Secure & Private Browsing

5 Most Secure Browsers - Secure & Private Browsing

Written by Douglas Crawford

Concerns with Regular Web Browsers

Commercial browsers such as Chrome, Edge, and Safari all pose privacy concerns.

Google is a company that fully cooperated with the NSA in its PRISM mass surveillance program.

Google has a detailed breakdown of how Chrome affects your privacy, but essentially, Chrome is just spyware for Google. Although Chrome does offer user-controlled privacy settings, they are hidden away in the browser, and users have manually to opt-out of features that invade their privacy.

Even with all user-controlled privacy settings locked down, there is every reason not to trust Google to not spy on you, anyway.

If you take your online privacy seriously, the first step is to download a private browser.

Browsers such as Chrome, Edge, and Safari all collect user data. This includes; Browsing history, login credentials, cookies (placed by websites you visit), and auto-fill information (on login forms). This is used in order to create user profiles so that they can advertise to you further down the line.

The safari, edge, and chrome alternatives in this article do not perform meaningful tracking (if any at all) for their developers, and many of them include built-in protection against tracking by websites.

Secure & Private Browsing

Best private browsers

Firefox

Firefox is a fast and private open-source browser, and it has been fully audited, which proves they do exactly what they say they do. It is developed by Mozilla Foundation, which is a non-profit organization.

Firefox is arguably at least as secure as Chrome. The new (ish) “Quantum” rendering engine has been built from the ground up to improve speeds and includes Tracking Protection built-in to the interface.

Firefox now also includes built-in protection against canvas fingerprinting, the most common form of browser fingerprinting.

Firefox is streaks ahead of its mainstream competition, as it does not track your web browsing to target ads at you.

Tor Browser

Tor Browser was designed to provide secure access to the Tor anonymity network. Tor Browser is based on Firefox but with additional security features.

Key features include:

- Uses HTTPS Everywhere and NoScript (all scripts disabled by default) plugins
- Blocks other browser plugins such as Flash, RealPlayer, and QuickTime
- Uses Disconnect.me as its default search engine
- Always uses Private Browsing mode (tracking protection, no browsing history, passwords, search history, cookies or cached web content saved)

Secure & Private Browsing

Waterfox

Waterfox is an open-source browser based on Firefox. In many ways, it is fairly plain vanilla Firefox 56, and there are no plans to move beyond that. This means that it supports both legacy Firefox add-ons, and the new add-ons. It includes tracking protection and will sync with your regular Firefox account. Some stability issues have been reported with Waterfox, but these only affect a tiny minority of users.

Waterfox is essentially a one-man project, and it seems to be doing a good job at ensuring that Waterfox incorporates the latest Firefox security patches. The problem is that these patches are for a different version of Firefox (currently 66.0.3). This could result in Firefox 56 (and earlier)-specific vulnerabilities being left unpatched.

Waterfox is available for Windows, macOS, Linux, and Android.

Brave

Unlike all the other browsers in this roundup, Brave is based on Chromium instead of Firefox. Chromium is the open-source code behind Chrome, with all the closed proprietary bits stripped out (at least in theory).

It comes with a built-in ad-blocker, tracking protection, script blocker, and HTTPS-Everywhere functionality. Brave also features one-click anti-fingerprinting and WebRTC leak protection. And anyone used to Chrome will feel at home instantly.

Despite all this, Brave is a controversial choice…

- Brave helps to fund itself via an ad-replacement program. This replaces "bad ads" which include tracking pixels with "good ads" from its network partners. Participating in this program is opt-in, but detractors feel it adds to a problem

that private browsers are supposed to be fixing.

- The CEO of Brave Software is ex-Mozilla CEO and JavaScript inventor Brendan Eich. Eich was forced to stand down from Mozilla in 2014 after he donated $1,000 in support of California's Proposition 8, which attempted to prevent same-sex marriage for LGBTQ Californians. This has no relevance to the quality of the software of course, but you may wish to consider if you want financially benefit someone with these views by using his product.

Brave is available for Windows, macOS, Linux, Android, and iOS.

Pale Moon

Pale Moon is a lightweight and highly customizable open source fork of Firefox. Unlike Waterfox, its code has separated completely from Firefox. It is compatible with many classic Firefox add-ons, but not all of them.

It is *not* compatible with Firefox's new WebExtensions add-ons, but it has a growing library of add-ons that have been rebuilt specifically for Pale Moon.

