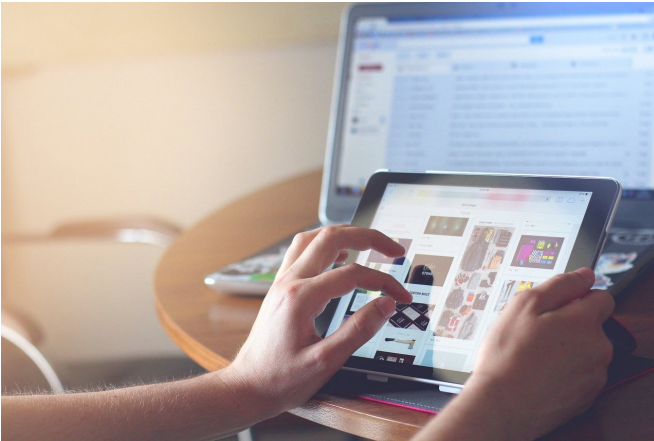


California is rewriting the rules of the internet and businesses are scrambling to keep up

27 December 2019, by Sam Dean



Credit: CC0 Public Domain

A sweeping new law that aims to rewrite the rules of the internet in California is set to go into effect on Jan. 1.

Most businesses with a website and customers in California—which is to say most large businesses in the nation—must follow the new regime, which is supposed to make online life more transparent and less creepy for users.

The only problem: Nobody's sure how the new rules work.

The California Consumer Privacy Act started from a simple premise: people should be able to know if companies sell their [personal information](#), see what information companies have already collected on them, and have the option of quitting the whole system.

But nothing is simple when it comes to the high-speed and largely opaque online data economy.

For more than two decades, tech companies have built a deeply enmeshed system to track the habits and identities of millions of users, every second of every day, and then swap or sell that information to further fine-tune marketing, advertising and business strategy.

Thanks to the technical complexity of the system and the rushed timeline for implementation, a number of basic questions remain unanswered. What does "sell" mean? How can companies be sure they're deleting the right person's data? And does simply having a website that keeps track of how many people visit each year mean you must wade into the regulatory thicket?

The Attorney General's office, which is tasked with both interpreting and enforcing the law, only published its first round of draft regulations in early October. A final set is unlikely to come until well into 2020, and the law won't be enforced until July.

In the meantime, businesses are scrambling to make sure they aren't breaking the basics of the law. Big companies are signing deals with firms that specialize in compliance to create "do not sell my personal information" buttons on their sites (and ensure they actually work). Small companies are setting up email accounts to deal with customer requests—or just keeping their heads down and betting that the attorney general won't bother picking on them once enforcement starts.

"There is not a privacy lawyer in the industry that is not working around the clock right now to get ready for Jan. 1," said Michael Hahn, general counsel for the Interactive Advertising Bureau, an industry group made up of companies in the online advertising ecosystem.

It began when Alistair McTaggart, a San Francisco

real estate developer, had a disturbing conversation going on.

about digital privacy with a Google engineer at a cocktail party. He decided to bankroll a 2018 ballot measure campaign. Sacramento lawmakers struck a deal to turn it into law, and unusually for a law that stands to affect billion-dollar companies, it remained largely unchanged by lobbying efforts through 2019.

In the data economy, users' personal information can be used in lightning-fast transactions, like the real-time auction that goes on behind each online ad, and stored in databases for decades.

Sometimes, companies sell personal information—someone's location, age or even name—without any contact information, or easy ways to verify that individual's identity.

The result is a murky mix of total surveillance and slapdash record keeping, which makes answering seemingly straightforward demands like "tell me what information you have collected about me" and "stop selling my information" surprisingly complex.

For businesses, the impact has been the digital equivalent of requiring every driver in the state to install a new catalytic converter in their car or face a fine—without sharing any brand names or technical specs of the required upgrade. A 2019 report commissioned by the Attorney General's office estimated that getting in compliance with the law could cost the companies affected \$55 billion up front, with the potential for an additional \$16 billion over the next decade.

The lawmakers behind the rules see the chaos as necessary to rein in an industry that's been operating unchecked for decades.

"It's really been the Wild West," says Bob Hertzberg (D–Van Nuys), the California State Senate majority leader who championed the bill in Sacramento.

"There's always a bit of a scramble, but the key is keep your eye on the horizon, and make it workable but deeply forward-facing in terms of consumer protection."

Companies affected by the new rules gave up on opposing them once it was clear that they would become law. Now they just want to figure out what's

At a meeting in early December in Los Angeles, representatives of powerful trade groups and concerned individuals alike lined up to express not so much opposition as confusion as part of the comment period that will shape the next round of draft regulations.

Peter Watson, a board member for the California Self-Storage Association, asked a basic question: which businesses have to follow the law?

The CCPA only applies to companies with more than \$25 million in revenue or access to the personal information of more than 50,000 people. So if a self-storage [company](#) has the information of 10,000 current and former tenants, but more than 50,000 people visit its website every year, thus sharing their IP addresses with the company, does that qualify?

Other questions circled around what seems like a contradiction: in some cases, companies might need to ask for more personal information in order to carry out a user's request to delete or get a copy of all of their personal information. They may know that someone named Maria Garcia is 36 years old, likes trucks and legal dramas, and regularly logs in from a phone in central LA, but if someone emails claiming to be Maria Garcia and asks for all that information on themselves, how can a company be sure it's the right one? Can they ask for more personal information, like an specific email or a social security number, to verify?

