Wired.com

‘Do Not Track’ Is Back, and This Time It Might Work California’s privacy law says businesses must respect universal opt-outs. Now the technology finally exists to put that to the test.

WHAT DO YOU call a privacy law that only works if users individually opt out of every site or app they want to stop sharing their data? A piece of paper.

Or you could call it the California Consumer Privacy Act. In theory, the law gives California residents the right to opt out of any business selling their data. In practice, it hasn’t seen much use. Most people don’t go to the trouble of opting out of every website, one at a time. One analysis, by DataGrail, a privacy compliance company, found that there were only 82 “do not sell” requests for every million consumer records over the first six months of the year.
A study published last week by Consumer Reports helps explain why: Opting out of everything is a complicated pain in the ass.

Change could be coming, however. The CCPA includes a mechanism for solving the one-by-one problem. The regulations interpreting the law specify that businesses must respect a “global privacy

control" sent by a browser or device. The idea is that instead of having to change privacy settings every time you visit a new site or use a new app, you could set your preference once, on your phone or in a browser extension, and be done with it.

When the attorney general issued those regulations, the technology for a global opt-out didn't exist. As of today, it does. This morning a group of privacy-focused tech companies, nonprofits, and publishers, including *The New York Times,* the Electronic Frontier Foundation, and the search engine and browser DuckDuckGo, announced the beta launch of a new global privacy control. The idea is to create a technical specification that qualifies as a universal opt-out under the CCPA, so that exercising rights under the law would flip from being hopelessly complex to extremely easy.

"This would provide a key component that's called for in the California law, which is a simple way for consumers to invoke their right without having to go to each website and find the button," said Ashkan Soltani, a privacy researcher who helped lead the effort. Soltani has spent as much time as anyone in the trenches of privacy controls. A decade ago, as a technologist at the Federal Trade Commission, he worked to develop the Do Not Track web standard, which was supposed to establish a universal opt-out.

That effort was ultimately doomed, however, because companies were under no legal obligation to honor Do Not Track requests, and most chose not to.

The technology, in other words, was too far out in front of the law. But now, with the CCPA, the inverse is true. “The law, for the first time, is kind of ahead of the technology,” said Soltani.

The idea for the new global opt-out started with Sebastian Zimmeck, a computer science professor at Wesleyan who began building a Chrome extension called OptMeowt with his students last spring. In April, he connected with Soltani, who helped pull more collaborators into the effort. As of today, users will be able to set a global browser opt-out in browsers including Mozilla, Brave, and DuckDuckGo, as well as the DuckDuckGo privacy extensions for Chrome. The code necessary for businesses to respond to the privacy control is publicly available. Publishers who have signed on, most notably *The New York Times* and *The Washington Post*, have agreed to honor the signal.

For California residents, the global privacy control, if enforced by the attorney general, would have a very different effect than existing privacy controls such as third-party cookie blockers. Those settings have no power over what a website or app does with the data

it collects directly from you. The global control, by contrast, would issue a legally binding order that, if violated, would be punishable by major fines.

The new specification won't become legally binding until the California attorney general blesses it. Even then, several obstacles could prevent it from having a big impact. The question of what exactly counts as a "sale" under the CCPA is still under debate and might eventually need to be settled in court. But even if that issue gets resolved in a way that exempts a lot of user data sharing, the setback would probably be temporary. The California Privacy Rights Act, on the ballot this November as Proposition 24, explicitly turns "do not sell" into "do not sell or share." The law, which is expected to pass, wouldn't take effect until 2023, but it would eventually force businesses to honor the global privacy control.

This could finally make privacy a real right for internet users in California, and perhaps nationally, if Washington takes notice. It could also push companies away from business models based on microtargeted advertising. "What the law does is incentivize companies to find other ways to monetize, of which there are many," said Soltani. That, in turn, could help the floundering news industry, because advertisers who can't rely on cross-site tracking to target users will have more of an incentive

to go back to advertising in particular publications to reach their audiences.

Because of the data-sharing deals they have made with ad tech companies, “publishers are no longer the exclusive owners of their audience data,” said Robin Berjon, the vice president of data governance at *The New York Times.* That makes it harder to make money by building a loyal audience. The *Times* has signaled a shift toward targeting advertising based on its own first-party data from its readers, but very few publications have a large enough subscriber base to follow suit. Turning off the third-party advertising spigot unilaterally would be too risky. If users adopt the global privacy control en masse, however, they could conceivably solve that collective action problem and save publications from themselves. “In a market in which publications are competing with each other, if one of us decides to pull their data out, then that publisher will probably be penalized in the advertising market. But if users are the forcing function and say, ‘Hang on, you’re not selling my data anymore,’ then that applies to everyone equally.”

More broadly, widespread adoption of the global privacy control would take away the largest incentive businesses currently have to engage in extensive surveillance.

“Privacy, at its core, is about stopping the data collection that creates profiles about people,” said Gabriel Weinberg, the CEO of DuckDuckGo. “That’s used for advertising, but the byproduct of that is all the other privacy harms. Filter bubbles, discrimination in ads, misinformation: the stuff that has really started to rip up society comes through the same profiles.”

The global privacy control isn’t designed only with the CCPA in mind. The group behind it—which goes by the rather literal name of the Global Privacy Control group—believes the technology will be legally enforceable under other privacy regimes, including Europe’s Global Data Protection Regulation. And they hope to get the control recognized as a standard by the World Wide Web Consortium.

“The time is right to do this,” said Zimmeck. The American public cares much more about privacy than during the failed Do Not Track effort, and now there is finally law on their side. But the law can’t accomplish anything on its own. “I think it’s really important to not just theoretically talk about how this could work,” Zimmeck said, “but also to actually do it.”