clear marker for an ambitious interpretation of the California Privacy Rights Act passed by the state's voters in 2020: It aims to put consumers in full control of their data, perhaps more so than any time since the advent of the commercial Internet.

California's new privacy regulator has set out its first clear marker for an ambitious interpretation of the California Privacy Rights Act passed by the state's voters in 2020: It aims to put consumers in full control of their data, perhaps more so than any time since the advent of the commercial Internet.

The California Privacy Protection Agency proposed some of the most far-reaching regulatory standards and limits to date when it released its first round of draft CPRA enforcement regulations on May 27 (see here). The draft regulations aim to limit "dark patterns" used to manipulate consumer decisions, enable global opt-out controls that consumers might tap to limit collection of their data, and allow consumers to control the downstream use of their personal data by entities that lack a direct relationship with consumers.

There has long been an information asymmetry between what businesses know about the personal data they collect from consumers and what consumers understand about its collection and use. That's intended to change under the CPRA: Consumers can no longer be surprised by who, or how, their data is being used, the privacy agency said Friday.

The first round of proposed regulations "clearly explain that the CPRA amendments now restrict businesses from collecting, using, retaining, and sharing consumer personal information in a manner that is inconsistent with consumer expectations, unless they obtain the consumer's explicit consent," the privacy agency said in a filing that details its reasoning behind the proposed regulations (see here). "In doing so, the regulations place the consumer in a position where they can knowingly and freely negotiate with a business over the business's use of the consumer's personal information."

The proposed regulations were written, the privacy agency said, with an eye toward harmonization with Europe's General Data Protection Regulation and privacy laws passed by the states of Colorado, Connecticut, Utah and Virginia. They are also intended to have a marketplace effect, by spurring "innovation in pro-consumer and privacy-aware products and services."

The CPPA's proposed regulations are aimed at making the process of exercising new privacy rights as easy and as transparent as possible for consumers. Any consumer choice that is manipulated or subverted by a company will be considered a dark pattern, which is forbidden under the CPRA.

Businesses, however, would face a host of new prescriptive requirements that some warn could have unintended consequences and hamper economic growth. As ambitious as they are, the proposed regulations — the CPPA board is due to discuss and perhaps vote on them Wednesday — don't appear to be in danger of being preempted by a federal privacy law. The compromise proposed Friday in Congress (see here) would exempt the CPRA from preemption by the federal American Data Privacy and Protection Act.

— Dark Patterns —

The proposed draft CPRA regulations set out specific requirements for how businesses should handle consumers' requests for information, and how they obtain consumer consent. The proposed regulations are intended to put the obligation on businesses, the CPPA said in Friday's statement of reasoning, to "ensure that the consumer's choice is freely made and not manipulated, subverted, or impaired through the use of dark patterns."

The proposed regulations are significant in part because they spell out in such detail what the California regulator will determine is a dark pattern and what is not, in a way few, if any, other privacy regulators have done.

"'Dark patterns' is definitely the first thing that caught my eye," said Ali Jessani, a privacy lawyer with the firm WilmerHale

who has reviewed the proposed regulations. It's "the first time we've seen a regulation come out with explicit standards about what constitutes a dark pattern."

When obtaining consent, businesses must use methods that are easy to use and understand. They must provide for "symmetry" in choice. For example, a "yes" button must match with a "no" button, and an "Accept All" option must match with a "Decline All" option.

Companies can't use confusing or manipulative language and elements, and must avoid manipulative language, including guilting or shaming language.

For example, businesses cannot offer choices such as "No, I like paying full price" or "No, I don't want to save money," according to the draft regulations.

The CPRA requires businesses that sell or share personal information to provide an opt-out link for consumers, and they're already required to post "Do Not Sell My Personal Information" links under the CPPA.

The draft CPRA regulations would add several new requirements for those links. They must appear just like other links posted on a company's homepage. For apps, links must be accessible and included in their privacy policy.

If a business processes sensitive personal information, it must also post a "Limit the Use of My Sensitive Personal Information" link.