Bo Kim, counsel for the California Chamber of Commerce, began with a plea to move the deadline to January 2021, then highlighted one way in which the draft regulations run up against the limits of human knowledge. One provision requires companies to share, in their privacy policies, the value of an individual user's personal data.

"The vast majority of companies impacted by the CCPA utilize technology but are not tech companies," Kim said. "As such, there is no particular value of data allocated on any existing balance sheet."

The most wide-ranging impact of the new law falls on the online ad economy and the businesses—including tech giants such as Facebook and Google and media companies like The Los Angeles Times—that rely on it.

The core mechanism of the online ad world is called real-time bidding: behind every ad on a webpage (including this one), there's a near-instantaneous series of transactions going on.

The page itself, through the use of digital trackers, collects data on the reader. Then, the page sends this user information up the pipeline along with a certain set of rules, such as what kinds of ads it's willing to show, and at what price. An ad exchange then instantly arranges an auction for the space and the user, often seeking the highest bid among ad buyers who have also pre-entered their preferred targets, prices and what their ads look like. Once this whole process takes place—in a matter of microseconds—the ad appears.

Today, each entity along the way typically saves whatever data it can for later. The more information that a page knows about a user, the higher the price it can charge for an ad—and each little slice of information can be added to a consumer profile, which can be sold to other companies down the line looking for a more targeted audience.

That practice has allowed the ad tech industry to amass consumer profiles on millions of people. The new law empowers Californians to stop that surveillance in its tracks.

The CCPA doesn't break the real-time bidding chain of data transfer and ad display—and McTaggart has been clear that that was never the intent—but it does allow users to opt out of the second phase of the process, where their data is stored and packaged to be sold in the future.

Those who opt out will likely see fewer hyper-targeted ads, the kinds that show users an ad for a product that they left unpurchased halfway through the checkout process, or that seem to eerily show an ad for a store they visited a few days earlier. Combined with multiple deletion requests, users could eventually see only ads that are related to the

page they are visiting—car ads on an article about cars, or meal-delivery ads on a food website.

The Interactive Advertising Bureau, a consortium that includes most major publishers advertisers, and ad [tech companies](#) in the U.S., spent much of 2019 convening meetings to figure out how the thousands of companies along the pipeline could honor users' requests to opt out of having their data sold. It came up with a complex framework of contracts and digital tags that functionally staple a user's desire to not have their data sold to the data itself, like an ink tag on a piece of merchandise.

Google signed on to this system in December, and gave its customers—which include most of the websites on the internet—a toolkit for building this opt-out system into their own sites.

Facebook, notably, declared in a blog post that it didn't need to change its practices to comply with the law. The company's argument hinges on the definitions of sales and third parties, working from the premise that since Facebook is the only entity gathering and monetizing personal data within their system, it doesn't engage in sales of user data to third parties.

If enough people opt out and ask that their data be deleted, this could have the effect of cutting advertising revenues across the board. Advertisers are willing to pay a premium for a higher-quality target: diaper companies, for example, want to show their ads specifically to new moms, not a random website visitor. This is how Google, which builds profiles based on users' searches, app usage, and any other information it can glean from devices, has become a \$930-billion company. And Facebook has reaped similar rewards from its user-generated trove of behavioral data.

But most industry experts seem to think that the new law is unlikely to affect the bottom line of data-driven businesses (beyond the cost of basic compliance), simply because most users are unlikely to bother to opt out.

"People say yes," says Ben Barokas, chief executive of the compliance management company SourcePoint. "Even when there's the option to say

no, maybe 10% of the people say no" to having their data sold to show more targeted advertising.

Europe's General Data Protection Regulation, or GDPR, is a useful point of comparison. Under that regime, users had to actively opt into being tracked online and having their data sold—a provision that some activists pushed to be included in the California law. But still, there's no clear data that overall ad revenues suffered long-term declines after the law kicked in in May 2018, and some reports show that 95% of users choose to be tracked in exchange for access to websites and services.

Even as companies hustle to get in compliance, the people behind the CCPA are preparing to introduce a new round of privacy regulations in the form of a 2020 ballot measure. The major changes include the creation of a distinct agency to enforce the laws, rather than leaving it to the AG's office, creating an opt-in system for users under 16, and further restricting the use of what the initiative calls "sensitive personal information," which includes data such as location, health status and sexual orientation.

McTaggart hopes that the next round, with a funded and staffed privacy agency, can set a new standard for the internet as a whole.

"We think it will do for privacy what the California Air Resources Board did for air quality nationwide," McTaggart said.

He said that the intent wasn't to destroy any businesses, but to make sure that businesses were using consumer data safely. Or to extend the car analogy to the digital smog of the data economy: "We think cars are fine, and we understand LA has a lot of cars, but it would just be nice to see across LA on a clear day."

©2019 Los Angeles Times

Distributed by Tribune Content Agency, LLC.

APA citation: California is rewriting the rules of the internet and businesses are scrambling to keep up (2019, December 27) retrieved 19 October 2021 from <https://techxplore.com/news/2019-12-california-rewriting-internet-businesses-scrambling.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.