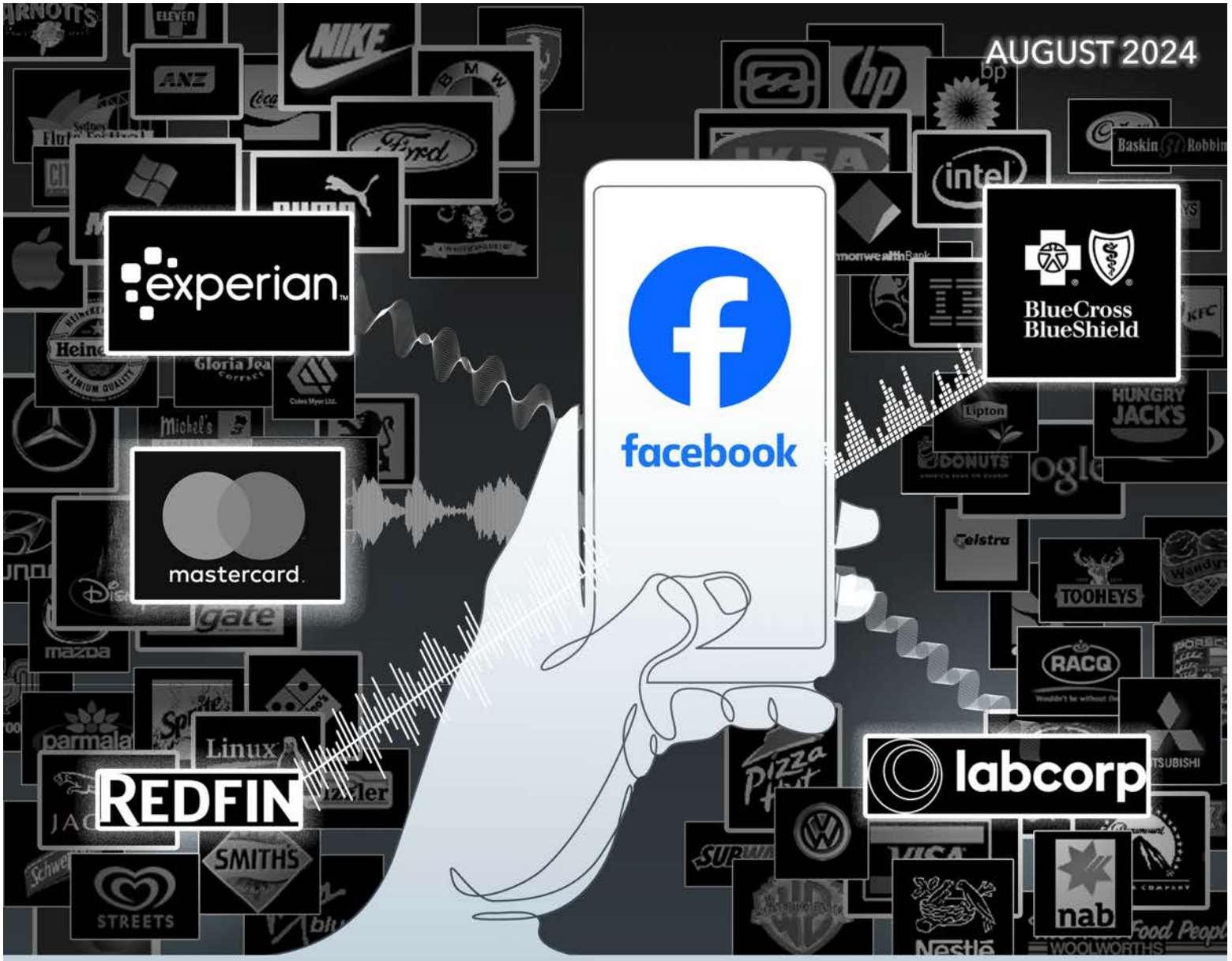


NO OPT OUT

WITH THOUSANDS OF COMPANIES SELLING YOUR DATA, THERE IS NO EASY WAY TO EXERCISE PRIVACY RIGHTS. BUT HELP IS ON THE WAY.

BY JUSTIN KLOCZKO

Consumer Watchdog

Table of Contents

Executive Summary

Even with strong laws in place in California, there is no easy way to opt out of our personal data being collected, used and shared by companies. For the average person, it means filling out thousands of forms and time no one wants to spend.

That's because the same tech companies that collect large amounts of data also own the most popular web browsers—Chrome (Google), Safari (Apple) and Edge (Microsoft). And they don't let us tell businesses all our privacy choices in one step because it's not in their financial interest to do so. Although businesses must accept a global opt out under the California Consumer Privacy Act (CCPA), most browsers don't offer such a signal unless a plug-in is installed. Even then, not all browsers accept it.

When I tried to take control of my data on Facebook, for example, I discovered how time-consuming and confusing opting out can be. I learned Facebook knows about over 2,500 companies that I've visited online, including my credit card company and health insurer, according to nearly 20 years' worth of data since I opened my Facebook account. The list also contains major data brokers like Experian and Live Ramp that I didn't interact with directly. Data brokers keep a low profile but traffic in our most personal details such as our eating, travel, purchasing, gaming, viewing and listening habits.

"Most Californians are worried about their personal data being shared or sold. But the problem is people don't understand what they can do about it".

And despite deactivating my Facebook account for a year, meaning my account was not visible to other accounts, the sharing between Facebook and companies I visited continued. According to the data, Facebook and advertisers still knew about 671 businesses I interacted with online, including my health insurer, credit card company, and bank[1].

