How to choose a browser for everyday use?

Introduction

Let's start with the basics. What is the point of a web browser? Originally, it was to be able to read HTML documents, but since then, the Web has changed massively, and modern browsers need to satisfy more demands. The basic terminal browser - links, w3m, Lynx, elinks - can still be used today to display websites only in text. Actually, elinks supports features that are somehow missing in "modern" web browsers (such as editing cookies, custom stylesheets or keybinding), but in the end, they can all be got back through addons. Maximum of 256 colors, no images, little or no Javascript support, limited CSS support, no loading of non-HTML content such as videos (but can load externally), and no addons make these unsuitable for modern day browsing.

I could mention many other browsers here. Surf is a graphical web browser that has image and Javascript support, but no tabs or an actual user interface. Midori has everything you'd expect from a modern web browser and even includes in-built functionality to replace some of the common addons, but it's not enough. Otter Browser is a promising project with a very nice UI, but has no addon support (so far, though it's planned). Qutebrowser is a keyboard controlled browser that recently added per-domain settings, but they are inferior to uMatrix. Many of its features can be replaced by, again, addons.

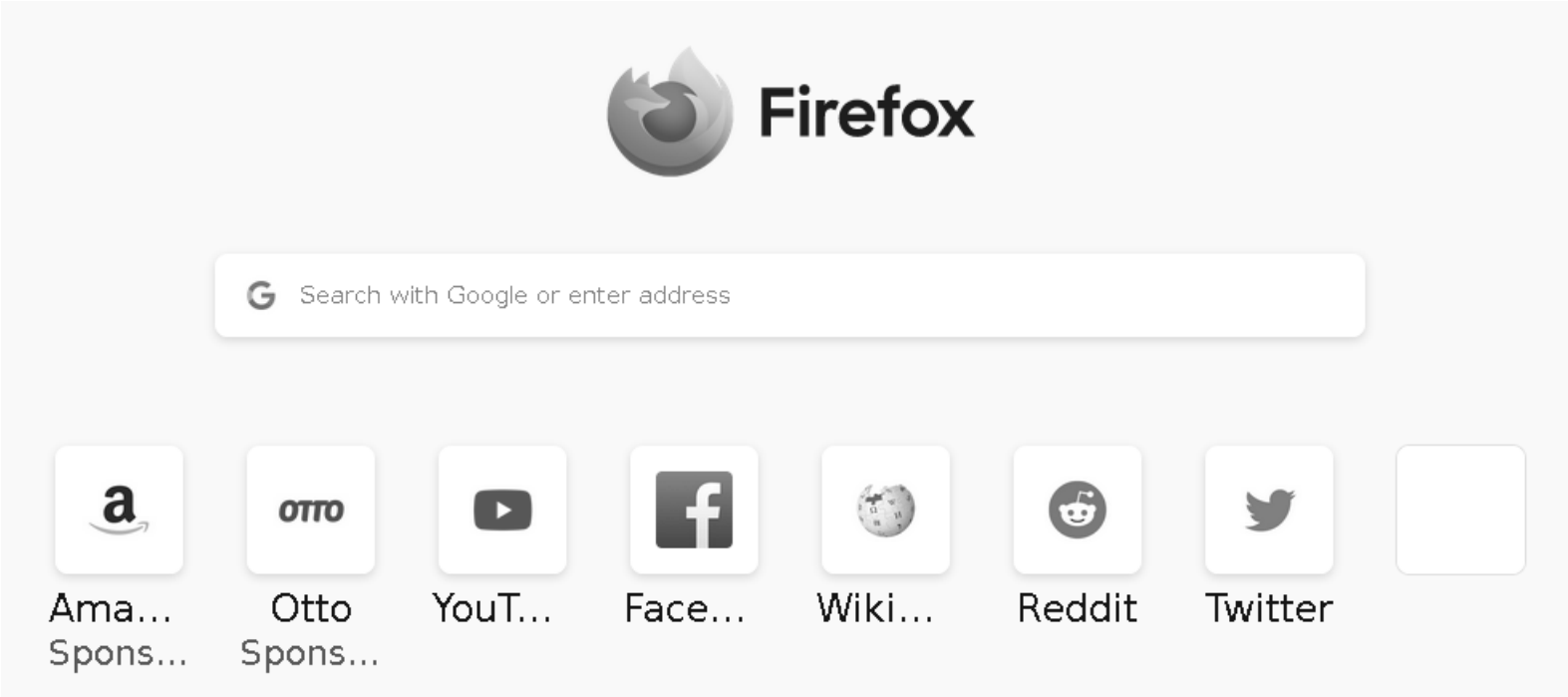
One advantage of these niche browsers is that they **don't spy on you**, but what I've learned from trying probably all of them is that, in the end, **addons are essential** - especially uMatrix is

irreplaceable. So, for a day-to-day browser, you have only two options: Firefox-based and Chrome-based. Since they all support the same addons (with slight exception in Pale Moon), we will have to use some other criteria to judge these browsers. These consist of **usability, privacy, customizability, philosophy, respect for the user, looks, and resource usage.** Let's analyze them one by one:

Firefox-based browsers

Mozilla Firefox

UPDATE July 2023: I just did some testing, in case you were wondering just how bad this browser is in terms of privacy. So, it sends 112 requests to various moz domains during your first run of it. But that's not enough for them. They have this crap called *Firefox Glean* that reports almost every interaction you have with Firefox to Mozilla, with a browser session ID, unique user ID, precise timestamp and various system information included. These requests happen anytime you visit a menu (Addons, Passwords, Settings, etc), change a preference, open a new tab, click through one of the four prompts that appear when you first run the browser, or do literally anything else. And **every time you turn off Firefox, it sends a giant request to Mozilla containing information about pretty much the entire state of your browser** at the moment of closure. It is quite eerie, if you watch it from the inside. So go whip out mitmproxy right now (it is easy) and see for yourself. This alone should be reason enough to trash this browser, but there is more. Firefox contains links to several big tech sites (that it pretends to fight) inside their New Tab page:



They also kept the Directory Tiles (sponsored pages) in there, that I thought they've killed. And of course clicking either of those is tracked. The UI reveals very few options for configuration, as expected. And about:config requires two fucking confirmations to enter, and isn't intuitive at all, anyway. I could go on and on about specific issues, but to understand Firefox in more depth, you have to dig into the history of it and its corporate creator - Mozilla. You will learn why all the anti-privacy stuff is in there, why you can't install addons without Mozilla's approval, why XUL addons got deprecated, why Firefox ignores user choice in terms of proxy settings, and many other juicy details. Knowing the context behind what's going on will provide you with a lot more understanding than just burying you with more specific issues, so go read the article.

But I have to mention some more relevant points for potential users of this browser. It uses ~260MB RAM with one empty tab; significantly more than that of many Chrome-based

browsers and over double that of Pale Moon. It requires GTK3, like all its forks. And those are all a lot better than the original, since they at least remove some / most / all of the spying. So, Firefox itself is completely useless. What about the others? They are all dependent on Mozilla. And consider that in August 2020, Mozilla has ceased caring about technology (archive) (MozArchive), but instead fully began focusing on social issues - *"From combatting a lethal virus and battling systemic racism"*. As if it wasn't already obvious earlier, they have now **thrown out 250 people mostly working on technical stuff** such as their rendering engine or browser security. I suspect this is preparation for ceding control of the web browsing ecosystem to Google soon (as predicted in Mozilla - Devil Incarnate, they were always controlled opposition). I doubt any Firefox-based browsers will survive this apocalypse, to be honest. Just know what you're signing up for, while you read the below.

