

OCTOBER 2022

PRIVACY DAWN

WHAT'S AT STAKE WITH OUR DATA
AND HOW IT'S BEING PROTECTED

BY JUSTIN KLOCZKO

Consumer
Watchdog

Table of Contents

Introduction	2
Findings	4
What is At Stake	7
Federal Preemption	10
How the CCPA Protects Your Personal Information	16
A Closer Look: Reproductive Rights	19
How CCPA Regulations Can be Stronger	21
Conclusion	23

Introduction

Our personal data is sold hundreds of times a day and worth hundreds of billions of dollars¹, but if regulations for California’s strongest-in-the-nation privacy law are drawn correctly, consumers will get unprecedented control over their personal information beginning in just a few months.

In 2020, California voters passed the California Privacy Rights Act (CPRA), the strongest data privacy protections in America. The CPRA is an expansion of the California Consumer Privacy Act passed by lawmakers in 2018.

Set to take effect in 2023, CPRA gives consumers unprecedented control over their data—the ability to prevent any information from being shared with third parties, prohibit the use by anyone of their most sensitive data, and to narrow how data is used.

CPRA sets in stone a guaranteed minimum for privacy protections and cannot be weakened by lawmakers **without the direct consent of California voters**. That means privacy in California can only grow more robust.

The most serious threat to those rights comes from Washington, D.C., where proposed legislation threatens to sacrifice Californians’ data privacy rights for a weaker federal law.

We live in a world where every click, tap and search is scrutinized by companies and governments to know more about us than we know about ourselves. There is no privacy. Existing means having your personal data continuously shared or sold, like a real-time credit score, but worse. The result is a hall of mirrors of advertising, tracking and pre-selected choices. It’s like a game where the most intimate information about you is sold to the shadiest actors, and you have no control over it.

For example, there is a whole unseen current of automated decision-making happening all the time, where a black box algorithm is choosing what job, house, or

¹ [“How Much is Your Data Worth?”](#) Robin Bloor, Permission, April 6, 2020.

criminal sentence a person will receive. As of 2020, almost 80% of businesses are using data to make automated decisions².

The average U.S resident has their data auctioned off 750 times a day, according to the Irish Council for Civil Liberties³. That's double the amount of Europeans and more lucrative than Amazon sales. These auctions occur in nanoseconds. And that's data from advertising alone, which generates half a trillion dollars around the world. There is a major incentive to sell our sensitive personal information because the more specific it is, the more money a company is willing to pay for it.

Americans are coming to realize that their data has a lot of value, but most believe they have little control over their personal information⁴. However, we are now in the middle of an awakening regarding how privacy and data is viewed.

During the summer of 2022, the California agency tasked with implementing the new landmark privacy law, the California Privacy Protection Agency (CPPA), rolled out its first series of draft regulations. Californians' expansive new privacy rights take effect January 1, 2023 and address: dark patterns, expanded rules for service providers, third-party contracts, third-party notifications, requests to correct, opt-out preference signals, and data minimization. Cybersecurity audits, risk assessments, and automated decision-making will follow in the next round of rule-making. This report will spotlight these regulations, what works and what can be made better, and the federal attempt to overturn them.

² "The State of Decision Making Report 2021," Signal AI, June 8, 2021, <https://www.signal-ai.com/press/95-7-of-business-leaders-and-decision-makers-believe-using-ai-will-transform-how-decisions-are-made>

³ "The Biggest Data Breach," Irish Council for Civil Liberties, May 2, 2022. <https://www.iccl.ie/wp-content/uploads/2022/05/Mass-data-breach-of-Europe-and-US-data-1.pdf>

⁴ "[Americans and Privacy](#)," Pew Research Center, November 15, 2019.