If I want to put a stop to this data sharing, I must navigate a confusing, seemingly endless labyrinth of privacy options obscured in legalese. I must choose separate

[1]"Facebook fuels broad privacy debate by tracking non-users," David Ingram, Reuters, April 15, 2018..

options to correct or delete information collected by Facebook, disconnect activity sent to Facebook by outside websites, or put an end to sharing of data about me between Facebook advertisers. And that means time spent going individually through thousands of businesses, a tedious undertaking designed to fatigue people from exercising their options in the guise of Facebook being a privacy-friendly company. Separately, it's not even clear that Facebook is complying with the CCPA, the data protection law that is in effect right now because even though Facebook says it does not share or sell your data, advertisers still pay for access to it.

The good news is there is pending state legislation to overcome this barrier, as well as pending regulations that will make exercising privacy rights easier for Californians. A "global" opt-out preference signal automatically tells businesses your privacy choices in one collective swoop, such as opting-out of the sale/sharing of personal information, and its use for targeted advertising.

If passed and signed by the governor, California Assembly Bill 3048 (Lowenthal), will allow Californians to opt out in one step by requiring browsers to offer the signal. And in 2026, Californians will be able to tell data brokers, who collect data from other parties, to delete all personal information in one step, thanks to an amendment to the CCPA called the Delete Act, or Senate Bill 362 (Becker) that was approved last year.

The average person using the Internet spends almost seven hours a day in front of a screen[2]. That's 17 years spent checking the Internet beginning at age 18 until the age of 80. We check our phones on average of 144 times a day[3]. This generates a lot of data. People are surveilled as they book doctor appointments, shop for food, and dial suicide hotlines[4]. Our every search, scroll and tap is monitored and monetized. Unfathomable amounts of data—64 zettabytes, or 6.4 trillion gigabytes —float around in a sea of mystery[5]. Each person has about 3,000 data points[6]. And based on that data algorithms and artificial intelligence are deciding jobs, health

---

[2] "Digital 2024: Global Overview Report," Simon Kemp, Data Reportal, Jan. 31, 2024.

[3] "Cell Phone Usage Statistics," Alex Kerai, Reviews.org, July 21, 2023.

[4] "Suicide hotline shares data with for-profit spinoff, raising ethical questions," Alexandra Levine, Politico, Jan. 27, 2022.

[5] The world generated 64.2 zettabytes of data last year, but where did it all go?" Channellife, March 26, 2021.

[6] "Privacy is essential to human flourishing," Laurie Clark, The Guardian, Oct. 2, 2022.

care, finances, down to the very way we receive information. There has never been a greater need for a universal opt-out.

Using Facebook as an example, what follows is a guide to navigating how one can learn about the extent of data sharing, how to opt out, and how help is on the way —if we fight for it.

Facebook, a Case Study

It is very difficult to extricate oneself from Facebook. It's more than a social media company. It's a news, advertising, and business platform. It owns Whatsapp and Instagram. The company makes it easier to log into other accounts by allowing access through a personal Facebook account. According to the Federal Trade Commission, Facebook is a monopoly and the agency sued Facebook for "illegally maintaining its personal social networking monopoly through a years-long course of anticompetitive conduct." It has its tentacles in lots of things. And one of the things it has a monopoly on is data.

(AP Photo/Carolyn Kaster)

How It Works

Facebook directly collects information a person enters into Facebook, such as profile details, as well as activity and interactions on the platform. Facebook gets your data on things you've "liked," ads clicked, content you create, or places you've checked into. Your age, location and gender is tracked. Your every move is scrutinized.

"Your every move is scrutinized."

Facebook also keeps tabs on a person's online life through cookies, ad trackers, pixels, and "Like" buttons that are placed on other websites. As a result, Facebook knows what you searched for, purchased, donated, or added to a shopping cart. This helps fuel targeted advertising, an industry that generates billions of dollars by preying on our attention spans[7]. When Facebook and businesses get your data, it is used to expose you and other people to more ads, which leads to more spending. For Facebook, data generates 99 percent of its revenue[8].

According to an analysis of all the data Facebook stores on my account going back nearly 20 years, Facebook knows a total of 2,423 businesses I interacted with, whom it shares with other businesses, who then used it to reach other similar profiles. A majority of them I don't recognize. These are advertising firms and data brokers who operate in the shadows. And the entities that I do know are concerning. They include my health insurer, the real estate listing company Redfin, my credit card company, Labcorp, which does bloodwork, and the state of California. Popular data brokers also used my information from a list of advertisers, including Experian and Acxiom, which sell data on geolocation and minors, according to a data broker registry maintained by the state of California[9].

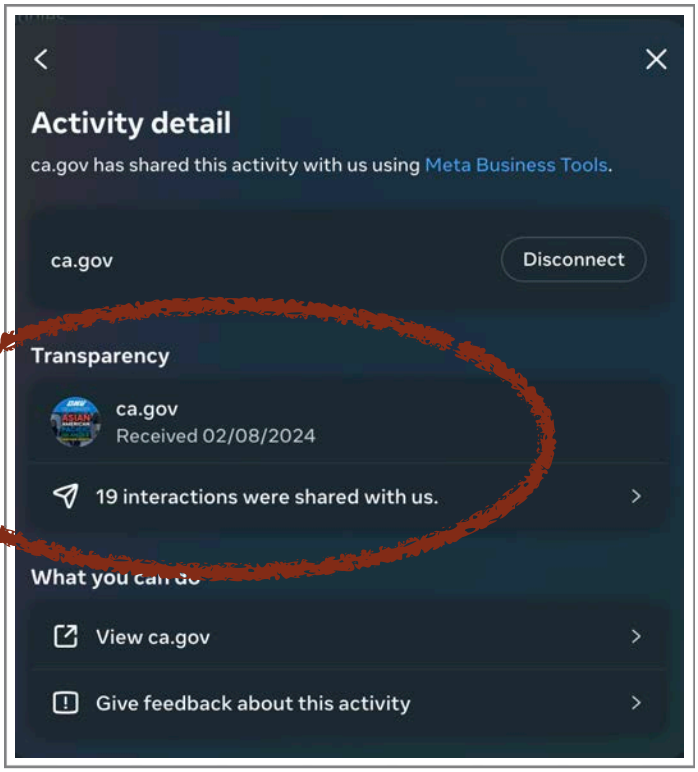
---

[7] Shadowy data brokers make the most off their invisibility cloak," David Lazarus, Los Angeles Times, Nov. 5, 2019.