GNU IceCat

UPDATE December 2023: Someone has compiled IceCat version 115 for Linux, Windows and Mac (the last officially supported version is still the ancient and insecure 60). And so, time for a new review. Brace yourself, for I will (maybe surprisingly) have a lot to say. Anyway, IceCat is still Firefox, but scrubbed of most unsolicited connections (but still has OCSP, and captive portal detection, it seems). With the updated version, the resource usage has also been "updated" to now clock at about 300mb RAM (compared to the 120 of old versions). What makes IceCat unique are the privacy-enhancing addons coming along for the ride. IceCat uses the extension *Privacy Redirect* to...well, redirect big tech services to their more user respecting replacements (Invidious, Nitter, etc). Not much to say there, it is a good and obvious addition - so let's move on.

As is tradition, IceCat includes LibreJS, that I don't really like; again, it has the same flaws as always, meaning lots of resource usage and the arbitrary allowance of "trivial" scripts. Additionally, it now brings with it **three** more extensions hoping to fix certain sites, that LibreJS would otherwise break. Is it really a viable approach to write replacements for scripts on every site which lacks the "right" license? Funnily enough, IceCat's LibreJS implementation includes **whitelists for reddit scripts** - lol! And the first script there even looks quite nontrivial to me. If the licensing issue is that important to you, then stop giving passes to big tech just because they're big.

Another included addon is JShelter, invented to prevent JavaScript-based fingerprinting by reporting fake data to certain JS functions. By this, it is trying to convince the site you're visiting that you're a different person than before. It's too complicated to explain it all here but let's just say that this approach is quite leaky in that it needs just one thing that cannot be faked or can somehow be detected by the fingerprinter to foil your attempts. JShelter admits it eg here (archive) (MozArchive):

> *No. We currently do not have a consistent method that spoofs fonts reliably. If you are concerned about font enumeration, you can track the relevant JShelter issue.*

I don't believe that this approach is very fruitful. JS is just too complicated, it's a real language that has access to everything that the browser is doing. And you can't "enumerate badness" well enough to block fingerprinting reliably this way. For another example, see Advanced Tor Browser Fingerprinting (archive) (MozArchive). Keep in mind that even if you like JShelter's approach, it (by default) is concerned **only with fingerprinting prevention** - it still lets the browser execute JS functions that might be malicious. However, I guess **there is no harm in JShelter being used** - at least it provides **some** protection if you're going to be enabling

JavaScript anyway. Blocking JS execution completely would be more effective, though; there's no need to fake data for functions that don't run at all (but of course, then you can't do anything that requires JS).

But this is still not that great against first party fingerprinting; you're connecting to the first party domain regardless, so it can use your user agent, IP, OS, etc. to add to the fingerprint. There is no perfect way to prevent first party fingerprinting; remember, you have to convince the fingerprinter that you're a different person than before, and any single piece of data can blow your cover. The best way is to use an entirely different physical computer every time you visit that site, or at least a different OS / browser combination and also change your IP. For third party fingerprinting, it is easy - just block the connections; if there is no connection made, there is nothing to fingerprint you by.

And so, we reach the final addon included in IceCat, namely the rarely seen TPRB (*Third Party Request Blocker*) - which actually has a lot of functionality not related to its name. For one, it is **able to block Cloudflare**, and can also redirect the pages behind it to their Web Archive versions - so it's a replacement for the abandoned *Block Cloudflare MitM Attack*. It can block specific CSS / JS functions, as well as file type downloads and do many many other things I don't care to list here. But the problem is that the defaults are very permissive - whitelisting YouTube, and again Reddit, as well as exposing you to the Cloudflare MitM rape (a decision I cannot justify at all). If you have the ability to prevent such a serious security vulnerability, why not make use of it? In terms of its main functionality (being a proto-uMatrix), TPRB **does block third party requests by default** - but you can only allow them selectively by domain, and not by type (so either all or none from a certain domain). Also, all third party CSS is let through - pretty much refuting the name of the addon (though you can change this, but we're talking about the defaults here).

And this exposes the problem with the entirety of IceCat's design - which is that its target audience **is the normie, and not the hacker**. That's why JS is enabled by default, and then there are all those measures attempted to contain it. It even gives up the FSF's favorite licensing crusade just to let people use reddit. And though it includes the extremely powerful TPRB, again the defaults are so permissive as to make most of its functionality irrelevant until the user digs deep into the settings. Overall, IceCat just does not know what it wants to be; it is a weird mish-mash of blocking undesirable things but also allowing stuff through the shields arbitrarily for convenience. It would be nice to finally have a modern browser perfectly mitigated by default, but IceCat is not it. It - like all other FF forks - is also on Mozilla's leash, and this won't ever change.

LibreWolf

UPDATE January 2022: old review kinda sucked, I'm rewriting it. LibreWolf is to Firefox what Ungoogled-Chromium is to Chrome. At least, so it seems, but it does not take a strict stance against unsolicited requests like Ug-C does (which is also my view - zero unsolicited requests is optimal). It includes the uBlock Origin addon by default (instead of the much superior uMatrix), and automatically updates the lists for it - as well as making a request to Mozilla's servers for their Tracking Protection. Otherwise, LibreWolf is not doing anything special, just changing some settings (which can also be accomplished by the many user.js files floating around). Their issue tracker is on gitlab which is Cloudflared and doesn't work in Pale Moon; this does not affect the browser directly, but shows the developers don't respect the users or care about their privacy (**UPDATE July 2024:** now on codeberg, but still used gitlab for a significant period of time). Packages for some distros, Windows and macOS exist - as well as an AppImage if your distro isn't on the list. Overall, this is the way to go if you want Firefox

without (most of) the privacy violations. But - since they've only got five devs on the team - LibreWolf will always be dependent on Mozilla and unable to reverse any of their major shitty decisions, so watch out. Let me reiterate, this is nothing more than Firefox with a few settings changed and uBlock Origin added on top.

Waterfox

UPDATE July 2023: retested. First of all, Waterfox's site is now behind Cloudflare. Even then, the download links are still on Github, so at least you can download this browser without dealing with the great MitM. Or so it would seem, but Github doesn't work properly in Pale Moon, so you're limited to the download of the beta version (which doesn't even run on my machine). I had to use a third party AppImage to test this; a total incompetence on the devs' part. The downloads should be hosted locally and Cloudflare should be ditched! But okay, I've grabbed the AppImage. What happens next?

Last time I used Waterfox, it made 100+ requests at launch. You'd think that after 4 (?) years the devs would have learned something, since they use privacy (archive) (MozArchive) as a selling point:

> *What you do within your browser stays with you. We don't need to know. Telemetry is disabled within the browser - and only limited data collection is used to keep your browser up to date and secure.*

And yet - at launch - Waterfox has immediately connected to:

- Mozilla's Location services

- Mozilla's Shavar services
- Mozilla's Push services (archive) (MozArchive) - *"We store your IP address for 90 days as part of this service."*
- Firefox Settings services (unique ID and precise timestamp included)
- Their own page, which in turn made many requests trying to load Cloudflare's captcha
- Mozilla again, to download a bunch of lists for Tracking Protection
- *http://ciscobinary.openh264.org/* to download some codec
- *https://accounts.firefox.com/metrics-flow?entrypoint=aboutwelcome* with a device ID included
- More Firefox Settings to download URL lists for who knows what

Then - when I thought it's all over - Waterfox started making hundreds of requests to *https://firefox-settings-attachments.cdn.mozilla.net/security-state-staging/intermediates/[randomstring.pem]*. When it reached 700 I knew it's going to go on forever (and crash my mitmproxy eventually), so I had to shut the browser down. It seems that disabling OCSP kills the requests, so I was able to resume testing after relaunching. How does this kind of crap get past the testing phase, if this browser even had one?

