The Ultimate Guide to Private Browsing

Table of Contents:

Why we should care about browsing privacy

You wouldn't let strangers into your home and allow them to take notes about what you thought, bought, or did that day. Yet, the door to online strangers is wide open all the time: the corporations, governments, and hidden players who profit from our personal information.

Consider that any time you use a web browser, your online behavior leaves a trail for others to follow. These include search engines, websites, and countless marketers who shadow every click, action, and move you make. And, contrary to popular belief, deleting cookies or browser history won't always help.

It's not just criminals who have to worry about online privacy. We all do.

The point is, it doesn't matter if you have nothing to hide. The power to control what others see and don't see about our personal lives is a fundamental human right. Sometimes we need to shut the door and assert our right to privacy. Here's a closer look at browsing privacy and how you can take back control.

Who's watching you

(hint: just about everyone)

We all know the internet isn't a private place. But what many people don't know is that a lot of very private, intimate information about our

personal lives is being gathered through invasive and sometimes illegal ways. We may not want to believe it, but it's happening all the time.Who are the players with the power to peer into our private lives?

Internet service providers (ISPs).

Internet service providers know quite a lot about us. For starters, they can see the website addresses their users visit, and can potentially read anything that's not encrypted. This includes email messages, logins, and passwords.

The U.S. government.

Government agencies think nothing of bypassing their own privacy protection laws — the very laws that were meant to protect citizens. They can monitor social media accounts, private communications, phone calls, and a lot more. And thanks to the 14-Eyes Alliance, private information can be shared across 14 nations.

Google and other search engines.

Google knows where you go, everything you search, your YouTube viewing history, and the apps you use. Google compiles surprisingly detailed ad profiles of its users. A typical profile might include your

location, gender, age, interests, and personal things that even a spouse or best friend might not know.

Social media sites.

Social media sites have become increasingly nosy over time — crossing boundaries that would have been unthinkable only a short time ago. Facebook knows about every search you've done, all of your chats and messages, your contacts, credit card information, and more.

Marketers and advertisers.

Advertiser tracking has become incredibly sophisticated. Like a digital stalker, the technology can follow you from site to site, tracking your actions and preferences. This information goes into a database where it's assigned a number for profiling purposes. As we search for products, our information becomes productized.

Browsers promise privacy, but is it an illusion?

Many web browsers offer the promise of online privacy. But it's often a mirage.

In Safari and Chrome, for example, you can ask websites not to track you. But doing this doesn't guarantee anything. Even though your browser may ask a website not to track you, websites usually don't listen and have no obligation to do so.

Nor is Chrome's Incognito mode everything it's cracked up to be. If you're logged into your Google account while browsing "incognito," Google can go back in later and connect all of your account information to your private browsing history. It's not so private after all.

There's no such thing as a free ride on the internet. Even so-called free products and services — including Google's popular Chrome browser — come at a high, yet often hidden, cost. The cost is our personal data, which is collected by the googol, i.e., a very, very large number.

But don't worry... we've got your back. Here's how you can browse privately.

Steps you can take to browse more privately

Most of us would be lost without technology. Unfortunately, the technology we love is riddled with loopholes and intentional surveillance features we may not be aware of or understand. For better or worse, it's

up to us to protect our online privacy. We can't expect companies to do it for us.Here are some places you can start:

- Configure and update your browser settings
- Lock down your social media profile
- Review your app permissions
- Use fake emails with email aliasing
- Use a no logs VPN provider

1. Configure and update your browser settings

While every browser is different, the important thing is to close down the areas that can compromise your browsing privacy. These include cookies, location services, web activity tracking, and synchronization across devices.

In Chrome, most of these options can be found in your browser settings under "Advanced" and then "Security and privacy."

In Chrome, we recommend the following:

1. Under "Advanced," click "Privacy and security" then "Content Settings" and "Cookies." Turn on "Keep local data until you quit your browser." This rids your cache of cookies every time you close your browser.

2. Under the same “Content Settings,” click “Location” and toggle on “Ask before accessing.” This forces Chrome to ask if you want to share your location with websites.
3. Turn off settings in Activity Controls to prevent Google from tracking web activities.
4. Turn off the Google Ad personalization service to prevent ad targeting.

5. Avoid using Google Sync to link your devices. If you do use it, encrypt your data.

2. Lock down your social media profile

While Facebook provides value to people, it’s not a neutral place. Its algorithms are designed to profit off our personal information. If you’re concerned about Facebook privacy — but not ready or willing to leave — you can still limit what others see about you.

We recommend taking these steps:

1. In Facebook, go to “Settings” and then “Privacy.” Here, you can limit who can see old posts, who can see your friends list, and most importantly, whether search engines can link your profile.
2. Under “Settings” and then “Location,” make sure location history is turned off.

3. To stop Facebook apps from accessing your information, you can delete the app or change the permissions. In most cases, the settings should be set to “Only Me.”

4. Under Your ad preferences, set “Ad settings” options to “Not allowed.”

3. Review your app permissions

Android Is now the most dominant operating system on mobile devices. According to research from the International Computer Science Institute, there are now approximately 17,000 Android apps collecting identifying information. These records of your activity cannot be erased. While likely in violation of Google’s own policies, it may not stop anytime soon.

Here’s what you can do:

- Unsync your apps. To stop apps from accessing your information, you can either delete the app or clamp down on permissions. On Android, go under “Settings” and then “Apps” or “Application Manager.” Tap the app, click “Permissions,” and toggle permissions off.
- Limit location sharing. Turn on location sharing only for apps that need it to work, e.g. Google Maps. Only use location sharing when the app is in use
- Close your apps. To prevent apps from trailing you around, close the app when you’re done using it.

- Check apps that can access your Google account.

4. Use fake emails with email aliasing

Sharing your email can make you an easy target for advertisers and spammers. To get around this, you can use multiple fake email addresses, aka email aliasing. Email aliasing substitutes a randomly generated email which is linked to your regular email account. Receivers can respond to your message, but won't see your real email address.

5. Use a no-logs VPN provider

Many people use a VPN (virtual private network) service to encrypt their personal data over Wi-Fi. But this doesn't guarantee ultimate privacy. If your VPN provider keeps logs, these can be used to identify you and your activities. If you're concerned about privacy, choose a VPN company that has a strict no-logs policy. This means they won't keep a history of your browsing activity on their servers.

You can take back control of your privacy

It's natural to be concerned about your online privacy.

It’s natural to be concerned about your online privacy.If anything, people are more aware than ever that their online privacy is under attack. Yet, many feel powerless in the face of these challenges. Others may not know how to take back control of their online privacy in a way that really matters.

It doesn’t have to be this way. We do have the ability to take control of our private lives.

We believe you have the right to browse privately, any time or anywhere. FigLeaf wants to help put the power back in your hands.

Find "The Ultimate Guide to Private Browsing" PDF version here.