Findings

Consumer Watchdog [analyzed the agency's draft regulations of the CCPA](#). The most important regulations empower consumers with the following new rights:

- **The ability to opt-out of data being shared with third parties.** Some companies argued that 2018's CCPA only prevented the 'sale' of data, not the data sharing that fuels the business model of many social media and advertising companies.
- **Businesses must display on their websites a “Do Not Share/Sell My Information” button and a new “Limit the Use of My Sensitive Personal Information” button on their home page.** Consumers will now be able to prevent the use of sensitive data by first parties, including: health, race and ethnicity, precise location, sexual preference, union membership, and religious beliefs.
- **More transparency:** businesses also must provide a list of categories of sensitive information collected, whether personal information is sold or shared, and the length of time the business intends to retain each category of personal information.
- **People can also use a single opt-out signal that every website and company must honor.** This enables people to notify websites of their privacy choices instead of individually opting out on each website.
- **Opt outs must be frictionless,** meaning they can't use deceiving language or logos to convince consumers to allow the sale of their data. “Dark Patterns,” or the deceiving ways in which businesses convince users to give up their privacy, are banned. In essence, a person's request to opt-out of sale/sharing should not contain more steps than a person's request to opt-in to the sale of personal information after having previously opted out.
- **The right to delete or correct inaccurate personal information a business has compiled,** and to notify third parties of requested changes. CPRA also expands deletion requests by mandating businesses notify third parties who have the data.
- **Data use needs to be proportionate to the purpose.** A company can't use data for a reason that's completely unrelated to the reason the consumer provided it. For example, a flashlight app cannot use your geolocation for its function.

- **Real accountability:** The CPPA can perform announced or unannounced audits of entities to check for CPPA non-compliance.

As a result of these regulations, California has the strongest data privacy laws in the country, paving the way for other states to pass their own laws, such as Colorado, Connecticut, Virginia and Utah. Over half of the 50 states have followed California’s lead and begun drafting privacy laws.

But California’s regulations can be stronger, by making it easy to choose privacy using a global opt-out signal, and requiring companies immediately honor a request to stop selling or sharing data. Consumer Watchdog has urged the agency to make such improvements.

Display Privacy Choices: The board should revert to its previous regulation stating that a consumer’s opt out choice be displayed. A business is not required to display on its website whether it has processed a consumer’s choice to opt-out of sale/sharing personal information, leaving people in the dark about whether they have exercised their privacy rights.

Identify Third Parties: Businesses should be required to identify third parties who collect personal information within a notice of collection. The privacy board has proposed to delete this requirement.

Making it Easy to Opt-Out: The proposed regulation says a business may provide the consumer with an option “to provide additional information.” The language could be interpreted as allowing companies to ask for a name and email frequently when someone opts out. Unnecessary hurdles in the opt-out process goes against the intent of the law. Consumers are likely to get fatigued if constantly asked to confirm their privacy choices. Businesses must not be allowed to make it difficult for consumers to exercise their global opt-out right if their global opt-out signal is on, or the “do not sell/share” button is enabled.

Immediately Honor Opt-Out of Sale/Sharing: Under the regulations, businesses have 15 days to honor a person’s request to stop selling or sharing data with third parties, as well as 15 days to limit use and disclosure of sensitive personal

*“Over half of the
50 states have
followed
California’s lead
and begun
drafting privacy
laws.”*

information. This is a massive window that threatens to upend the intent of the entire law. Even when someone opts out, personal information will still be sold because businesses are granted a two-week grace period. Businesses should be forced to honor a person's opt-out request just as soon as they are able to sell your data, which privacy experts say is mere seconds. This gap should be eliminated.



Artists' rendering of the nonstop auction of personal data. (*Consumer Watchdog*)

What is At Stake

The old saying goes, “If the product is free, then you are the product.” Companies like Google, Facebook and Twitter that allow us to use their products without charge are okay with that because they make tremendous amounts of money off personal data. We are now only beginning to realize the value of that.

An American’s personal data is estimated to be worth between \$2,000 to \$3,000 per year⁵. Data privacy company LetAlone says Facebook earns up to \$900 per user annually selling personal information to companies⁶.

“Data is power,” said Albert Fox Cahn, a lawyer and executive director of the Surveillance Technology Oversight Project (STOP), a pro-privacy group. “Data is harnessed by police to track us, jail us, and enforce any law on the books, increasingly bans on abortion. And so in a world where abortion is a crime, digital search technologies will be one of the main tools for enforcement.”

Data mining is a creepy, cynical business. On a commercial level, it directly feeds into the advertising-industrial complex that exploded in the 20th century, which since inception preyed on people’s insecurities to sell products. Today’s version is on steroids thanks to reams and reams of personal data available to companies to analyze. Because businesses now have super specific data about us, it is used to make us feel like something is missing, so you have to spend money to feel better.