Bing is the default search engine, which is quite the embarrassment for a browser advertising privacy. And they even submit every typed letter to it separately for suggestions, by default...ugh. This doesn't seem like a privacy-based browser. Hey, I even disabled everything I found suspicious in the *Settings* menu, and yet, Waterfox keeps connecting to crap. Yeah, I could probably kill that in the dumpster known as about:config, but your mom won't be able to. And if a browser markets itself as privacy-based, it needs to be such for everyone - not only

tech enthusiasts. To me, Waterfox isn't even a little bit privacy based, unless just being an improvement over Firefox is enough to qualify for that category. Its *Sync* functionality even parasites on Mozilla's service, which is quite pathetic and of course will share your data with them, again. Remember how they claimed only *"limited data collection"* is done? Well, they can't control that since they depend on Mozilla for so much functionality. They do not even have their own Addons store, so they have to hope that their overlords Google and Mozilla won't eventually just start deleting undesirable addons.

I really do not see the point to this browser. All it does is change a few settings of Firefox to become slightly less violating. But it can't even disassociate itself from Mozilla, what with being integrated with Firefox Accounts, using Mozilla for location, push, codec downloads, etc. And all of that means massive amounts of data collection that Moz is famous for. Hey, you have a few more options in the *Settings* menu...you can put your tabs at the bottom. Who really cares, there are surely extensions for this. You can auto-hide the bookmarks bar and the back / forward buttons, which appear to be the only useful new options. Waterfox even uses up more RAM than FF itself, clocking at 300mb. Never knew what's the big deal about this browser, and I still don't all these years later. They seem to have done nothing but to include a few more cosmetic options in the UI, most of which (like the *Square* ones), are barely noticable; and more spyware compared to the 16 requests that a tester reported to me a few years back. Ignore the shilling and avoid.

SeaMonkey

This will be short and might not be completely technically accurate, as this browser has too many flaws for me to bother with it. As expected from FF offshoots, it spies on you. Here are

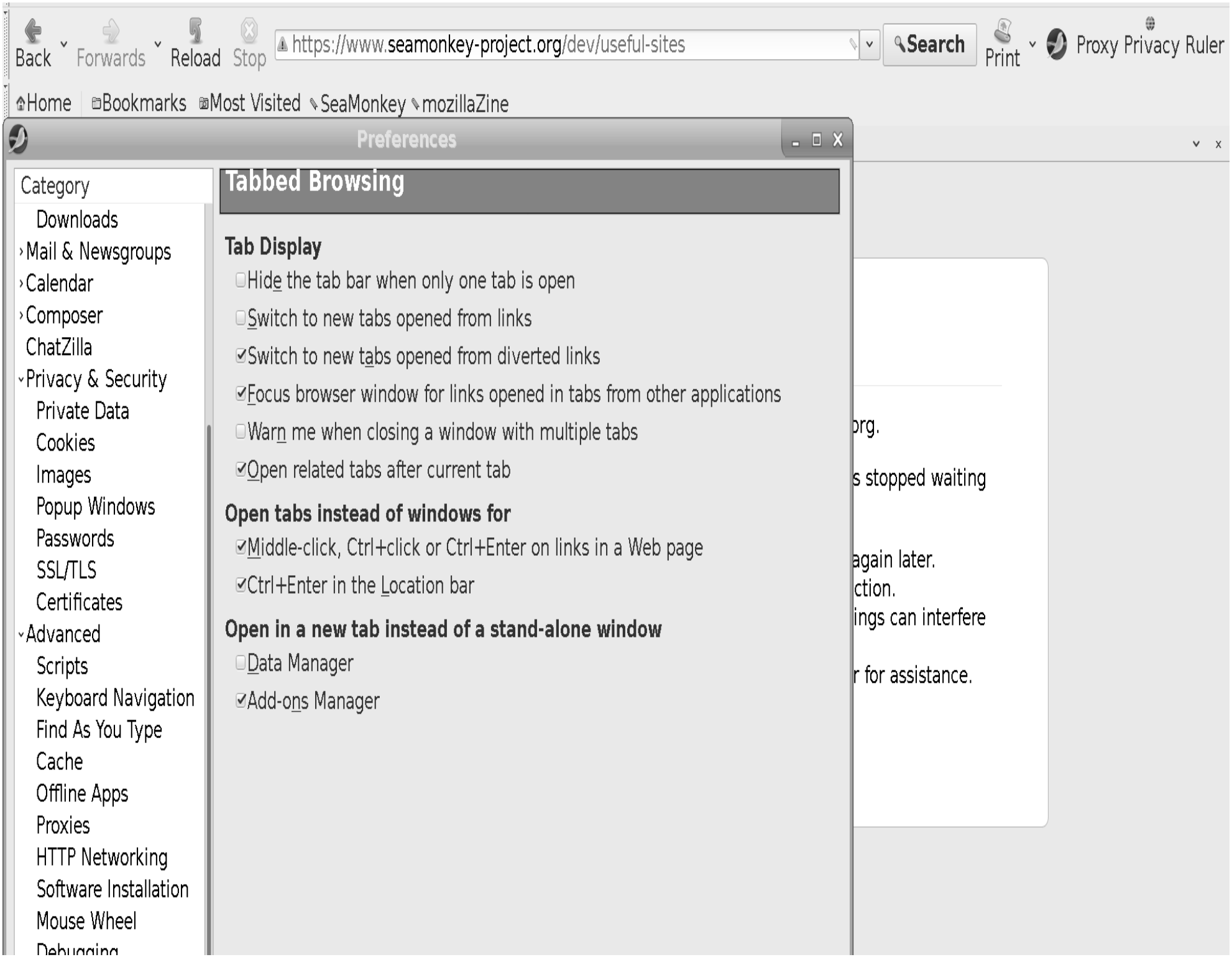
the requests that SeaMonkey sends at launch:

```
POST https://location.services.mozilla.com/v1/country?key=no-mozilla-api-key
     ← 200 application/json 53b 453ms
GET https://www.seamonkey-project.org/releases/seamonkey2.53.17/
    ← 304 [no content] 271ms
GET https://www.seamonkey-project.org/css/artemia/template.css
    ← 304 [no content] 360ms
GET https://www.seamonkey-project.org/favicon.ico
    ← 404 text/html 4.1k 365ms
GET https://www.seamonkey-project.org/images/seamonkey16.png
    ← 304 [no content] 384ms
GET https://www.seamonkey-project.org/css/base/template.css
    ← 304 [no content] 328ms
GET https://www.seamonkey-project.org/css/artemia/content.css
    ← 304 [no content] 300ms
GET https://www.seamonkey-project.org/css/base/content.css
    ← 304 [no content] 276ms
GET https://www.seamonkey-project.org/images/template/header-logo.png
    ← 304 [no content] 279ms
GET https://www.seamonkey-project.org/images/template/header-background.png
    ← 304 [no content] 222ms
GET https://www.seamonkey-project.org/images/template/breadcrumbs-background.png
    ← 304 [no content] 211ms
POST https://shavar.services.mozilla.com/downloads?client=navclient-auto-ffox&appver…
     ← 200 application/octet-stream 8b 633ms
GET https://safebrowsing.googleapis.com/v4/threatListUpdates:fetch?$ct=application/x…
    ← 429 application/x-protobuf 650b 338ms
GET https://live.thunderbird.net/services.addons/api/v3/addons/search/?guid=inspecto…
    ← 302 text/html 568b 518ms
GET https://services.addons.thunderbird.net/api/v3/addons/search/?guid=inspector%40m…
    ← 200 application/json 4.3k 1.40s
GET https://versioncheck-bg.addons.thunderbird.net/update/VersionCheck.php?reqVersio…
    ← 200 text/xml 154b 512ms
GET https://versioncheck-bg.addons.thunderbird.net/update/VersionCheck.php?reqVersio…
    ← 200 text/xml 339b 514ms
GET https://versioncheck-bg.addons.thunderbird.net/update/VersionCheck.php?reqVersio…
    ← 200 text/xml 556b 574ms
GET https://versioncheck-bg.addons.thunderbird.net/update/VersionCheck.php?reqVersio…
```