[8] Targeted Advertising Statistics By Countries, Companies and Platforms, Barry Elad, EnterpriseAppsToday, Aug. 21, 2023.

[9] State of California Data Broker Registry, 2024

For example, Ca.gov shared with Facebook 19 interactions I had with the website[10]:



Nineteen interactions on a state of California website were shared with Facebook.

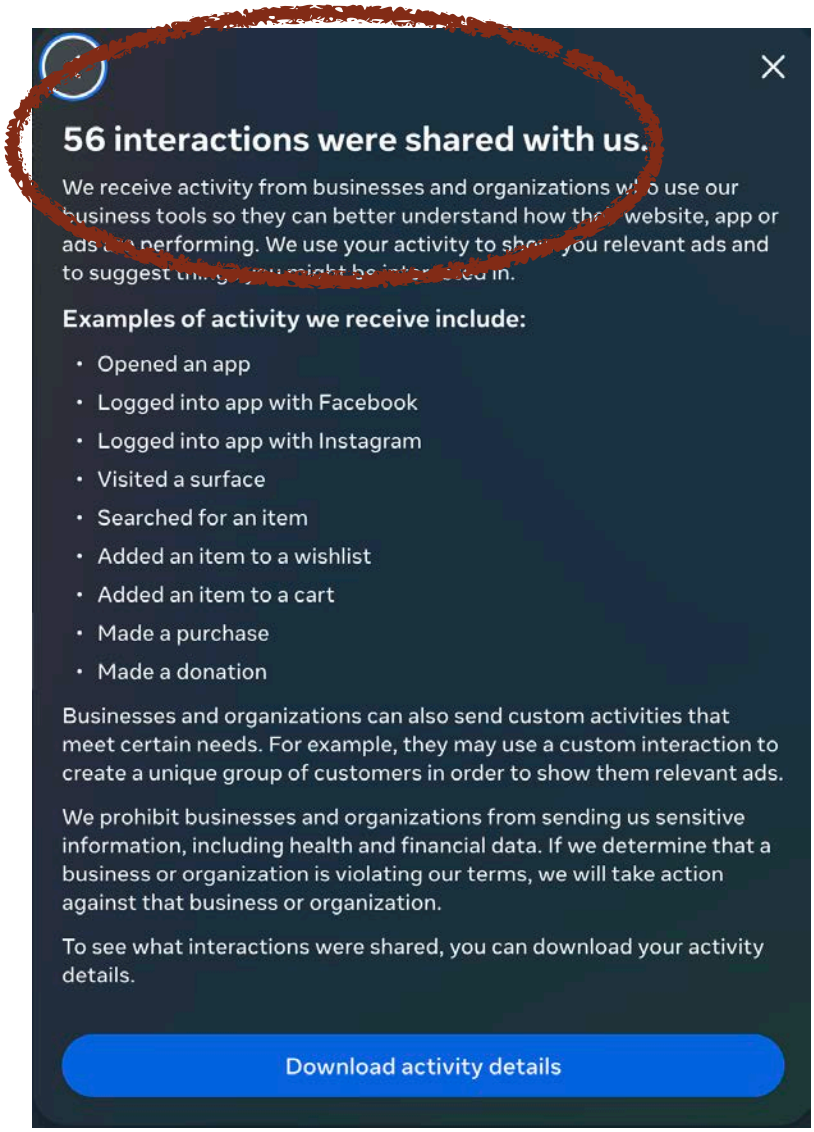
But the data is not a complete list:

"We receive more details and activity than what appears here," states Facebook. "For technical and accuracy reasons, this list doesn't show all the activity that we've received. This includes information we've received when you're not logged into Facebook or Instagram and details such as the items you add to your shopping cart on other websites."

And despite deactivating my Facebook account for a year, meaning my account was not visible to other accounts, the sharing between Facebook and companies I visited continued. According to the data, Facebook and advertisers still knew about

[10] State of California Data Broker Registry, 2024

671 businesses I interacted with online, including my health insurer, credit card company, and bank[11].



An example of my activity on other websites that businesses shared with Facebook.

[11] "Facebook fuels broad privacy debate by tracking non-users," David Ingram, Reuters, April 15, 2018..

Facebook receives this data even if you aren't logged in or have deactivated your account. A person must disable their "Off-Facebook activity" or activity from ad partners before deactivating their account in order to stop the data collection and sharing.

Facebook is like an invasive parasite siphoning off your data for profit. This is the world we live in: thousands of mysterious companies always watching us.

"Facebook is like an invasive parasite siphoning off your data for profit."

Even when a person does everything possible to stop Facebook's data collection, severing the data pipeline between businesses and Facebook is never complete. The data only becomes anonymized. Even if you don't have a Facebook account, Facebook collects data on you. These shadow profiles are like accounts out of view and only seen by Facebook and other businesses.

When a person opts out, it merely unlinks a person's identifying characteristics from the data.

What Data is Used For

If you start seeing ads for baby products on Facebook, or a particular website, it's because you searched or bought similar items on another website, maybe prenatal vitamins or parenting books. If you also search for camping gear on another website, these data points are combined, and you might get ads for camping gear for children. That's targeted advertising.

A more specific, and increasingly ubiquitous kind of targeted advertising used by Facebook other companies is collaborative filtering. Collaborative filtering isn't just being shown content based on your personal data, but also data of others who have similar interests as you. By combining the information of like people, Facebook and advertisers can use information collected about certain groups to build predictions about their actions and interests in the future.