“The more you know about a person, the more likely you are to win the auction for their ad impression,” said Dan Frechtling, who runs Boltive, a company that monitors dark signals. “Partnering with others, synching profiles, skirting the rules, and layering more and more personal data gives an edge,” he said.

Once data gets into other hands, it goes everywhere and is nearly impossible to know who has it. We know about Facebook and Google, but it’s the less known data miners that must be watched. An app like Uber may sell your location data to a data collection company, which then contracts with another company, or government agency. A location data company called SafeGraph collected information on those who went to abortion clinics and put it up for sale on the

⁵ [“How Much is Your Data Worth?”](#) Robin Bloor, Permission, April 6, 2020.

⁶ [“This is how much money Facebook earns from your data each year.”](#) Jim Martin, Tech Advisor, Jan. 28, 2022.



Life-sized cutouts of Facebook CEO Mark Zuckerberg wearing 'Fix Fakebook' t-shirts are displayed by advocacy group, Avaaz, on the South East Lawn of the Capitol on Capitol Hill in Washington, Tuesday, April 10, 2018, ahead of Zuckerberg's appearance before a Senate Judiciary and Commerce Committees joint hearing. (AP Photo/Carolyn Kaster)

open market⁷. That information could have been purchased by anyone, including anti-abortion vigilante groups or police. Purchasing data is one way governments circumvent the constitutional protections that require them to seek judicial approval through warrants before they violate our Fourth Amendment rights against unreasonable searches.

“It’s not so much the technology has changed. The times have changed,” said Sebastian Zimmeck, an assistant professor of Computer Science at Wesleyan University. Zimmeck helped develop the Global Privacy Control, a way for consumers to universally signal their privacy preferences instead of individually opting out on each website. The law has finally caught up to this idea. In California, businesses must honor a global opt-out. “The technology is ready to go,” said Zimmeck.

⁷ [“Data Broker is Selling Data Location of People of Visit Abortion Clinics.”](#) Joseph Cox, *Vice*, May 3, 2022.

It's not just the battle for reproductive rights that will be in danger. Communities of color, low-income workers, the undocumented, the LGBTQ community, and marginalized people everywhere will be disparately impacted by data getting into the hands of government.

U.S. Customs and Border Patrol has weaponized personal data to devastating effect⁸. Palantir, the largest data analytics company in the world, has contracted with the Department of Homeland Security to conduct immigration raids⁹. And fears about government tracking of immigrants has led to a decrease in use of services from food stamps to health care¹⁰. Other branches of the government, such as the FBI and DEA, have contracted with the data broker Venntel, which purchases data from another, Mobilewalla, that covertly monitored the location and identity of almost 17,000 people who assembled during the Black Lives Matter protests in 2020¹¹.

The CCPA allows Californians to opt out of this location surveillance, limit data use, as well as opt out of data sharing, including when companies contract with government contractors like Palantir, Safegraph and Venntel.

But then there is the specter of federal preemption...

⁸ [“Ice is Buying Up Massive Troves of Location Data...For Some Reason.”](#) Nikki McCann Ramirez, *Rolling Stone*, July 18, 2022.

⁹ [“The war inside Palantir.”](#) Doug MacMillan, *The Washington Post*, August 22, 2019,

¹⁰ [“Fears about government tracking of immigrants has led to a decrease in use of services from food stamps to health care.”](#) Helena Bottemiller Evich, *Politico*, Nov. 14, 2018.

¹¹ [“How Cellphone Data Collected for Advertising Landed at U.S. Government Agencies.”](#) Byron Tau, *The Wall Street Journal*, Nov. 18, 2021.

Federal Preemption

One of the biggest threats to privacy rights ironically comes from recently proposed federal privacy legislation, the American Data Privacy and Protection Act, which would preempt the CCPA as well as many other state privacy laws in California and across the country. The legislation is awaiting action on the floor of the House of Representatives after passing the Energy and Commerce Committee on July 20th.

But preemption is a false choice. State and federal laws do not have to be binary. Strong federal privacy laws already co-exist with stronger state privacy laws. Many other federal laws, like the Clean Air Act, set a federal floor, not ceiling.