First, we have it connecting to Mozilla's location services, who then obviously learn your location. Then a bunch to SeaMonkey's own site. The *shavar* thing has something to do with Google's Safe Browsing, and can only be disabled from the dumpster known as about:config. Later, the actual download of the Safe Browsing lists that comes every 30 minutes. Updating addons through Thunderbird's (Mozilla's) site; hey, I don't care to be telling Moz what browser or OS I'm using, okay? Why not use your own site for updates? Downloading blocklists again from Thunderbird's site, this time telling Moz whether you use Pulseaudio or not. For some reason SeaMonkey connects to a *firefox.settings* domain...fuck it, I'm tired of this. The only

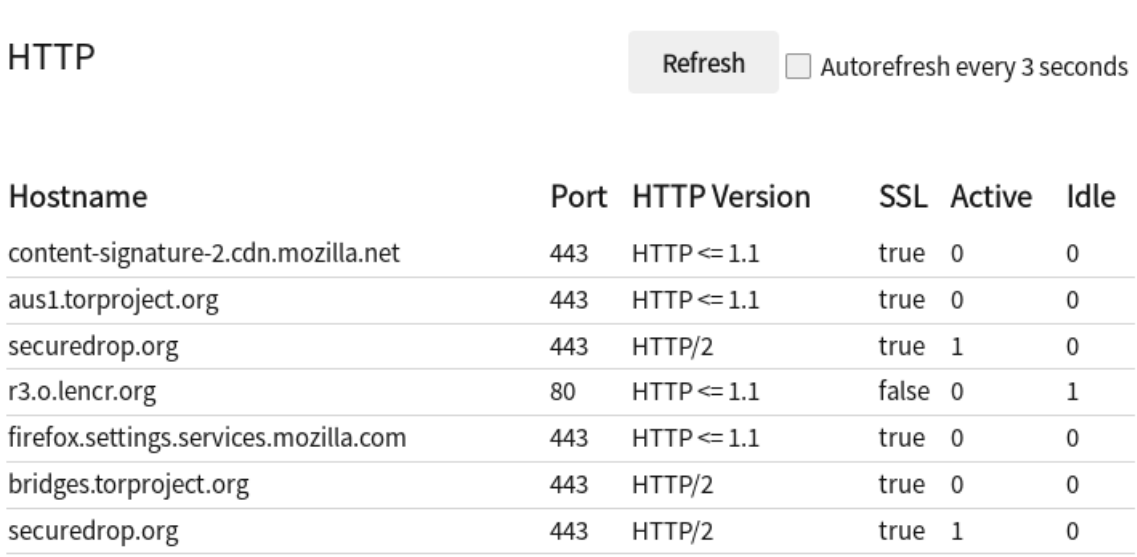
justifiable requests are those to SeaMonkey's own domains for update lifting, but even they **should be disabled by default**. SeaMonkey clearly doesn't care about user privacy too much, though it's miles better than vanilla FF in that it doesn't track your specific movements.

SeaMonkey uses XUL (like Pale Moon), so FF addons are incompatible with it. Though the rendering engine is actually Gecko, so you get Firefox's website compatibility. In terms of the addons, however, it seems somehow different in its internals than Pale Moon, because **PM addons don't work with it**, either. So extensions have to be specifically coded for SeaMonkey support, and it seems not many people care about that. No uMatrix here, my friends! Therefore, effectively, this browser becomes minimal-like at least in terms of content blocking capabilities. Even if all the addons worked, this browser requires you to add obnoxious custom about:config entries so that they are actually allowed to be installed. Can I get a browser that doesn't treat me like a Down's syndrome patient and exposes all its functionality through the UI? Even better, just take off all blockages by default and I'll deal with any eventual breaks, thank you very much. SeaMonkey also includes an IRC client, RSS client, and mail client inside it, which is just pointlessly duplicating stuff I already have (and I have tested none of them). But I guess some people like it all in one place, so if you're one of those, SeaMonkey might be right up your alley. And you can use only the web browser part if you want to. RAM usage is 120mb, similar to old versions of IceCat. GTK3 is required, and a cursory look tells me this browser doesn't really have a lot of support at all. It seems that the only semi-positive of SeaMonkey is that the UI is still old school, with separate menus and many options. Edit: I forgot to mention that it includes the RSS button by default in the address bar. But that's surely not enough and Pale Moon is still way superior.


Back
Forwards
Reload
Stop
https://www.seamonkey-project.org/dev/useful-sites
Search
Print
Proxy Privacy Ruler
Home
Bookmarks
Most Visited
SeaMonkey
mozillaZine
Preferences
Category
Downloads
Mail & Newsgroups
Calendar
Composer
ChatZilla
Privacy & Security
Private Data
Cookies
Images
Popup Windows
Passwords
SSL/TLS
Certificates
Advanced
Scripts
Keyboard Navigation
Find As You Type
Cache
Offline Apps
Proxies
HTTP Networking
Software Installation
Mouse Wheel
Debugging
Tabbed Browsing
Tab Display
Hide the tab bar when only one tab is open
Switch to new tabs opened from links
Switch to new tabs opened from diverted links
Focus browser window for links opened in tabs from other applications
Warn me when closing a window with multiple tabs
Open related tabs after current tab
Open tabs instead of windows for
Middle-click, Ctrl+click or Ctrl+Enter on links in a Web page
Ctrl+Enter in the Location bar
Open in a new tab instead of a stand-alone window
Data Manager
Add-ons Manager
org.
s stopped waiting
again later.
ction.
ings can interfere
r for assistance.

TOR Browser

Auto-updating piece of trash. Enforces connections to the TOR network (which can also be done in any other browser), but **will not even run** if you have TorDNS enabled system-wide (*"Failed to bind one of the listener ports"*). **UPDATE**: it was reported to me that this issue can be fixed by changing the default torrc ports away from what TB uses, but I did not confirm this myself. Default addons include NoScript, which is much inferior to uMatrix. Yet, the TOR Project discourages modifying the addon setup, even though the whole basis for this has been refuted by Moonchild (archive) (MozArchive). Yes, a properly configured Pale Moon is **better against fingerprinting than TB**. TOR Browser is still dependent on the evil Mozilla - which means that when a bug like this (archive) (MozArchive) happens (yes, the one that disabled all addons) TB is also affected, and its security laid bare. Using TOR Browser does allow you to bypass Cloudflare browser checks, but this is likely because **they work together to help Cloudflare spy on people wanting to be anonymous**, making TOR Browser a honeypot. This is further supported by the fact that the TOR Project deleted a ticket criticizing Cloudflare (MozArchive) - but left all other tickets alone, proving it was not because of a *"pedophile attack"*, like they claimed. I see no reason to use this browser, really, when PM can be configured to use TOR all the same, with all the other advantages. TB also includes a few unsolicited connections (aside from the updates) that are hard to disable. **UPDATE August 2022**: more requests have surfaced, and the securedrop one **cannot be disabled** according to a contributor:



Hostname	Port	HTTP Version	SSL	Active	Idle
content-signature-2.cdn.mozilla.net	443	HTTP <= 1.1	true	0	0
aus1.torproject.org	443	HTTP <= 1.1	true	0	0
securedrop.org	443	HTTP/2	true	1	0
r3.o.lencr.org	80	HTTP <= 1.1	false	0	1
firefox.settings.services.mozilla.com	443	HTTP <= 1.1	true	0	0
bridges.torproject.org	443	HTTP/2	true	0	0
securedrop.org	443	HTTP/2	true	1	0

UPDATE May 2022: it was just reported to me that, even after mitigating the spyware (archive) (MozArchive) in this browser, it just comes back after an update - so the mitigation has to be repeated. See the danger with indiscriminate (and especially automatic) updating now?