The algorithms of X, Spotify, and Netflix are popular examples of this. They keep you ensconced in an echo chamber.

A Google engineer described collaborative filtering this way: "The most successful recommendation systems are those that understand users and their preferences better than users understand themselves."[12]

So What Can Be Done About It?

Taking control of your personal information in an age where our identities exist mostly online is important, but it currently requires time most of us don't have. To see what data Facebook collects, stop businesses from sending data to Facebook, as well as to limit targeted advertising on Facebook, follow these steps:

Directly Collected Data

Facebook collects data that you enter into your profile, such as location, education and profession, as well as what you click on and who you interact with.

Access or download your Facebook information here. You could look at all of your Facebook history, such as which Facebook groups you joined, to whose profiles you visited, or what you searched for at any given time period.

However, it is not clear that Facebook is complying with the CCPA. While Facebook directs you to various "privacy rights," such as "deleting and correcting personal information" that were mandated under the CPRA, Facebook merely highlights the ability for people to edit or delete their profiles. It is not clear how one can act to limit, correct or delete personal information that Facebook *stores.*

Facebook also maintains that it does not share or sell personal information. While that is technically true, advertisers still pay for *access* to your data through Facebook without *directly buying it.* For example, if there's an ad for people who are getting ready to retire, the advertiser can tell that the people who clicked on the link are people Facebook thinks are retiring. And that's how something like an IP address, which identifies a person, can be collected via Facebook. Put another way, while Facebook might not outright give advertisers a list of people who are between the

[12] "Who Chooses What You Watch? You or Netflix?" Sean Thorne, The Drum, July 19, 2023.

ages of 60 and 65, Facebook will allow you to flash ads to them. That's how companies like Facebook get around sharing and selling your data[13].

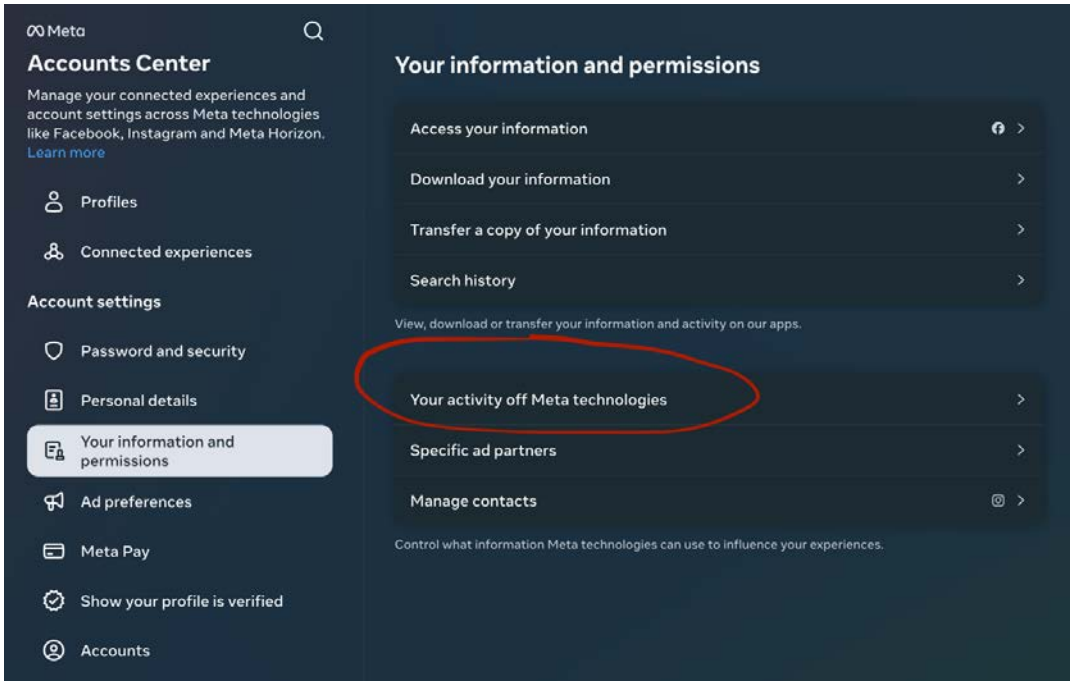
Off-Facebook Activity

Facebook users can go through lists of companies that have sent data to Facebook and stop the data sharing on an individual basis here.