For example, the Gramm-Leach-Bliley Act (GLB) and the Health Insurance Portability and Accountability Act (HIPAA) both established national policy “floors” and let states enact more privacy-protective legislation. Thanks to GLB’s policy floor, not ceiling, the CPRA built on it to give Californians stronger financial privacy protections. For banks that could mean, for example, any personal information collected and inferences made about a consumer as they consider a bank but before they sign up for financial services. Preemption will supersede the progress of states like California who wish to improve on the laws put in place federally.

The federal law is not as stringent as the CCPA, and it would remain vulnerable to weakening by industry lobbyists, do little to stop government surveillance, and swiftly cancel years of progress California has made on privacy.

There's one reason the tech industry likes the federal law: They don't want to comply with California's stronger protections. Once Congress locks in a law we may not see movement again on the issue for decades.

According to an analysis by Consumer Watchdog, Californians would lose the following rights because of federal preemption:

- **California law protects against government surveillance.**

Governments and law enforcement agencies are using data brokers to avoid obtaining warrants for location and other information about Americans. California’s law applies to companies who contract with the

government, allowing people to opt-out of data collection and stop their sensitive information from getting into the hands of the government. A major loophole in the ADPPA allows companies who contract with a local, state or federal government for data collection to avoid compliance with the law. That means unfettered access by governments to mass data collection by tech companies like Google as long as they have a contract.

- **California’s law cannot be weakened – except by Congress.**

CPRPA sets in stone a guaranteed minimum for privacy protections and cannot be weakened by the legislature *without the direct consent of California voters*. That means privacy rights in California can only get stronger – unless Congress decides to preempt the law. ADPPA would replace California’s floor with a federal ceiling that stops states from enacting stronger protections. No matter how strong a federal law is, industry lobbyists will seek to weaken or even eliminate it with future legislation.

- **Californians who are protected now would face a 2+ year delay.**

CCPA is already in effect, and 2020 amendments making the bill even more protective of sensitive data like race, sexual orientation and location will be implemented in less than three months. ADPPA overrides those rules and will put privacy on hold for at least two years as the Federal Trade Commission writes regulations. And delay is denial.

- **Audits and enforcement.**

Because rulemaking would still have to occur under the FTC pursuant to the federal law, which has ambiguous or timelines that take years, companies will very likely not comply with the federal law in the meantime. They will argue that enforcement is premature because the rules aren’t on the books yet. It will likely take three to four years for the FTC to draw up regulations. In the meantime, Californians will lose out on rights it already has.

The California Privacy Protection Agency can audit companies’ compliance with the law. The ADPPA would allow companies to only self-audit. While amendments to ADPPA nominally allow California to enforce the law, the Agency cites “significant uncertainties” in its ability to do so. State enforcement matters because, while the FTC receives no new enforcement funding, the California Agency has a guaranteed \$10 million annual budget.

- **More protection against coercive pricing.**

California's law has stronger protections when a company imposes differential pricing on consumers who exercise their privacy rights. It prohibits such charges from being "unjust, unreasonable, coercive or usurious" and requires companies to prove a different price for those who choose privacy is "reasonably related to the value provided to the business by the consumer's data." ADDPA would override these provisions.

- **Direct opt-out of discriminatory profiling and automated decision-making.**

California's law creates a right to opt-out of profiling and automated decision-making, allowing consumers to prevent discrimination in access to jobs, housing, loans, etc. that occurs when biased algorithms go to work and ignore civil rights. This broad opt-out from automated decision-making is in some ways more protective than the ADPPA's bar on racial discrimination, because the ADPPA relies on companies to decide if their algorithms are biased. California's law will allow consumers to simply say, "don't profile me at all."

- **Broader right to delete data.**


California allows consumers to view and delete all of the data a company has collected about them since the law was enacted. Data deletion is limited to a two-year look-back in the ADPPA.

- **A private right of action.**

Federal preemption takes away California's ability to create a stronger private right of action. The ADPPA only appears to give people rights in court, when in reality it's a mechanism to transfer power to a state attorney general or the Federal Trade Commission, which has not been a strong enforcer for decades. The ADPPA effectively leaves us without enforcement rights.

The FTC can block state action, and someone with a potential lawsuit would have to notify a state attorney general, who doesn't have to take on a lawsuit. And depending on the political winds at the time, a presidential administration not prioritizing privacy laws could simply sit on these lawsuits. We will not be allowed our day in court.