I mean, let's be clear here about what TOR Browser even is. It is just Mozilla Firefox with a few changed settings and TOR enforcement. It is not magic. And it still makes unsolicited requests (which are violating), so it's not a hero. Look at what they say in their design document (archive) (MozArchive):

> *In general, we try to find solutions to privacy issues that will not induce site breakage, though this is not always possible.*
>
> *Keystroke fingerprinting is the act of measuring key strike time and key flight time. It is seeing increasing use as a biometric.*

> *Design Goal: We intend to rely on the same mechanisms for defeating JavaScript performance fingerprinting: timestamp quantization and jitter.*

So instead of just disabling JavaScript by default, they try to submit fake data for every value that could possibly be used to fingerprint you. This is just enumerating badness and inferior to the uMatrix approach of blocking it all by default. **It is impossible to have a truly mitigated browser when you allow websites to do whatever they want**; but the TOR Browser - hoping to avoid *"site breakage"* - is trying that, regardless. When it is the bloated sites and the technology they are based on that are the problem.

How likely is it that the TB approach will continue to be fruitful (assuming that it even is now) when Mozilla keeps adding more attack vectors like WebAsm, new JS / CSS functions, etc? TB should probably be based on something lighter, with no JS support at all, maybe a Lynx derivative. But then is TB even needed in that case, instead of just hooking up Lynx to TOR? Maybe it's time to realize that there are fundamental problems with the web that can't be fixed with a bunch of bandages that TB provides.

Summary

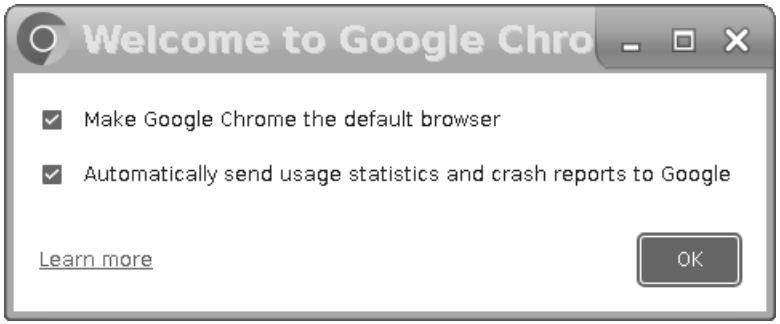
Firefox is absolutely terrible and its forks have not much to be proud of either, as we can see. Though some of them do remove (some or all of) the spyware problems, they either add their own or have some other issues, like IceCat's incompatibility with Flash Player and lack of updates, or Waterfox' shady ownership. And all require GTK3. LibreWolf, the only project with actual potential, has been ~~abandoned~~ resurrected, but still only a few people are involved. The other, more important reason to avoid Firefox-based browsers is that **they are all still dependent**

on the evil Mozilla. If they ever officially cede control to Google (as is already happening in all but name (archive) [MozArchive]) - the whole Internet will be pretty much taken over by an even more evil corpo. I have predicted this in the report above, but it was somewhat speculative at the time. Now, it's pretty much a certainty it will happen in a few years. **UPDATE August 2020**: Mozilla is self-destructing (see above) so a Google owned web might soon become a reality. Knowing this, it is obvious Chrome forks can't be any better, but let us check them out anyway:

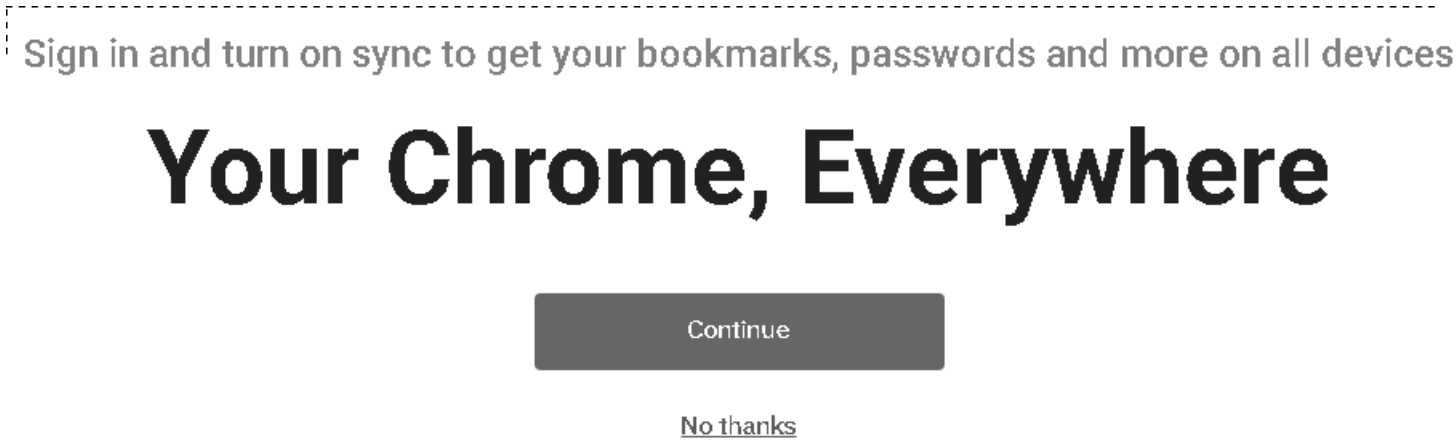
Chrome-based browsers

Google Chrome

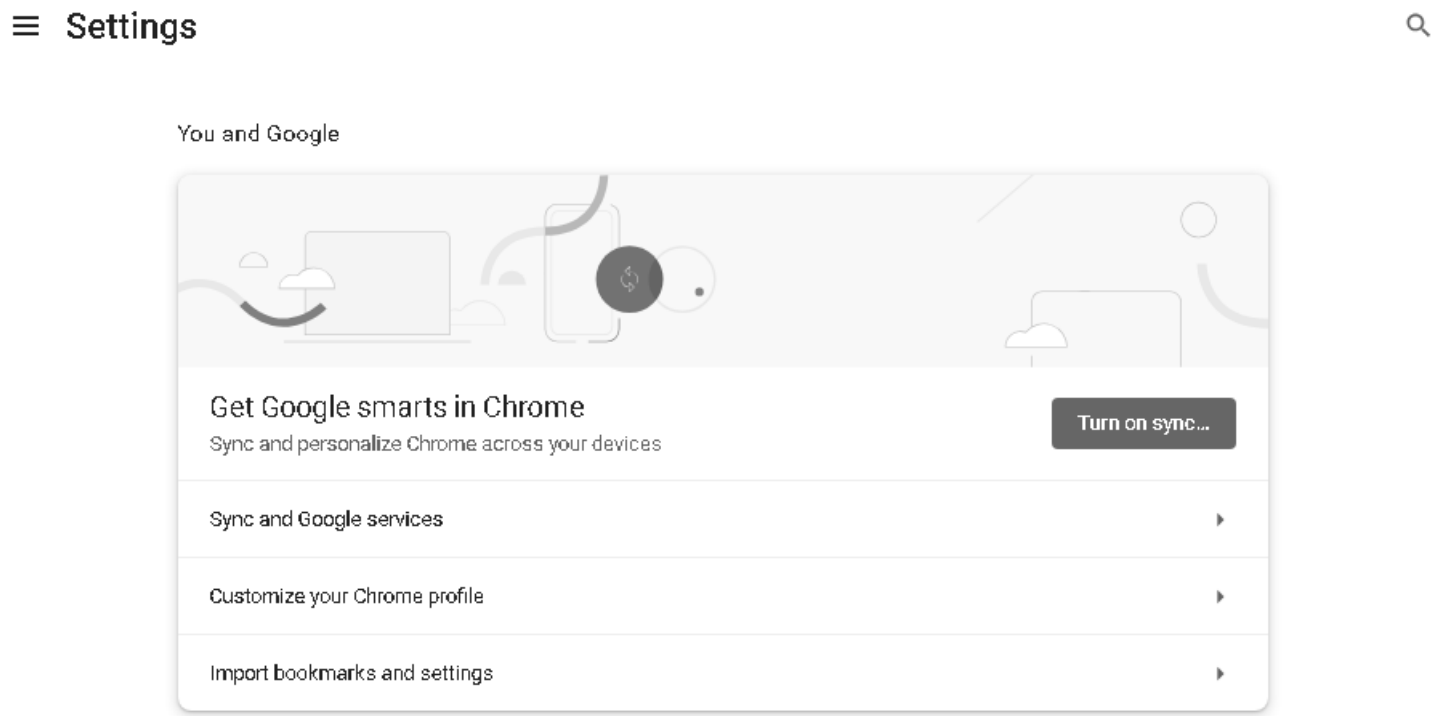
Everyone knows what this is, so let's move on to the specifics. First of all, this browser has quite a few dark patterns. Upon turning on Google Chrome for the first time, a window appears with two options: making Chrome the default browser and enabling the sending of crash reports. Both are on by default:



When you reach the main browser window, you are pestered to login to your Google account:



The same happens when you enter the *Settings* menu:



Yes, that's the Settings menu. To enter the actual settings, you need to click those three lines on top. Anyway, if you do end up logging in, it might be the biggest mistake of your life as Google

will now be grabbing everything (archive) (MozArchive) you do in the browser and connecting it to your real life identity from the Google account:

> *When you're signed-in and have enabled sync with your Google Account, your personal browsing data information is saved in your Google Account so you may access it when you sign in and sync to Chrome on other computers and devices. Synced data can include bookmarks, saved passwords, open tabs, browsing history, extensions, addresses, phone numbers, payment methods, and more.*

It is important to realize just how much privacy you lose this way; for example, you are sending your browsing history to Google, whereas otherwise, it stays local. But, you don't have to use this feature, and then you're left with "only" the heavy spyware Chrome has by default. Google tells you exactly what they do, in excruciating detail, in the whitepaper linked above. Unlike Mozilla, they are actually transparent. But , of course, always confirm everything with mitmproxy. I can tell you one thing for sure: the spying isn't even close to what FF does; there is no equivalent to *Firefox Glean* that monitors every interaction you have with your browser. I don't see three different requests appear every time I click a menu or change a pref in Google Chrome; I can actually modify settings in peace, knowing it's not all sent in real time to Google - with system info, unique IDs and other crap included. Don't be fooled though, Chrome is still heavy spyware, as their privacy whitepaper will gladly tell you. There is so much of it, I kind of can't be bothered to analyze it in detail; just read the whitepaper, if you care. There are many Chrome forks with (some / most / all of) the spyware removed, so we shouldn't spend that much focus here. I'll give a few examples, though:

- Chrome sends an update request on launch, that includes your OS, kernel version, browser version, installation method, bunch of processor info, RAM amount, and

unique ID.

- Chrome sends update requests for what seem to be extensions (even though I didn't install any). These seem to 403 if running through TOR.
- Chrome, like most other browsers, has SafeBrowsing enabled by default, and downloads the lists for it every 30 minutes.
- Chrome still appears to have "recommendations" (ads) in your New Tab page, and has to download them every so often.
- Chrome has Google as the default search engine, and sends every letter you type in there separately to its overlord. Meaning they pretty much know what your thinking process is.
- Chrome has an option to *"Continue running background apps when Google Chrome is closed"* that is enabled by default, suggesting that it does what it says.

For more, read the whitepaper or fire up mitmproxy. When I tried to de-spyware Chrome, I didn't even come close; the waves of update requests still kept coming. Moving on... as you can imagine, the amount of options revealed in Chrome's UI is relatively little. There isn't even the dumpster known as about:config, so it's worse than FF in terms of customizability. The most egregious issue is that proxy settings can't be set through the UI; not only that, but **running Google Chrome through proxychains will error out**. So the only option to set a proxy is an in-built command line option - meaning you **have to trust that Chrome respects the proxy**.

There are no special features in Chrome, it's all going to have to be added through extensions. Keep in mind that due to Manifest V3, certain functions are inhibited and eg. the full version of uBlock Origin doesn't work anymore (in Chrome and all its forks). The amount of RAM usage with one empty tab - in my testing - was 170mb. Though I guess the system configuration

matters somewhat, since others reported 140. GTK3 is required; actually, I had a problem running this browser at all since it seems to depend on several new libs, and I still base on Slackware 14.2. And the errors are kind of unintuitive, but I managed to figure it out, eventually. Since it's big corpo Google, the developer of the most advanced browser engine Blink, you can expect the most compatibility with the modern web out of all browsers. Which I guess is what made Chrome so popular in the first place (aside from being the default everywhere, of course). Well, it was kind of fun testing this, but now I'm going to trash it (still feel kind of dirty). Of course, Google Chrome is still pointless to use, since we have many derivatives that lack the spyware and are fully open source. Check out some of them below:

Iridium Browser

Everything in this browser is the same as Chrome except less data collection and fully FOSS. Billing itself as *"A BROWSER SECURING YOUR PRIVACY. THAT'S IT"*, it actually fulfills the claim aside from a few spyware issues still left in. Specifically, your *"private"* Iridium Browser will make a connection to Big G every 30 minutes to download their Safe Browsing database - what a joke. The devs have reacted dismissively (archive) (MozArchive) to the issue, plus have sneakily added more recent spyware (archive) (MozArchive) - so I don't think they're to be trusted. **UPDATE June 2022**: this browser is slow to update, and has packages only for a few distros (plus Windows and Mac). There's no AppImage or portable build, making installation a bigger problem. This was my browser of choice for a long time (until I found the one below), but it doesn't do anything aside from disabling automatic connections - and not even all of them, at that. If you want a private Chrome-based browser, this one is a much better choice:

Ungoogled-chromium

Unlike Iridium, Ungoogled-Chromium actually disables all automatic connections and other Google integration. The dev is also a really nice and skilled guy (at least he doesn't have a problem with people reporting stuff - unlike Pale Moon, or worse - Mozilla). However, keep in mind the Chromium codebase is massive, and it's doubtful this single guy can keep up for long (then again, he does lift patches from other similar projects such as Bromite, and has a helpful userbase). He's doing better than the Iridium team, though - with his browser being much more up to date. In the end, Ungoogled-Chromium is still just a **bunch of bandages applied to Chromium**, and keeps Uncle G in control of the Web. There are not any real features added beyond the privacy fixes and a few CLI options (archive) (MozArchive). Still, it is surely the best Chromium fork out there if a Google monopoly doesn't bother you. The packages are available only for a few distros (plus Windows and Mac), but fortunately, **there's an AppImage** as well as a portable build that **work everywhere**.