Much of Pale Moon has been updated with code from more recent versions of Firefox, but its user interface remains the highly customizable XUL-based front-end last seen in Firefox 28. This includes support for a wide range of custom themes and skins.

Pale Moon does not offer any "special privacy features" as such, but it doesn't contain dubious, privacy-invading software, included in other mainstream browsers.

Although it provides a *"close adherence to official web standards and specifications"* Pale Moon is still working on full support for HTML5 and CSS3, so it can struggle when rendering some web pages.

Secure & Private Browsing

Some users say that it lags behind with security updates, but this is very unfair. It can take up to a week before Mozilla allows the Pale Moon developers access to its latest patches, but these are always implemented as soon as possible and are always up-to-date.

Pale Moon is available for both Windows and Linux.

Firefox Focus

Firefox Focus is a private browser for Android and iOS. Key features include tracking protection and ad-blocking (using the Disconnect block list). All browsing is effectively performed in Private Mode, so no browsing records are stored locally.

It is also a very stripped-down browser, and so does not have all the unwanted “features” found in full Firefox.

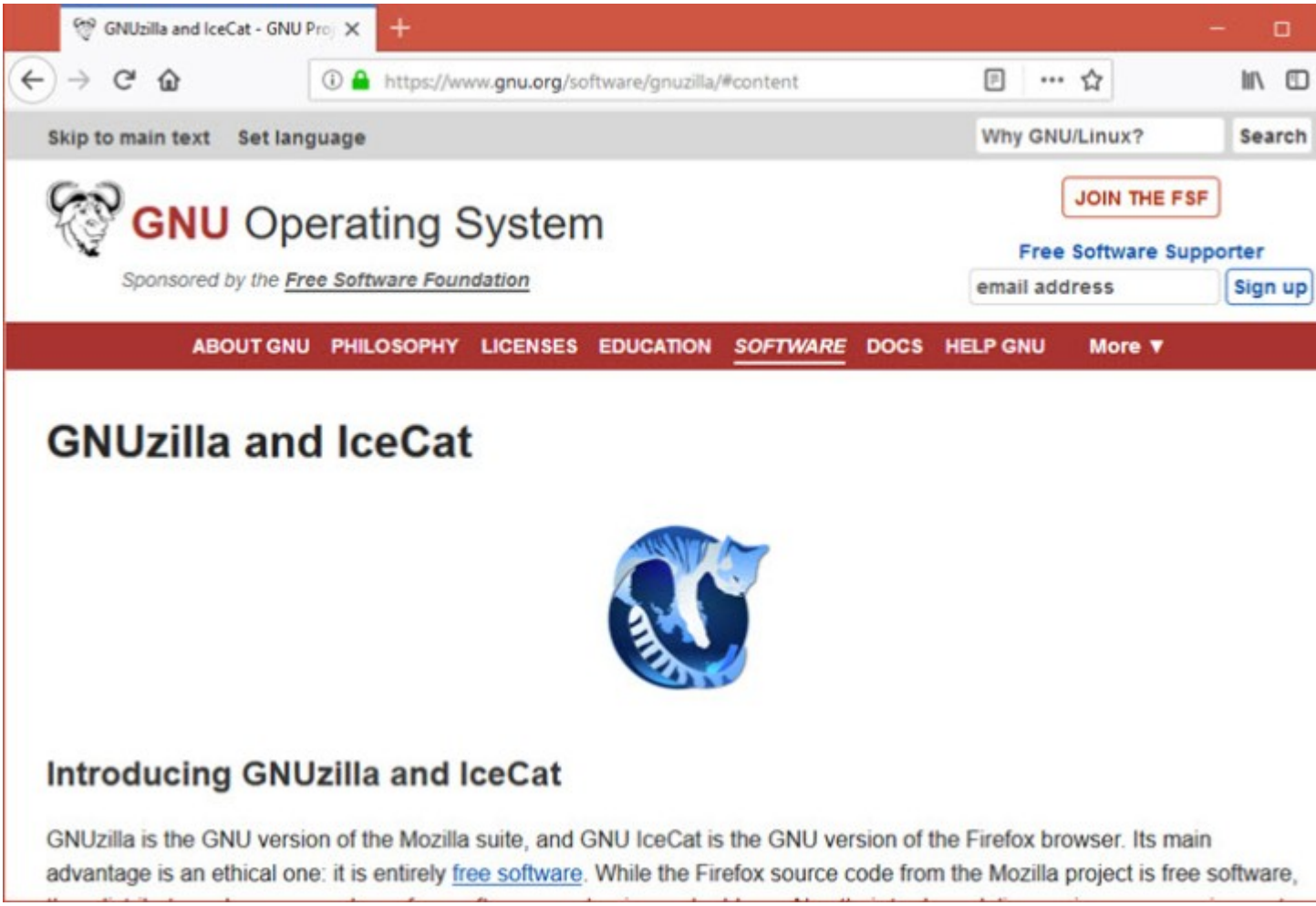
On the day-to-day usability front, however, its lack of full support for tabbed browsing makes Firefox Focus difficult to recommend. Tabbed browsing *is* now supported, but only by right-clicking on an existing link -> Open link in new tab.