In addition, virtually all such cases would be litigated in federal court, which has been on a conservative tilt for decades. Plaintiffs would not see any compensatory damages or injunctive relief, whereas under the CCPA, plaintiffs are entitled to statutory damages. Statutory damages are a strong deterrent for companies to violate the law, but they are not a remedy under the proposed federal privacy law. The ADPPA also blesses forced arbitration, eliminating the court system as an option for resolution.



*Federal
preemption takes
away
California's
ability to create
a stronger
private right of
action.*

American Data Privacy and Protection Act compared to California Consumer Privacy Act

	ADPPA	CCPA/CPRA
Amendments	Congress can weaken the law at any time.	CPRA ballot initiative can only be amended to make privacy laws stronger. Legislature cannot go below a floor of protections.
Government Surveillance	A data collection company selling information, including geolocation, to a government agency does not have to comply with the law. Loophole emboldens government surveillance.	Entities contracted with governments aren't exempt from the law, so they must comply with consumer privacy choices just like any other business - protecting geolocation and other data from governments.
Enforcement	ADPPA would be enforced by the FTC, with no additional funding set aside. States California Privacy Protection Agency can also enforce, but Agency cites "significant uncertainties" in its ability to do so. No audit authority.	California Privacy Protection Agency has \$10 million annually in dedicated funding to enforce CPRA. Agency can seek civil penalties under state law, but not under ADPPA. Audit authority of businesses and third-parties to ensure compliance.
Implementation	It will take two years for the FTC to write rules to implement many provisions of ADPPA.	40 million Americans already have strong privacy protections from 2018's CCPA. CPRA's strengthened protections take effect in less than 6 months.
Civil Rights & Profiling	Explicit ban on discrimination that bars not only intentional bias but also disparate impacts. However, companies test themselves for compliance. No opt-out of automated decision-making or profiling.	Consumers can opt-out of automated decision-making and profiling, allowing consumers to prevent discrimination in access to jobs, housing, loans, etc. that occurs when biased algorithms go to work and ignore civil rights.
Right to Access, Correct, Delete Data	Consumers can access, correct or delete their data dating back just two years.	CCPA allows user to access, correct and delete all data back to Jan. 1, 2020. In 10 years, users can see all their data, versus only 2 years under ADPPA.
Global opt-out	Companies must honor global privacy signal as a consumer's opt-out choice. Allows businesses to impose an authentication ¹⁴ requirement before honoring.	Mandatory for businesses to accept an opt-out preference signal as a user's expression of their privacy choice. Companies must honor signal without authentication.

<p>Financial entities</p>	<p>Does not stop banks or lenders from being data brokers because of FTC carve out.</p>	<p>Applies to any data collected by banks and other financial companies that is not account information, for example data collected on a bank website about your geolocation, internet browsing, or purchases.</p>
<p>Retaliation</p>	<p>A business can charge someone more, or offer different service levels, for exercising their privacy rights. Ex: AT&T will provide high-speed internet in exchange for your browser history.</p>	<p>A business can charge someone more, or offer different service levels, for exercising their privacy rights. However financial incentives can't be "unjust, unreasonable, coercive, or usurious in nature." Requires different price to be "reasonably related to the value provided to the business by the consumer's data."</p>
<p>Unique Identifiers</p>	<p>Covered data "may include" unique identifiers such as IP addresses. Language is not absolute.</p>	<p>CCPA is stronger on unique identifiers. If it "is reasonably capable of being associated with a particular consumer or household," it's covered data that can be protected.</p>
<p>Private Right of Action</p>	<p>Individuals can sue for violations of many protections - including sensitive data violations, pay-for-privacy, and child protections, but others like bias prohibitions are excluded. Right to sue severely undermined by limits: Government must be notified and can take over a case; companies have a right to cure; companies may force dispute into mandatory arbitration; unspecified statutory damages; no mandatory attorney fees; four-year delayed implementation.</p>	<p>Lawsuits can only be brought over data breaches. Right to sue is strong: Statutory damages of \$100-\$175 per violation; consumer need not show harm; no right to cure; attorney fees mandatory; no government right to take over case; in effect today. Not preempted by ADPPA.</p>
<p>Dark Patterns</p>	<p>Obtaining consent in misleading or manipulative ways is barred.</p>	<p>Obtaining consent in misleading or manipulative ways is barred. Identifies specific ways to obtain consent that are not manipulative.</p>

How the CCPA Protects Your Personal Information

What the CCPA mainly does is rein in rampant abuse of our personal data by third parties. And a major protection bars companies from sharing personal data with government agencies without user authorization. Additionally, under data minimization requirements, companies who get your data directly can only use it for certain narrow purposes.