Brave Browser

This browser has made waves thanks to its built-in privacy protections - such as AdBlock, HTTPS everywhere and script blocking - but in the end, they are outclassed by uMatrix. More than that - after checking them out, I can confidently say **the Shields are pretty useless** - the vast majority of trackers are left alone; in fact, sometimes it seems that a site can have hundreds of them, and yet none of them will be blocked by the Shields. Script blocking option simply blocks JavaScript fully - it's just NoScript revisited. Brave used to be able to install Chrome extensions only from source, but now does it the same as the other Chrome-based browsers. Despite those, it not only spies on you (archive) (MozArchive) but is **actively working against**

your privacy by whitelisting Facebook and Twitter trackers. Brave has also been soliciting donations in the name of other people **without their consent**!

Here (archive) (MozArchive) is a thread discussing the issue. **UPDATE August 2020:** since I wrote this, more shady shit from these guys has surfaced. For example, not only do they have sponsored backgrounds (archive) (MozArchive) (recall Mozilla's Directory Tiles?) in their New Tab page but they were also earning big money (archive) (MozArchive) from the included affiliate links without telling you (this is illegal and they've locked the convo as expected)! More recently, they were caught rewriting typed web addresses (archive) (MozArchive) to add

referrals for various partners. Brave Browser also has auto-updates (archive) (MozArchive) that **cannot be disabled** which is extremely malicious (complete with a closed topic, of course - in a Mozilla-esque fashion). The only real reason to use Brave is their so-called *"Brave Rewards"* program with which you can earn their *"Basic Attention Tokens"* in exchange for watching ads (displayed as system notifications). Here's the catch: to pay out their BATshit tokens, you need an account on Uphold, whose Privacy Policy (archive) (MozArchive) states this:

> *To verify your identity, we collect your name, address, phone, email, and other similar information. We may also require you to provide additional Personal Data for verification purposes, including your date of birth, taxpayer or government identification number, or a copy of your government-issued identification*

Facebook tier surveillance. But wait, it's not over:

> *We may obtain information from affiliated and non-affiliated third parties, such as credit bureaus, identity verification services, and other screening services to verify that you are eligible to use our Services, and will associate that information with the information we collected from you.*

They will also stalk you all over the Internet to try to find already existing information. There are still more violations coming, so sit back and watch:

> *Uphold uses Veriff to verify your identity by determining whether a selfie you take matches the photo in your government-issued identification. Veriff's facial recognition technology collects information from your photos that may include biometric data, and when you provide your selfie, you will be asked to agree that Veriff may process*

> *biometric data and other data (including special categories of data) from the photos you submit and share it with Uphold. Automated processes may be used to make a verification decision.*

As soon as I thought I've found the biggest privacy violator possible, the cold hammer of reality struck that stupid idea right out of my skull. Anyway - again - **the only way to pay out BATshit tokens is by using this service**. Even then, you can only do it once a month and Brave still swipes 30% (archive) (MozArchive) of it - *"You'll earn 70% of the ad revenue that we receive from advertisers."* This is portrayed as a way of revolutionizing the Internet ad industry - *"the middlemen and platform operators capture most of today's ad revenue, while creating malware distribution and ad fraud opportunities. Brave Rewards upends this broken system and provides a new way forward for creator support."* However, the real revolution will happen when the whole ad business model is dead and buried, or even better - when content creators don't need to worry about "earning a living" because the capitalist monster has been slain or at least put on a leash. For now, you can just support the sites you like directly with Bitcoin (or better - Monero), anonymously and on your own terms. All you need is a wallet and a person you want to donate to. Anyway, at the beginning I was way too forgiving for Slave (certainly nothing *"Brave"* about it) Browser - let it rot along with all the scams they're pulling.

Dissenter Browser

This Brave fork was whipped out in literally a few days in response to the recent wave of censorship from Twitter, Facebook, Mozilla etc. Its claim to fame is being integrated with the Dissenter extension (banned from Firefox's and Chrome's extension stores (archive) (MozArchive)) which allows you to comment on any article from any website, bypassing their

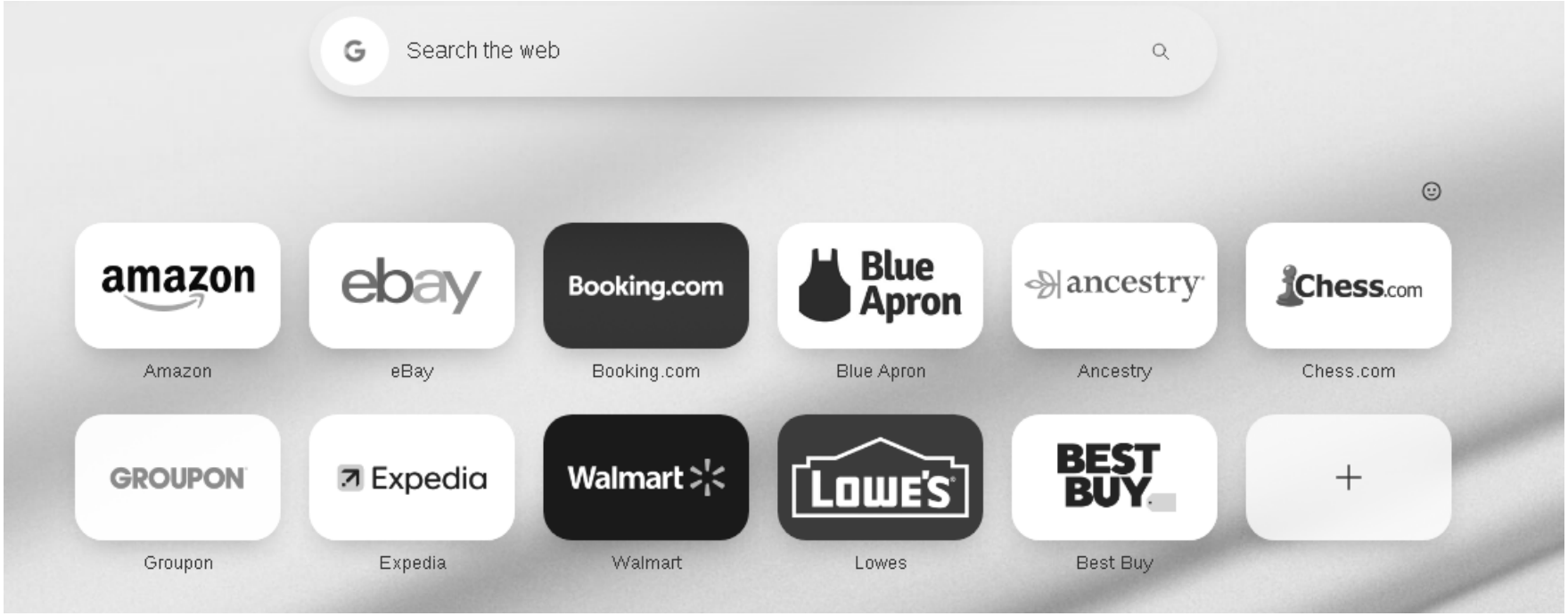
censorship policies. Quite handy. To use it, however, you need to sign up for their social network, which **requires ReCaptcha** (devs have dismissed the issue (archive) (MozArchive)). Then, to post a comment, you of course have to share the site you're on with Dissenter, which - if used extensively - could **build quite a profile of your browsing history**. Who's to say they won't run away with all that data then? Their privacy policy (archive) (MozArchive), consisting of one fucking sentence **says literally nothing about what they collect and share**, so you might assume it's everything with whoever. As for the browser, it contains the usual Brave shit like Shields, whitelisted trackers and safebrowsing. In addition to those - whenever you open a new tab, Dissenter will connect to a bunch of news sites and youtube, as well as clearbit to download their icons; fortunately, this can be disabled. Their site is also cloudflared, which means **all your history and comments will be shared** with the evil tech giant (archive) (MozArchive), MITMing from the shadows. All in all, this browser is just a fad riding on the current anti-censorship climate. In fact, I'd say it's very likely a **honeypot designed to collect the browsing and comment history** from as many people as possible and share them with the great centralizer (Cloudflare), to help eventually create an Internet that is fully controlled by the so-called "elites". The idea is nice (and I hope someone worthy repeats it) but the execution could not have been worse. **Run the fuck away** faster than you would from an angry, rabid dog! Speaking of dogs, the Spyware Watchdog has an in-depth review (MozArchive) of some other issues with Dissenter.