Additionally, businesses will have to confirm that they've processed consumer opt-out requests. A "business may display on its website 'Consumer Opted Out of Sale/Sharing' or display through a toggle or radio button that the consumer has opted out of the sale of their personal information," according to the draft regulations.

Some privacy lawyers, many of whom lost much of the Memorial Day weekend as they scrambled to read the highly anticipated California regulations, said they were surprised the dark-patterns rules would apply to more than just a request for consumer consent, but would also apply to consumers' efforts to apply other CPRA privacy rights, such as data transparency or deletion requests.

"I thought that was pretty significant, because the CPRA regs have pretty prescriptive orders," said Jenna Rode, a member of the global privacy and cybersecurity practice at Hunton Andrews Kurth.

— Opt outs —

Proposed regulations around global opt-out signals will be another point of contention.

The CPRA gives businesses the option of recognizing opt-out preference signals as valid consumer requests to opt out of the sale or sharing of personal information and to limit the use of sensitive personal information.

Last July, California's attorney general's office said that businesses must honor the Global Privacy Control, a browser signal that automatically lets consumers exercise their right to opt out of the sale of their personal information (see here). Businesses must treat GPC "as a valid consumer request to stop the sale of personal information," the AG said.

Now under the proposed CPRA regulations, companies would be required to recognize "opt-out preference signals." To make things more confusing, the draft regulations don't lay out any technical specifications for opt-out signals.

If a company processes opt-out signals in a "frictionless" manner, however, it doesn't have to post opt-out links. Processing in a "frictionless" manner means a business can't charge a fee when consumers use an opt-out preference signal. They also can't change the product or the service that is offered, or display any sort of pop-up notification in response to an opt-out preference signal.

"This regulation is also necessary to strengthen consumer privacy and is consistent with the CPRA's amendments that limit how complying entities use consumer personal information," the privacy agency said, explaining the need for the rule.

— Downstream data regulation —

The proposed regulations also expand the privacy obligations for the business partners and other third parties that store or process consumer data as part of their relationship with the company that collects personal data – entities that lack a

direct relationship with a consumer.

If a company receives a request from a consumer to delete personal information, the proposed regulations specify that the company must notify any service providers or contractors that hold that data to delete it, “and to notify all third parties to whom the business has sold or shared the personal information to also delete the information unless this proves impossible or involves disproportionate effort,” Friday’s filing says.

The proposed regulations require companies to identify the specific business purposes and services for which the service provider or contractor is processing consumer data on behalf of the company that collected that data. The proposed regs spell out that the privacy agency can audit not only the company that collected the data, but also may audit a service provider, contractor, or person that partners with the company collecting data to ensure CPRA compliance.

The proposed regulations define an audit as “an investigative tool that can be used to determine whether a violation" of the CPRA occured.

Jessani said that means companies that collect consumer data will have to spell out specific contractual terms with partners that receive access to that data. “It makes you evaluate all of your business relationships,” Jessani said. “It’s creating a pretty high standard for everybody that deals with Californians’ data.”

The 66-page set of proposed regulations are widely expected to be followed by other installments, before the CRPR takes effect Jan. 1. Enforcement is due to begin in July 2023. The California privacy agency has yet to release proposed regulations for areas such as automated decision-making and profiling, and cybersecurity audits.

But the first round of proposed regulations does begin to flesh out the specifics for how the new law will be enforced.

“They provide a lot of examples, and I think a lot more insight into what the regulator is really concerned with,” Rode said. “I wouldn’t say it’s groundbreaking and it’s going to completely change how a company’s compliance program is going to operate, but it’s new, additional obligations that need to be fulfilled.”

Please email editors@mlex.com to contact the editorial staff regarding this story, or to submit the names of lawyers and advisers.

Related Portfolio(s):
Data Privacy & Security - California Privacy Protection Agency - Creation and organization of California's new privacy regulatory agency (US)

Areas of Interest: Data Privacy & Security

Industries: Communication Services, Information Technology, Interactive Media & Services, Media, Media & Entertainment, Software and Services

Geographies: California, North America, USA

Topics:

CCPA (California Consumer Privacy Act) | Cybersecurity | Data Privacy | US state privacy legislation