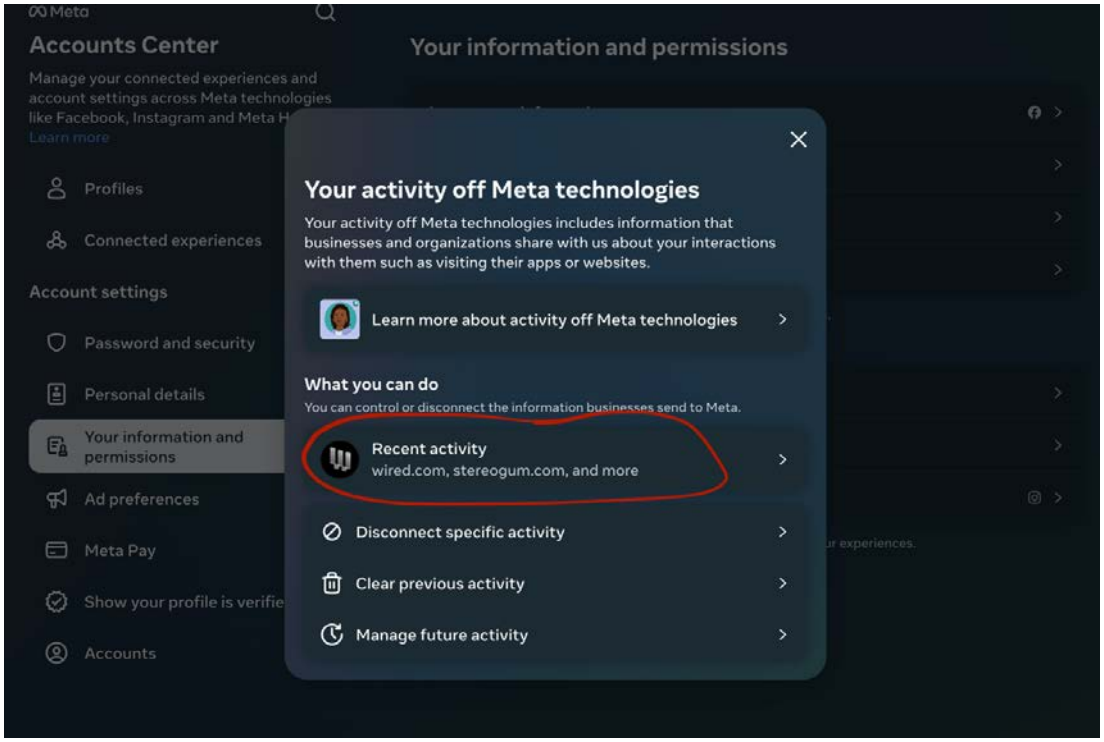
In order to disconnect specific data sharing, clear previous sharing, and manage future activity, go to "Your activity off Facebook technologies." By choosing "disconnect activity," entities will stop sharing data with Facebook the things you do on their websites, such as details about what sections you go to, for how long, as well as what you look up and purchase.

[13] "What Does it Actually Mean When a Company Says, 'We Do Not Sell Your Data?' Alfred Ng, The Markup, Sept. 2, 2021.

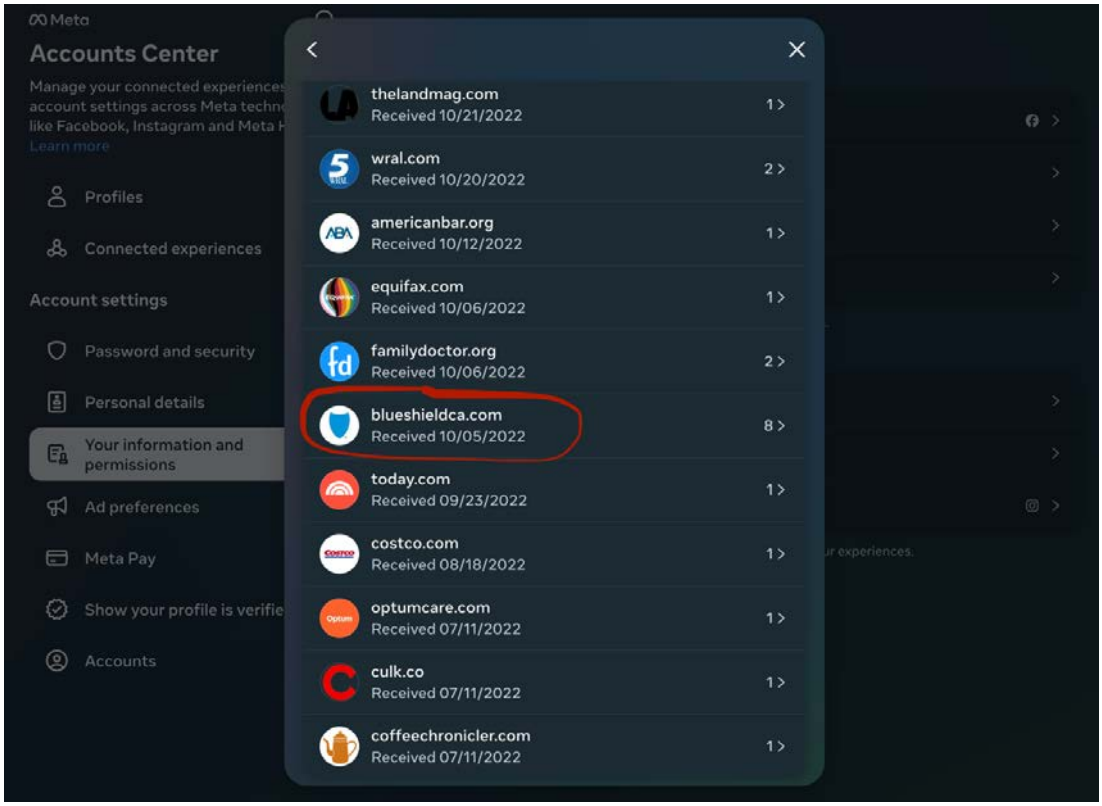
Follow these steps to disconnect:



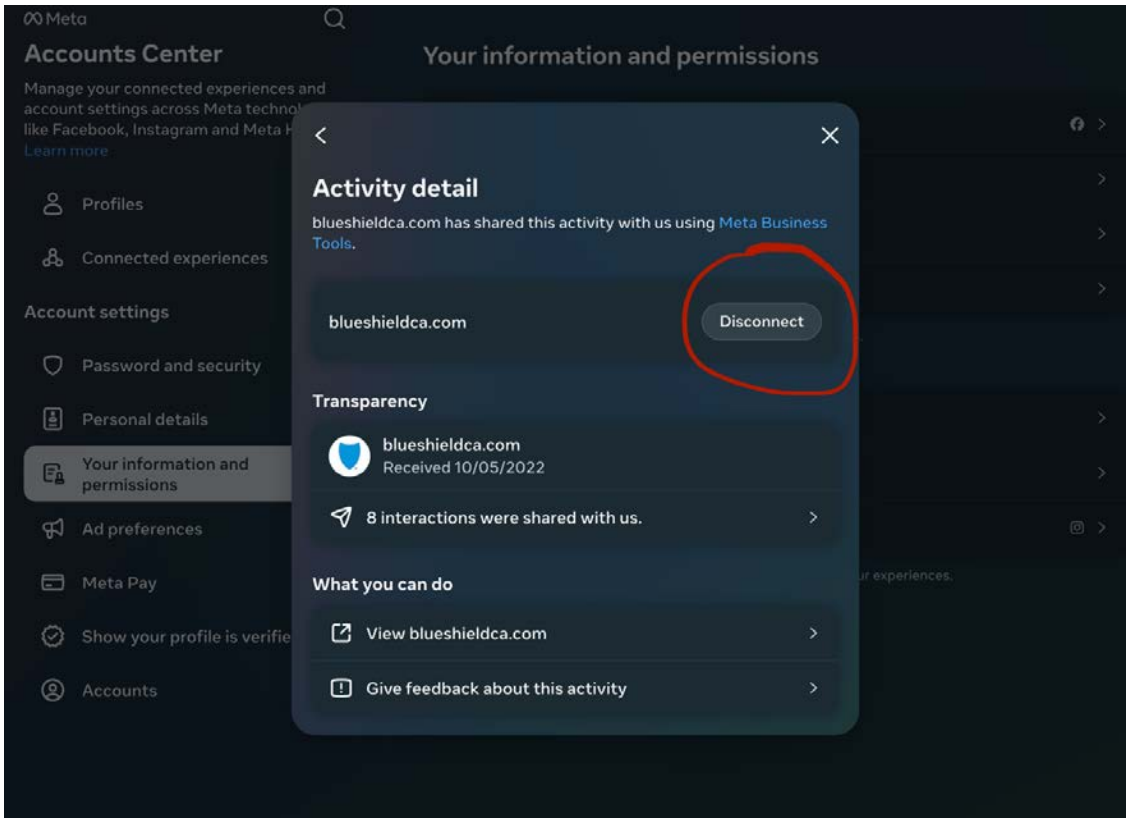
1) Click “Your Activity off Meta Technologies”



2) Click “Recent activity"



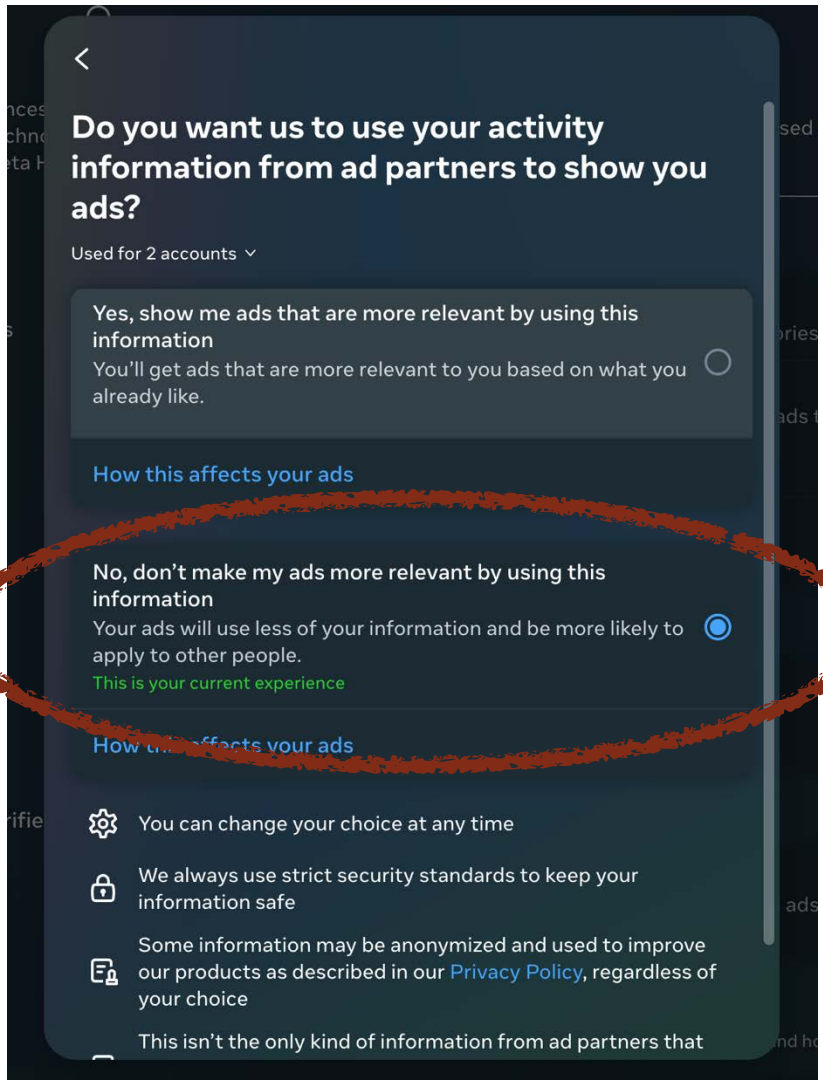
3) Select a business



4) Select “Disconnect”