The fact that you are permanently in Private Mode also means that passwords and logins are not saved between sessions (although this problem is mitigated in iOS by keyboard access to Keychain).

Another major issue is that about: config is not accessible in Firefox Focus. This means you cannot disable WebRTC, which makes VPN users potentially susceptible to WebRTC leaks.

Secure & Private Browsing

IceCat and IceWeasel



GNU IceCat is just Firefox with the trademarked branding removed to comply with the GNU Project's free software guidelines.

It will block third-party zero-length image files, also known as web bugs. It will also detect and block non-free JavaScript, and has the option to set a different user agent string each for different domains in about:config. This is good for defeating browser fingerprinting.

IceWeasel is very similar to IceCat, except for Debian (Linux) and without IceCat's additional privacy features. Now that Firefox has returned to Debian, IceWeasel is no longer

maintained. IceWeasel is based on an older (pre-Quantum) version of Firefox, but Icecat is based on the latest Firefox ESR. This means it can use up-to-date Firefox add-ons and has a Quantum speed boost.

IceCat is available for GNU/Linux, Windows(unofficial build), Android and macOS (self-compiled).

SeaMonkey

SeaMonkey, like Pale Moon, uses Firefox code and the Gecko rendering engine. However, It is different from all the other services in our private browser list.

It incorporates a browser, an email and newsgroup client and a WYSIWYG HTML editor. Some might argue this makes it very bloated, but most modern hardware can handle the bloat easily.

SeaMonkey is great for those who want an old-school internet experience, but in terms of updates and security patches, it lags behind Firefox.

This is the same for all other commercial browsers. Microsoft also collects user data, and it has been reported they also have worked with the NSA, so it's Edge and Internet Explorer browsers cannot be trusted.

Apple is primarily a hardware manufacturer, so does not rely on advertising revue as its business model. It also has a robust global privacy policy. It did participate in the NSA's PRISM program, however, and Safari is closed source.

Opera is now owned by a Chinese consortium and clearly states in its Privacy policy that it collects a fair amount of data which *"may be considered personal"*.

Crucially, all these popular browsers are closed source. This

Secure & Private Browsing

means that there is no way to verify that they contain no creepy code or are otherwise not doing something they shouldn’t.

Is private browsing mode secure?

All modern browsers feature a private or incognito mode. It is important to understand what this feature does because its name is in many ways quite misleading. This can result in people surfing the internet while wrongly thinking their privacy is protected in ways that it is not.

So what does private browsing mode do?

Private browsing mode is primarily aimed at preventing people who have direct physical access to your computer (such as family members) from seeing what you have been up to online. When using private mode:

- Websites you visit are not saved to your browser history
- Searches are not saved locally
- Form data is not saved locally
- Cookies are deleted when the session ends
- Your browsing sessions are isolated from your regular sessions

By deleting cookies between sessions private browsing mode does usefully prevent some basic tracking by websites, but the benefits of this are easily overstated.

What does provide mode not do?

Basically, private mode does not make you private on the internet:

- Websites can see your unique internet (IP) address
- Websites cannot track you using cookies but can track you using browser fingerprinting canvas fingerprinting, and various other methods
- Your internet provider (ISP) can see every website you visit

Secure & Private Browsing

on the internet
- Downloaded files and bookmarks made in private mode are saved as normal
- Keyloggers and malware installed on your system can track everything you do online

The takeaway

If you want to hide birthday present shopping from your spouse on a family computer or hide your adult viewing habits on a shared laptop, private mode is great. It is, after all, often referred to as porn mode for a reason!

What it does not do is provide any meaningful privacy (let alone anonymity) from your ISP or anyone watching on the internet. For this, you need to use a VPN to hide your IP address, and various browser add-ons to prevent web tracking (which may or may not be bundled with the privacy browsers discussed above).

All the browsers in this list are open source and provide much more privacy than Chrome, Edge/Internet Explorer or Safari.