A Complete Guide to Internet Privacy

figleaf

Table of Contents

Your privacy, your choice

Privacy should be a choice. But right now, our choices are limited to agree and accept or not—a binary yes/no, all-or-nothing scenario that just is not functional in today's digital world.

That's because every digital action comes with a digital payment: your personal information.

Sometimes, this can be useful. Personalized recommendations—created thanks to your data—can help narrow down your selections when shopping online. They can be used to deliver better search results.

But sometimes that data is used in ways that maybe you don't want it to be. Every individual should be able to choose specifically what gets shared, how, with whom or what, and the duration of that sharing. Full transparency of data use is the linchpin of a healthy digital society.

To understand digital privacy, you need to know what's at stake.

The data economy

For years, an enormous global data industry has been built without the majority of consumers realizing that their personal information is its foundation.

The basis of many a tech company's business is data, what's been termed "surveillance capitalism." Gathering this data is legal (for the most part), although not always obvious. And it encompasses almost everything anyone does online, from logins to clicking on an ad link to even seemingly innocuous activities like mindlessly streaming music. Every click, ISP, country, duration, search query result, signup, login, image, language, language translation, web history...the list goes on. Metadata is, basically, data about data; it's the details about your digital actions. Metadata gets captured as well. Although personal data can be anonymized, researchers have shown that, in fact, data doesn't stay anonymous for long.

That information gets traded and passed from one site to another. An example is how a certain social networking site that had a major motion picture made about its founding gathered information from people, even if they didn't have an account with said platform, and sold that to advertisers. That included facial recognition biometrics and placing invisible codes that tracked users around the web. So not only did individuals not give permission for this to be done, but they don't know how that information is being used and by whom or what entity.

In the U.S., as in many other countries, the standard is opt-out—meaning an individual is automatically sharing their data unless they explicitly select not to.

Collecting personal data has become the standard—as opposed to personal privacy protections—mostly because, simply put, these companies could. As the technology to collect and store and sift through data became both cheaper and better, that data collection increased but without any accompanying rules or legislation (for the most part) to act on behalf of the individual. In the U.S., as in many other countries, the standard is opt-out—meaning an individual is automatically sharing their data unless they explicitly select not to. Of course, as many can attest, opting out is rarely a simple matter. (Also, do you have a spare 250 hours a year to read Terms of Service agreements?) The other standard, opt-in, puts the onus on the company to ask for users' permissions first. Or you could try to live without using these services. Good luck with that.

What about regulations?

After many examples that vividly demonstrated how personal information is being used, there have been recent steps to turn this data Titanic around.

The most lauded or despised—depending on your point of view—is the EU's implementation of GDPR in the spring of 2018. The GDPR is actually an update to pre-existing privacy laws. But the general idea is this: Individuals have control over their data, including the ability to withdraw it, and companies that do not comply with any aspect of GDPR receive hefty fines. There are also stricter rules about gaining consent to collect and use data.

In the U.S., one of the problems is the patchwork of state regulations when tech knows no borders. The California Consumer Privacy Act of 2018 is the closest the U.S. has to GDPR-level rules. In the past, regulations in California have set the standard for the rest of the country (e.g., automobiles), so there's a possibility other states will follow suit. Vermont passed a law in late 2018 to regulate data brokers. Even some industry bigwigs are calling for privacy laws, including Apple's Tim Cook.

Where’s my data?

Every single action online on any device captures data. That includes just carrying a device with you as you go about your day.

Online data collecting has been happening since the 1990s, right when the internet was becoming accessible to the average person, thanks to the World Wide Web.

Personal data travels in many ways. There are various forms of trackers—software that “travels” with you from one site to another—with various levels of invasiveness. Browsers capture data, websites capture data, internet service providers capture data, search engines capture data… you get the idea.

Then there’s the data you give up when you agree to a site’s rules, which could only be considered truly voluntary if those rules were clear and comprehensive. Which they often aren’t. Social media accounts, for example, collect data to both ensure that you’re not doing things counter to its terms of service agreement, and also to create a user profile.

The collected data is linked to a personal profile, and that’s gold to advertisers, whether they’re hawking the latest sneakers or working on behalf of a political group.

Data brokers are companies that trade in this data. It’s a big business, and, in the U.S., mostly unregulated. They can provide personal information—like home addresses, phone numbers, and birthdates—for marketing by creating demographic categories and for “risk mitigation,” amongst other purposes. (Data brokers also collect off-line info, like public records).

Social media accounts, for example, collect data to both ensure that you’re not doing things counter to its terms of service agreement, and also to create a user profile.

Who controls your data?

(probably not you)

Maybe you don’t care if advertisers know you prefer a particular brand of sneaker. But do you care if they know every one of your credit card charges? Your health information? Information about your children?

There is a range of actions you can take to protect your data. The simplest include VPNs, password managers, 2FA, VCCs, privacy-oriented search engines, and a Tor Browser.

VPN (virtual private network) A VPN is a service that masks your identity and location by sending your web traffic through a series of its own servers.