Ad Partners

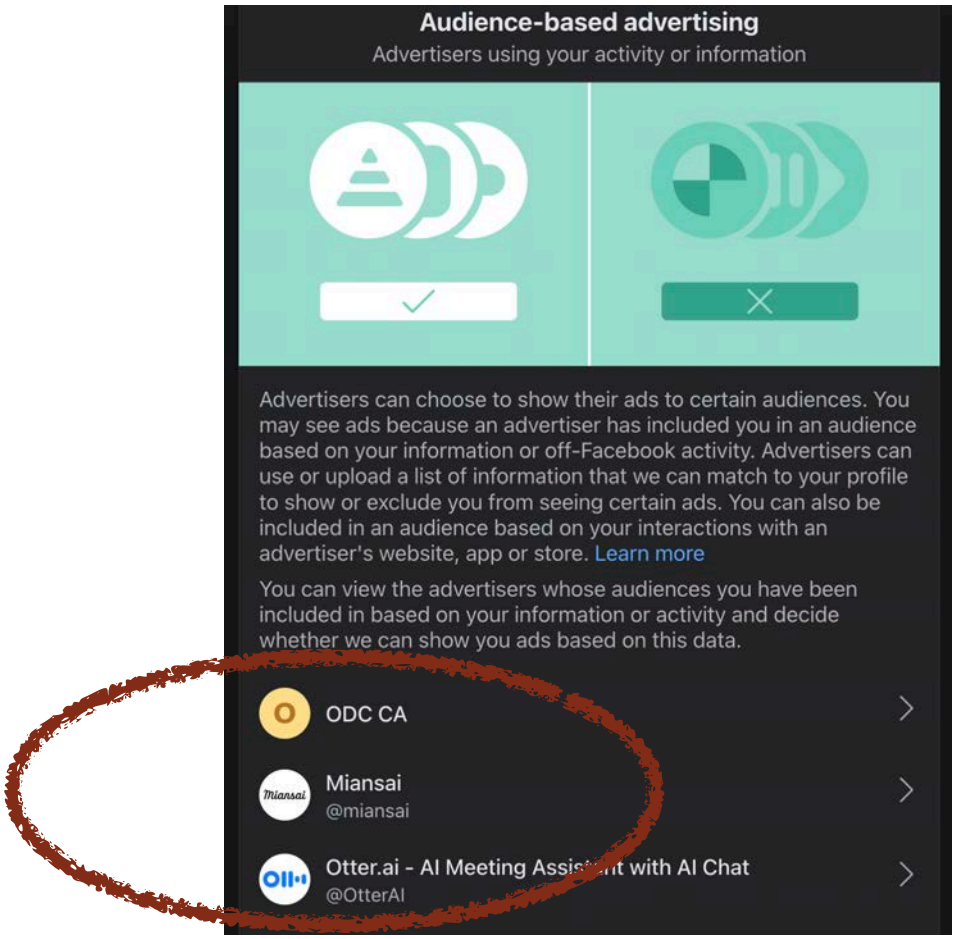
Stop activity from ad partners here. This makes your scrolling habits more private and helps minimize the information used for targeted advertising. Companies that advertise on Facebook send Facebook information such as the things you search when you visit their websites or apps in order to show content you're more likely to engage with. In order for Facebook to limit how your information used to show you ads, follow this step:



Stopping your activity from being used to target ads. Select "No."

Audience-Based Advertising

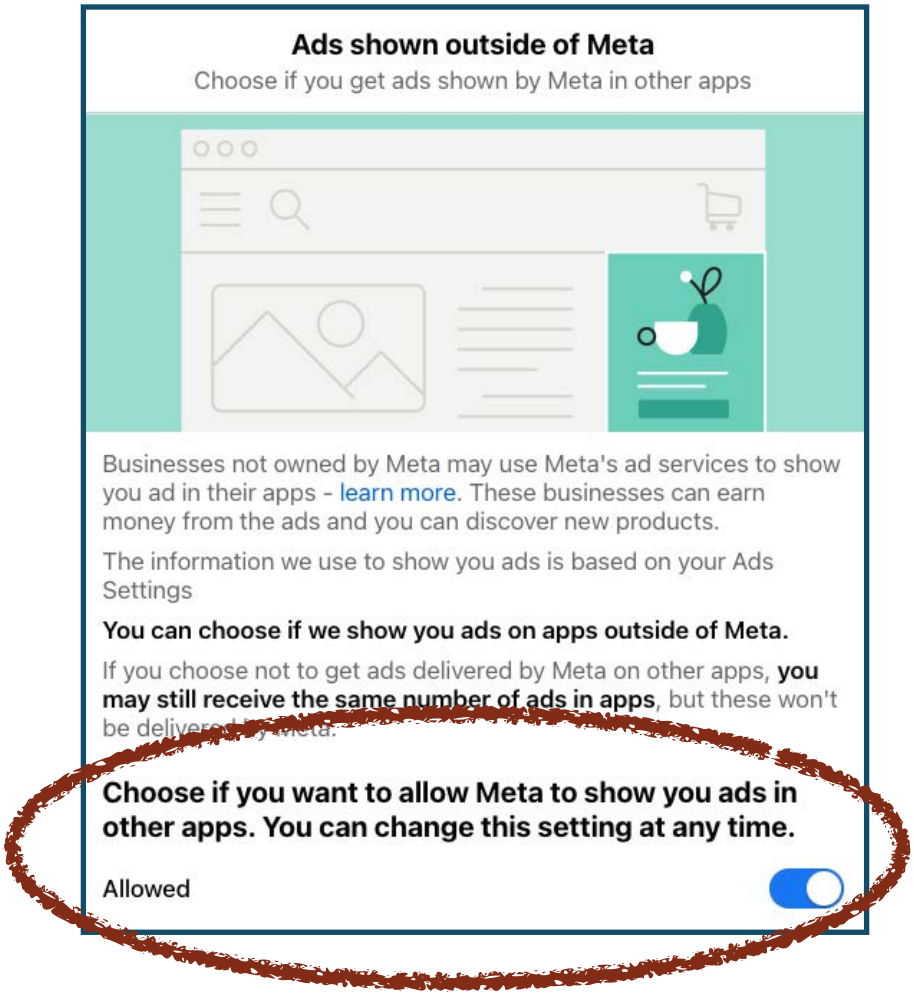
Another reason you might see certain ads on your Facebook feed is because an advertiser has included you in a list based on your data. Advertisers can use or upload a list of information that Facebook can match to your profile to show certain ads. To see which companies use this list based on your information, and to disconnect this feature, go here.