Under California's law, any resident who exercised their opt-out choice is protected from a government's extra-judicial purchase of their private information, or the ability of any company to sell or share your data.

The first round of regulations under the CPRA brought clarity in the area of global opt-out, and what exactly is considered a dark pattern:

- The ability to opt-out of data not only being sold, but being shared. Previously under the CCPA, entities could not sell data, but businesses argued they could share it and still be compliant with the law. In response to the passage of the CCPA, Facebook [contended](#) that sharing did not constitute a sale, and did not change its web tracking practice. Now Facebook can't make that argument after the CPRA amendment. Businesses now must display on their websites a "Do Not Share/Sell My Information" button and "Limit the Use of My Sensitive Personal Information" button on their home page. The homepage button is crucial for informing consumers who are not aware of their privacy rights.
- A new category of sensitive personal information, which includes any piece of information that can be linked back to you, or creates a profile of your likes and characteristics. This could include your name, email, purchases, search history, or more broadly, inferences made to determine your political leanings, sexual orientation, class and overall identity.

For entities that do collect personal information to perform a service, that entity cannot use it for any other reason than for the stated purpose. For example, websites often require too much information for simply signing up for a mailing list. Under CPRA's data minimization principles, an entity could not ask for a date of birth or address to complete a request to receive an

email. Or geolocation by a trucking company may be placed on a truck driver's route, but only during working hours.

- The right to correct inaccurate information or delete any personal information collected by a business.
- A global privacy preference signal, which is a way for people to notify websites of their privacy choices instead of individually opting out on each website, must be accepted by businesses as a viable opt-out function. The global opt-out is critical to make privacy choices as seamless as possible for those who already know they want to exercise their rights. Requiring global privacy signals be honored by businesses is an easy, fluid way for consumers to notify all businesses of their privacy preferences.



A woman carries a fire extinguisher past the logo for Google in Shanghai.(AP Photo/Ng Han Guan)

That many advertising and tech industry firms who see our data as a pot of gold have come out against a global opt-out, including the California Retailer's Association and the California Chamber of Commerce, says something about the importance of such mechanism for consumers. The chamber, which includes among its members major

personal data recipients Google, Amazon and Facebook, insurance companies State Farm and Allstate, and big banks Wells Fargo and JP Morgan Chase, said, incorrectly, "a global opt-out is voluntary under the California Privacy Rights Act." Following statements from the California Attorney General's office and the draft regulations, it is now clear that a global opt-out must be accepted by businesses.

- Opt-outs must be frictionless, meaning they can't use deceiving language, logos or sounds. If it isn't, then it's classified under the regs as "dark patterns," e.i the deceiving ways in which businesses lull users into collecting personal

information. We see these everywhere. When an “X” is so small it’s impossible to not click on the ad, redirecting you to the ad’s website. A “Sign Me Up” button that is larger than the opt out button. Cookies are another good example. It’s often easy to accept cookies, but opting out requires multiple steps. Under CCPA, users should be given equal or “symmetrical choices, such as “yes” and “no.” For example, users faced with the choices “Yes” and “Ask me later” is a dark pattern.

- Data use needs to be proportionate to the purpose a consumer provided it for. The regulations require data collection and use by any business—including a business collecting data through the infotainment system in cars—be proportionate to the purpose. For example, under section 7002, a flashlight app on a person’s phone should not collect geolocation without that person’s consent because an average person would not expect the app to have to know geolocation for the function of the flashlight.

Likewise, a car company that knows your location for emergency services such as a car accident should not use geolocation for purposes unrelated to safety. In light of car companies collecting reams of personal data such as geolocation and other information, the regulations will stop companies from using or selling that data beyond a “legitimate operational use.” The regulations on use limits ensure drivers can protect their data.