Password manager A password manager is a service that will create and keep your passwords, and often other site information, like answers to security questions.

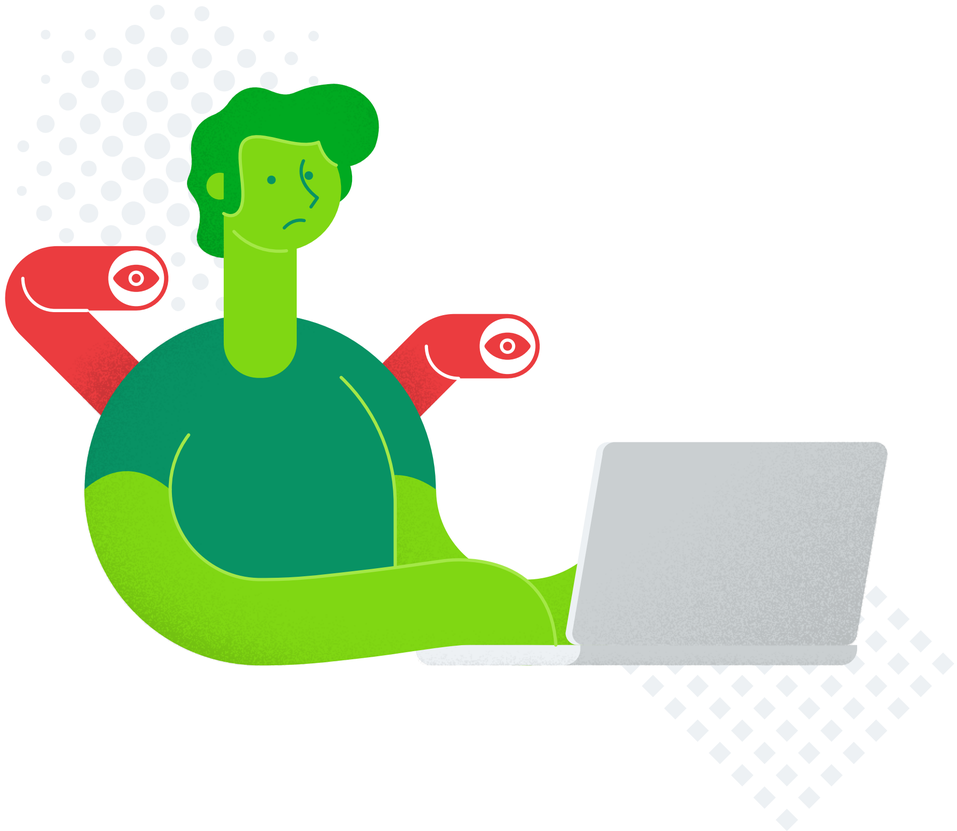
2FA (two-factor authentication) 2FA comprises a second security step. The most common is a numerical code sent via SMS to a cellphone.

VCCs (virtual credit cards) VCCs were developed to add security to online financial transactions. A VCC is a single-use number that looks like a regular credit card number but expires after a transaction so it can’t be stolen or tracked.

Privacy search There are several search engines available that promise not to log personal data. Two of those are DuckDuckGo and Startpage.

Tor Browser For big privacy aficionados, Tor Browser runs on the Tor network—Tor stands for “The Onion Router,” so-named because of the many, many layers it uses to maintain users’ anonymity.

Privacy plug-ins There are plenty of privacy plug-ins for browsers that track when you’re being tracked, block trackers, etc.



But none of these solutions is a complete answer to digital privacy. Some VPNs are routinely rejected by websites, which will mean making it through many security tests (storefronts of the world, anyone?) or complete site blocks. Password managers are not infallible and have themselves been hacked. Two-factor authentication is not completely secure because SMS and phones aren't completely secure. Tor Browsers can be extremely slow or outright blocked or banned. Privacy plug-ins don't always live up to their promises and can be confusing.

The reality is that lacking any substantial federal legislation (and perhaps even if that does come to pass), managing personal digital privacy will soon become another task, just like managing personal finances and going for regular dental checkups. Maybe not your idea of a good time, but necessary.

The move to data privacy

Consumers are now more aware than ever of how their data is being collected and used, and are speaking out about their lack of privacy rights. They're realizing that their data is being used in ways with the potential to influence their choices in life, and not just in terms of a targeted sneaker advertisement, but for much bigger—and more serious—decisions.

And that's what digital privacy comes down to: choice. The choice to share, or not, our digital lives in the way we see fit. To live our lives as we choose.

Responding to this demand are companies that want to put the power of privacy in the hands of individuals—where it should be.

The rise of choice

Frankly, today's digital business model is not designed to benefit consumers above corporations. While we're seeing a shift away from the all-data-access model that has prevailed in the tech industry, true data privacy will only come from individuals making their own choices about what to share.

FigLeaf empowers individuals with the choice of privacy.

One click delivers private email, password, payments, and online activity. Digital privacy that doesn't disrupt your life, online or off—that's the power of choice.


figleaf