You can be removed from an advertiser list by selecting each business.

Ads Outside of Facebook

You can stop Facebook from showing you ads on other apps. Businesses not owned by Facebook might use ads delivered by Facebook to show you an ad. To stop this go here.



More Protections Are Coming

Facebook CEO Mark Zuckerberg said most Facebook users don't exercise their privacy options[14]. It's worth asking, why? Is it because people don't care about what happens to their data, or because it's not easy to control it? Evidence points to the latter, as most Californians are worried about their personal data being shared or

[14] Zuckerberg Congressional Testimony, 2018.

sold. But the problem is people don't understand what they can do about it, according to recent polling.[15]

It's too difficult to exercise those rights.

However, the public is catching up and our laws like the CCPA continue to evolve. There is rule-making happening by the California Privacy Protection Agency (CPPA), which is developing regulations for data brokers under the CCPA. On the other front, a number of legislative bills are attempting to expand upon the CCPA to give stronger rights to Californians. The CCPA is a unique law in that establishes a floor on privacy rights, but not a ceiling, so the law can continuously evolve, but it cannot be easily eroded.

Global Opt Out

Under the CCPA, businesses must allow for Californians to globally opt out of the sharing and selling of their personal information, but most browsers don't offer these signals. The top three browsers—Chrome, Safari and Edge—make up for nearly 90 percent of the browser market share and they do not allow users to express their data privacy preference signals in one step, leaving people clicking through a maze of privacy options that will surely end in user fatigue.

You can install a Global Privacy Control signal on certain browsers to tell websites to stop collecting and sharing data. This can be done in under a minute by downloading the Electronic Frontier Foundation's Privacy Badger, or DuckDuckGo Privacy Essentials.

But even that isn't a cure-all. Safari, which is the default browsers on iPhones, does not accept the signal, for example.

To install the Global Privacy Control for Chrome and Edge and to enable it on Mozilla Firefox, follow this guide.

However, if it passes out of the California legislature and is signed by the governor, California Assembly Bill 3048 (Lowenthal), will allow users to opt out of the sale of personal information directly collected by businesses in one step by mandating that browsers offer the signal. Without such a bill, Californians will be more likely to

[15] California Privacy Protection Agency, Polling, March 2024.

give up on exercising their privacy options if they have to opt out of the sharing, selling and use of their data on a business-by-business basis.

By having a mechanism by which to trigger a global opt out, the sharing and selling of data by companies to companies like Facebook can be stopped quicker and easier. For example, if Spotify is sharing or selling data on your podcast listening habits to a clothing company to target you for a Nirvana shirt, that transfer can be stopped.

The law also requires that the opt-out signal be easy for consumers to find and use, and gives power to the California privacy agency to adopt regulations surrounding the opt out, including updating the law to address technological changes.

Data Broker Delete Act

In 2026, Californians will be able to direct data brokers to delete all the information they've collected on a person thanks to the passage of the Delete Act (Becker). Before, data brokers under the CCPA were only required to delete data that was *directly* collected from an individual. Think of this law as the global opt out, but aimed toward data brokers. Californians will also be able to direct data brokers to:

- Correct personal information
- Learn what personal information is being collected and shared
- Opt out of personal information being collected, sold and shared
- Limit the use and disclosure of sensitive personal information

Beginning this year, data brokers have to register with the California privacy agency, informing the public if they collect data on geolocation, minors or health care, as well as providing information on how to delete or correct, or opt out of personal information that is collected or shared. Those brokers who do not register with the state face penalties of $200 per day, and $200 per deletion request if they don't comply with the request. Those data brokers that send information to Facebook? You will be able to direct all of them at once to delete your personal information.

Conclusion: Threats On All Sides

Data privacy rights are under attack from different sectors of industry, from tech to advertising to Wall Street, who hide behind front groups you've probably never even heard of to give off the appearance of a plurality of opposition. But in the end, it's the same tech monopolies behind the curtain who want to protect their bottom lines: Google, Amazon and Facebook. These tech companies have waged battles in the courts and through federal legislation that would override the privacy rights of states with stronger laws.

The California privacy agency is a small agency tasked with regulating a personal data market that is worth billions of dollars. So far it's withstood major opposition and influence from industry groups in the form of lawsuits, lobbying and rule-making. The California Chamber of Commerce, whose members include Facebook, sought to invalidate newly enacted draft CPRA regulations by bringing a lawsuit that it ultimately lost.

Those companies have also spread disinformation about the nature of privacy rights enshrined by the new law while pushing for a weaker federal law that would preempt California's more stringent data protections. Tech front groups like the California Retailers Association and TechNet have also said a global opt out is "voluntary[16]" under the CPRA, something that was put to bed by the California Attorney General's office, who said the preference signal "must be honored[17]."

It's no surprise the very companies that stand to benefit most from the profiting and sharing of our personal data are also the companies fighting to stop laws such as the CPRA. These rights are important, but they need to be more well-known and user-friendly if we wish to avoid a scenario where people give up their rights because exercising them turns into a game of Whac-A-Mole.

Soon, a total merger of tech, advertising and commerce will ensconce consumers in a virtual buying universe, as companies like Disney and Amazon seek to sell products people see in shows and movies as seamlessly as possible[18].

---

[16] CPRA Rulemaking Comments.

[17] Enforcement Update CA Attorney General, July 19, 2021.

[18] "Disney Debuts Future of Entertainment and Advertising at 5th Annual Tech & Data Showcase at CES," Jan. 11, 2024.

"Soon, viewers can discover and explore products as they watch by sending products they see in films and TV straight to their second screen with Shop the Stream," unveiled Disney this year.

This is a near future we need to work to stop, and that work starts now.