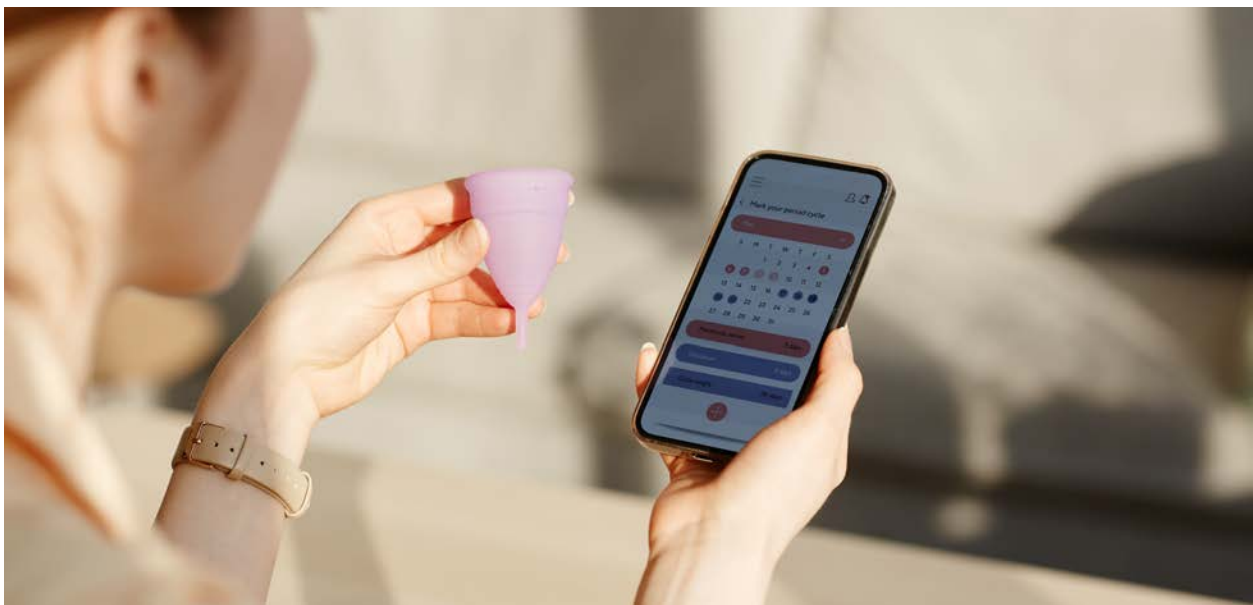
More simply put, consumers will have the right to not be tracked if they want to just drive their car.

- More transparency: businesses also must provide a list of categories of sensitive information collected, whether personal information is sold or shared, the length of time the business intends to retain each category of personal information.

A Closer Look: Reproductive Rights

The CCPA helps those wishing to better protect their reproductive choices. Years ago, Target developed a pregnancy predictor based on people's browsing and purchasing habits. If items such as non-scented lotion, certain vitamins, or even certain clothing colors were purchased, it triggered Target to send to the customer baby coupons for items like strollers or formula. In one incident, a young women's father discovered his daughter was pregnant before she told him.

This type of targeted advertising is common now, but under the CCPA a person could tell Target to delete the personal information it has collected about them to stop this sort of surveillance advertising. A user can also tell companies to stop profiling them.



Apps tracking menstrual cycles also pose a risk to those seeking or having abortions. These apps collect medication usage, period cycles, and geolocation. This personal information is not protected by health laws and could be subpoenaed as part of a criminal probe prosecuting abortion seekers. Imagine simply forgetting to input menstrual data, which could be indicative of an abortion or miscarriage. How do you defend that? The popular app Flo settled a case with the government after it was discovered to share fertility data with Facebook and Google¹². But under a law

¹² [“Flo Gets Slap For Sharing User Data When it Promised Privacy.”](#) TechCrunch, Natasha Lomas, Jan. 13, 2021.

like the CPRA, a user of the app can limit use of the data or stop altogether third parties from obtaining it.

A location data company called SafeGraph collected information on those who go to abortion clinics and put it up for sale on the open market. Including people who merely attend an abortion clinic unfairly implicates a large group of people. That information could have been purchased by anyone, including anti-abortion vigilante groups or police. SafeGraph collected such geolocation information from other sources, but under CPRA, users could opt out of geolocation because it is considered sensitive personal information.

