OPTING OUT

NOTICE AND CONSENT

What gives Data Brokers and businesses like Facebook the right to collect our data?

According them, we do.

Our privacy regulatory model is based on the concept of "**notice and consent**." In other words, a business can do whatever it wants with your data if it provides notice to you about what it's going to do, obtains your consent to do so.

In reality, "notice" is often buried in the **Terms of Service (ToS)** on an app or website, and though most companies have a **Privacy Policy**, they are usually so vague that they don't really explain what the business will do with your data, or they're worded in such a way that they don't really restrict the business from doing anything with your data. Our failure to read these agreements is not due to laziness. One study found that if the average internet user were to read every privacy policy they consented to, it would take 76 workdays to complete all the reading!

Once you are showed the voluminous reading, you may be asked to click a button to say "I accept." If you don't you cannot use the app or website, and if you do, you have agreed to give up the rights to your data. If every website has similar terms, your option is to consent or stop using the internet. You might wonder if you're really "consenting" when you don't know what you're consenting to and you don't have real choice. Unfortunately, the law seems to believe that this consent is valid.

Some privacy advocates have suggested we move to an "**opt in**" model whereby if a business wants to share your data, they must clearly and explicitly ask you for permission. This permission is sometimes referred to as **express informed consent**.

One place where express informed consent is the norm is at health care facilities, which are covered by the **Health Insurance Portability and Accountability Act (HIPAA)**. A doctor must get your consent in writing to share your health information with any parties outside certain ones that are necessary to provide you health care. Another example of express informed consent involves websites and apps that cater to children, where the parents must provide

verifiable consent before the business can collect, use or disclose personal information from their kids. This is due to the **Children's Online Privacy Protection Act (COPPA)**.

Where a business is using your data without express informed consent, they might argue that you can always **opt out** of information sharing. Not all businesses let you opt out, and the ones that do often make it inconvenient to do so. But even where consumers have the option, very few people tend to take advantage of the ability to opt out.

One way to opt out of information collection is through your browser and browser settings, the apps and online services you choose to use and their privacy settings, and your device privacy settings.

Here we explain some additional ways that you can opt out of information sharing. Many of these can also be found on the FTC's website on opting out.

HOW TO OPT OUT

FINANCIAL INSTITUTIONS

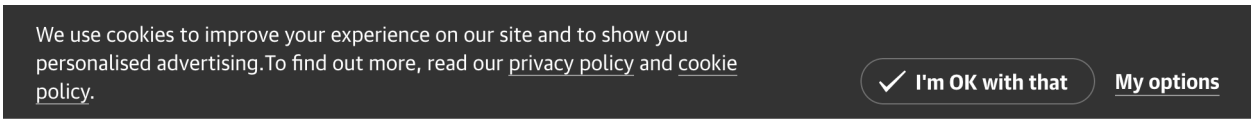
Banks and other financial institutions are required to provide you with an annual **privacy notice** under the federal **Gramm-Leach-Bliley Act of 1999**. This notice gives you information about what data sharing practices you can and cannot opt out of, and instructions on how to do so. You can also find privacy settings under your profile or account settings and potentially choose to opt out of the sharing of some data.

SCHOOL

Any school or university which receives federal funding is required to comply with the **Family Educational Rights and Privacy Act of 1974 (FERPA)**. Under FERPA, you (if you're over 18) or your parents have the right to inspect and correct the educational records that the school has about you. The school must also get written permission from you to release information from your education record – this requirement has *many* exceptions, but it's something.

COOKIES

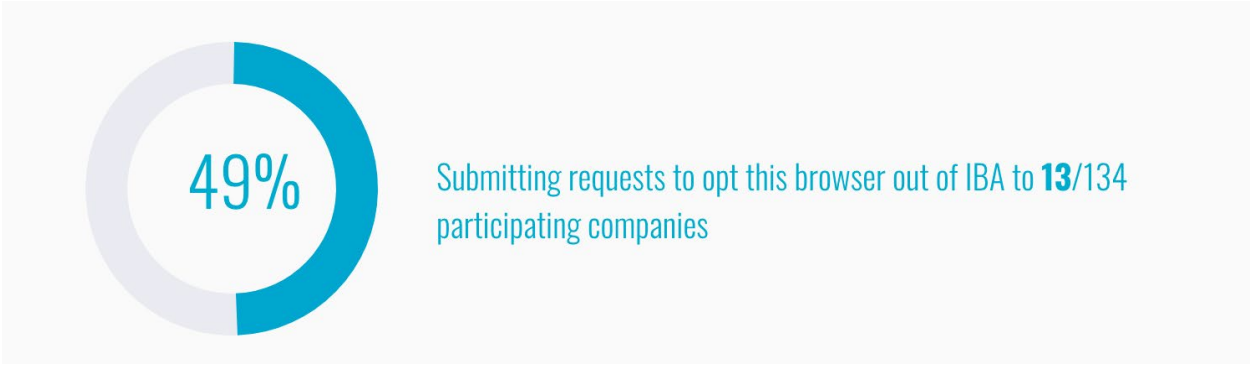
You may have noticed that a lot of websites now show you a window where you can manage your cookies when you arrive at the site. This is likely due to new regulations put in place in Europe called the **General Data Privacy Regulation (GDPR)**.



