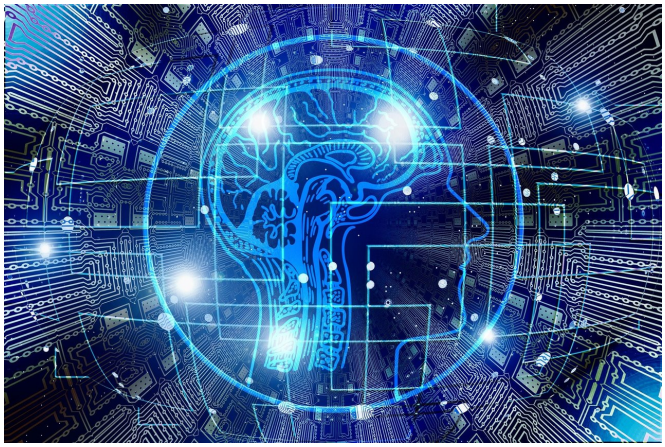
# In 2020, Californians will have new privacy rights online. But they might have to show ID

2 January 2020, by Sam Dean, Los Angeles Times



Credit: CC0 Public Domain

The internet is going to look, and work, a little different starting today. That's because Californians have new rights over how their personal information is gathered, stored and sold by any company operating in the state as of Jan. 1, thanks to the California Consumer Privacy Act, or CCPA.

As businesses scramble to get in compliance with the law, you've probably seen a rash of pop-up notifications and emails about privacy policy updates. You may also have noticed the small-print "do not sell my information" buttons that have started appearing at the bottom of websites.

But what are these new rights? How can you actually exercise them? And will any of this make a difference in how you use the internet?

Three new rights are at the heart of the CCPA, the strongest consumer data privacy law in the nation: the right to know, the right to delete, and the right to opt out.

**Knowing is half the battle**

The right to know means that you can ask a company to produce a copy of all the personal information it has gathered on you over the years, and let you know the categories (although not the specific names) of businesses it gathered that information from or sold that information to.

This also means that companies have to notify you—typically in their privacy policy—which categories of personal information they collect, and let you know if they're selling it to third parties.

**Hitting delete**

The right to delete means that companies must delete all the information they have on you when you ask, and if they had shared your information with another company they hired to perform a service, they must tell that company to delete it, too. Companies can still keep data they deem necessary for some uses, such as completing an ongoing transaction or detecting security breaches, but by and large they're required to zero you out if you request it.

Companies subject to the law (which include most companies with websites and customers in California) have to provide at least an email address and a toll-free phone number where you can submit these requests, which you should be able to find in their privacy policies.

A separate law passed in California this year will require any companies that act as data brokers—these are companies that never interact directly with consumers, but who amass and sell data from other sources—to register with the state

by Jan. 31. The attorney general will then post that list of data brokers online, and you can go through and make information or deletion requests there, too.

Where it gets complicatedBut a knotty problem lies at the heart of both of these new rights: How can companies make sure that they're deleting or sharing the right person's information?

Despite the eerie accuracy of some hyper-targeted ads and the (correct) feeling that you're being watched at all times online, the sophisticated system of tracking and sharing your personal data is not perfect. Technical challenges baked into the architecture of the internet make it difficult for many companies to verify, with complete accuracy, who is on the other side of the screen at any given moment.

Thanks to this fundamental fuzziness, even Facebook, the company that probably knows the most about you, is telling users that it might need to ask for a photo of a government ID before it can comply with a right-to-know or right-to-delete request. This extra level of verification is intended to prevent situations where one David Lopez gets sent the comprehensive profile of a different David Lopez—or even worse, someone impersonating David Lopez gets their hands on his most personal information.

And this information is personal. The law concerns information that is specific enough that it could be clearly linked to you or your household. That includes things like your name, address, IP address, device ID number, social security number, email address, purchasing history, face or fingerprint image, browsing or search history, physical location, employment or education information, audio or video recordings, and even descriptions of your physical characteristics.

**Get out**

The third right—to opt out—seems like it should be straightforward, but it comes with a lot of caveats and technicalities.

For starters, it entitles users to opt out of having their data sold on to third parties, but it does not allow them to opt out of having their data collected and used in the first place.

If you click one of the many "do not sell my personal information" buttons that will soon be on every website you visit (though you might need to scroll down to the bottom to find them), the company operating the website is obligated to earmark your personal information as a chunk of data that it can't package and sell to a marketing firm or data broker. But it can still keep collecting data every time you visit for its own uses—which includes selling targeted advertising.

Alastair Mactaggart, the San Francisco real estate developer who led the initial effort to have this privacy law passed as a ballot measure in 2018, has always maintained the law wasn't intended to abolish targeted advertising. Having an ad follow you around the internet may be one of the more viscerally uncanny experiences of the data economy, but the set of rapid transactions between sellers and buyers that produces those ads is kosher under the CCPA, since each business along the pipeline is only using the personal information to deliver a service (the ad), not selling the information on to a third party.

This system stands in contrast to Europe's more stringent privacy law, the General Data Protection Regulation, or GDPR, which requires that companies ask users to opt into having their data collected in the first place. Under that system, users have the ability to cut off the data stream that fuels the targeted ad economy at the source.

Under the California system, it might be difficult to notice much of a difference in the browsing experience even for the most active exercisers of these new rights. If you request that every website you visit delete your personal information and opt out of having your information sold whenever you can, there's a chance that you'll see less and less specific advertising as time goes on.

But the law's transparency provisions are set to give users an unprecedented look into how their personal information is shared and monetized across the internet. And the law's main backers,

including Mactaggart and California state Senate Majority Leader Bob Hertzberg, D-Van Nuys, are preparing a new ballot measure for 2020 that will beef up the regulations surrounding more sensitive personal information, such as location, health status and sexual orientation, create a GDPR-style opt-in system for users under 16, and fund a new standalone state agency to enforce these rules.

Already, a number of large businesses are changing their privacy policies for all U.S. users to match California's requirements.

So California—where much of the digital world we all live in today was first invented—may yet lead the rest of the country toward a more privacy-oriented internet.