Inferences, or what details can be made from a dataset, also are regulated by CPRA. If a woman is filmed or photographed at or near an abortion clinic, that data cannot disclose that she is having an abortion. Similarly, if a data inference is, “So and so doctor is performing abortions,” that data cannot be disclosed. That’s because a photo, image or a video is considered protected sensitive personal information under the CCPA. Under the proposed federal privacy law, the ADPPA, a photo, video or image is not considered protected personal information. So the person getting an abortion, or say, attending a police protest, would be exposed to harassment or prosecution because entities could get their hands on that data.

For example, a woman from an anti-choice state such as Texas comes to California seeking an abortion. She searches on her phone for reproductive health centers, consults her local physician, gets assistance from a trusted person, then proceeds to secure care. Local police could flag the woman’s search traffic for abortion clinics, track travel purchases, and use location tracking to follow her to the clinic. That data could be used as evidence for criminal prosecution of her or her local friend.

California’s law does a better job at protecting data from the government than the federal proposal, whose government data service provider loophole would leave vulnerable an unconscionable amount of sensitive data on the open market.

A California resident who travels outside of the state has some CCPA protections. For example, a California doctor who performed an abortion for a woman from another state would have his or her personal information protected, even shielding the doctor from potential criminal prosecution if he or she went to the patient’s anti-choice state.

How CCPA Regulations Can be Stronger

There is concern that businesses will make it difficult for consumers to exercise their global opt-out right, and create a loop of opt-out requests that will fatigue people. Under the proposed regulation Section 7025, it says, “a business may provide the consumer with an option to provide additional information if it will help facilitate the consumer’s request to opt- out of sale/sharing.” This opens the door to a lot of friction in the form of pop-ups asking for more information or worse service, which goes against the intent of the law.

For example, companies may still ask for information even if “do not sell/share” is enabled. The law could be interpreted as allowing companies to ask for a name and email frequently, and consumers will get fatigued for being punished for exercising privacy rights. The ability for a business to have the so-called “last say” in this exchange over data sharing should be simply eliminated. Indeed, the Agency’s regulations state, *“The path for a consumer to exercise a more privacy-protective option shall not be longer than the path to exercise a less privacy-protective option.”*

Under Sections 7026 and 7027, businesses have 15 days to honor a person’s request to stop selling or sharing data with third parties, as well as 15 days to limit use and disclosure of sensitive personal information. This is a massive window that threatens to upend the intent of the entire law. And the regulation is not backed up by the statutory language. The problem is once people’s data is acquired it is usually sold by businesses right away, oftentimes in seconds. Once data gets out into the world, it can get into anyone’s hands. Even when someone opts out, personal information will still be sold because businesses are granted a two-week grace period. It will also spur companies to concentrate on using and selling data within the window, producing a Wild West effect on data selling. And even though it says a business should honor a request “as soon as feasibly possible,” a business will cite 15 days as “soon as feasibly possible.” Businesses should be forced to honor a person’s opt-out request just as soon as they are able to sell your data, which apparently is mere seconds. This gap should be closed.

Additionally, the privacy board has made some last-minute proposed changes to the regulations that are not beneficial to consumers.

For example, a business is not required to display whether it has processed a consumer’s choice to opt-out of sale/sharing personal information, leaving people in the dark about whether they have exercised their privacy rights. The privacy

board proposed to delete the display requirement during its final rule-making period. But this simple notification will protect consumers from going through additional opt-out steps if they are unsure their rights have been honored. It will also enable consumers to flag websites for enforcement by the CPPA if those rights are not honored.

Further, businesses should be required to identify third parties who collect personal information within its notice of collection, but the privacy board proposed to delete this requirement. Consumers deserve to know who exactly will be handling their personal information when exercising their rights.

Conclusion

As is usually the case with policy, California leads the way, and data privacy is no different. The CCPA is elemental because it addresses the abuse of our private information. It is the best law yet to shield our data from companies and government agencies who use it for less-than-ideal means. Now consumers can opt out of data selling and sharing, stop being tracked, have a right to know what's being collected about them, and can correct or delete such information. Multiple states are now looking to pass their own privacy laws, whereas just a few years ago California was an outlier in the fight.

But the fight doesn't end here. The privacy regulations look great on paper, but all eyes will be on the state attorney general's office and the California Privacy Protection Agency to see how enforcement will be carried out. Federal preemption will continue to be the biggest threat to California's privacy rights, and must be addressed. As people come to understand that data has become a valuable extension of themselves, they can now take back what is theirs, empowered by laws like the California Consumer Privacy Act.