When you see one of these windows, you can click on the options and opt out of certain kinds of cookies, like those relating to targeted advertising.

TARGETED ADVERTISING

You may have never noticed, but many online advertisements have a little symbol of an "I" in a triangle. This is the symbol for a self-regulatory campaign by the advertising industry (the National Advertising Initiative) called "AdChoices." If you click on the triangle you should be redirected to a site that lets you manage your targeted advertising choices called YourAdChoices.com. It is website has a tool that will show you many advertising companies that are tracking you and offer you the option of opting out of Internet Based Advertising (IBA) from them.



The website also offers an "AppChoices" app that you can download onto your phone to presumably control App-based advertising. You can also opt out by going to optout.networkadvertising.org.

DATA BROKERS

Many data brokers claim to offer you the option of opting out of their data collection or sale of data about you. Assuming that these companies are true to their word, you can follow procedures on their websites to opt out. One problem is *finding* the data brokers to figure out how to opt out. In 2018, Vermont implemented the country's first Data Broker Registry, where all data brokers collecting Vermont resident data must register and provide information about how to opt out. In 2020, California is implementing its own version of the registry.

Some websites list the data brokers and where to go to request optouts like StopDataMining.me and JoinDeleteMe.com. This can be very time consuming, so subscription-based services offer to contact data brokers on your behalf and opt you out. Two such services are DeleteMe or Privacy Duck.

DIRECT MARKETING (MAIL & PHONE)

If you don't want to receive direct mail (aka junk mail), a service which is heavily reliant on acquiring your data from data brokers, you can opt out through the Data Marketing Association's website.

If you don't want to receive telephone calls from telemarketers, you can add your number to the national Do Not Call registry at DoNotCall.gov. Note that while many legitimate companies do comply with the Do Not Call list, the recent influx of unsolicited robocalls and scam calls shows that many are ignoring it. They are, however, breaking the law.

CREDIT REPORTS

Whenever you take out a loan, request a new credit card, apply for a job, or rent an apartment, the bank or landlord or whomever will want to look at your credit report. This is a report issued by a credit reporting agency (Equifax, Experian, TransUnion, or Innovis) that basically says (or at least tries to guess) whether you can reliably handle money and pay your bills on time. The safest way to stop identity theft by people who want to open accounts in your name is to **freeze your credit reports** – this means no one can request a report on you (and therefore open an account) unless you personally unfreeze (or "thaw") the account. You can learn how to freeze your credit reports at the FTC's website.

In addition, credit card issues will often send you unsolicited offers of credit. It's generally a good practice to only open a credit card when you need one, on your own terms, and to ignore these solicitations. You can stop them by going to OptOutPrescreen.com.

SPAM EMAIL

Does your inbox get filled with marketing emails? Under a federal law called The Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (CAN-SPAM), businesses must put information into marketing emails about how to opt out of receiving them. If you scroll to the bottom of the email you should see a link called "Unsubscribe" or "Manage my Email Preferences." Following this link will let you unsubscribe from the emails. It can take a few days for the company to unsubscribe you during which you will still receive messages.

If you don't see the link, or a business doesn't unsubscribe you when asked, you can report them to the FTC. The current penalty for violations is $42,530 per individual email!

CALIFORNIA CONSUMER PRIVACY ACT

In 2018, California passed a major new law called the **California Consumer Privacy Act (CCPA)** which went into effect in 2020. The CCPA only applies to businesses of a certain size or that collect certain amounts of data. The CCPA also only affects California residents, but other states may be passing their own versions soon. Also, some companies might just decide that it is simpler to apply the CCPA's protections to all of their customers. Some of the new rights that the CCPA provides include:

- Websites must have a prominent "**Do Not Sell My Personal Information**" button or link.
- Consumers can request that a business **stop selling** their data.
- Businesses must inform consumers of the categories of information they collect, and the purposes for which the categories will be used.
- Consumers can **request a copy** of the specific data that the business has collected about them.
- Consumers can request that a business **delete** all of the data that the business collected from them.