Opera

UPDATE July 2023: I did some testing (as you could have guessed :D). 83 requests at launch to various Opera and Google domains. There is nothing like *Firefox Glean* that monitors your entire browser activity, so at least it seems you can change settings, etc in peace. But, Opera has

a spyware feature that is **probably the most violating in existence**, namely that it sends every website you visit to itself (through the request *sitecheck.opera.com*), collecting your entire browsing history (fortunately, you can disable this). Even though Opera has recently whined (archive) (MozArchive) about being called a spyware, nothing has changed; the amount of unsolicited requests at launch is even exactly the same as all those years ago (archive) (MozArchive).

This browser has a lot of features, and has included many new ones since I last tested it. Integration with spyware platforms like WhatsApp and Telegram is still there, but also ChatGPT as a recent addition. A "VPN" that is probably a Chinese honeypot since Opera is now owned by a Chinese company. Automatic currency conversion, built-in adblocking (but not enabled by default; the acceptable ads list is automatically downloaded from Adblock Plus and reports your browser). Wallpapers, cryptocurrency integration (I'd be wary of using this, but didn't test in depth), IPFS, many many more things I didn't even look at; even has weather reporting in its new tab page which of course sends your location. And a bunch of ads (these are **location-aware**):



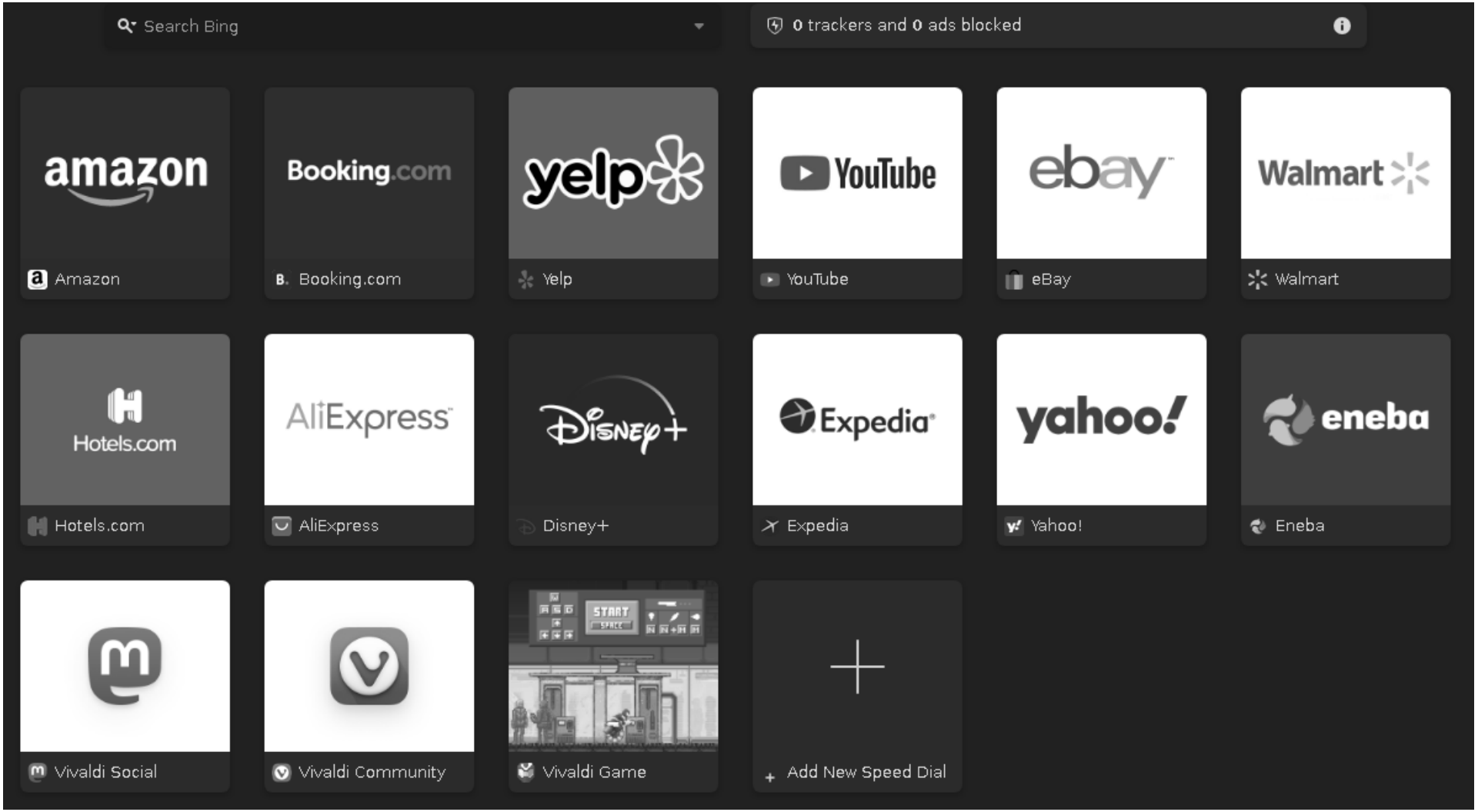
By default, it does the same crap as Google Chrome in sending every letter you type to its search engine live. But it's modifiable and you don't even have to use Google as the search engine - though the defaults are disgusting, and they matter. I don't really like this browser; it's really heavy spyware and isn't even open source - but does contain many many features not found elsewhere that will surely appeal to some. Uses 260 mb RAM with one empty tab; requires GTK3 like all Chrome-based browsers. Hey, WebRTC can be nicely disabled from the settings menu, which is a positive, I guess; but again, the default sucks. In the end, you have to stack the features against the spyware and the lack of source code; for me, Opera is still in a losing position since extensions can replace many of the features, while the spyware remains. Hey, I even tried to disable all the spyware just to be charitable, but **it's not possible**. There are still auto-update requests at every Opera launch, requests to Google for some updates, requests to download the location-aware ads with a unique ID attached, and even a TCP request to *mtalk.google.com*. Sorry, but your features are not enough to save you from being a violator.

Vivaldi

UPDATE July 2023: It's time for another checkup at the examination table for Vivaldi. Privacy-wise, it's still doing this crap (archive) (MozArchive):

> *When you install Vivaldi browser ("Vivaldi"), each installation profile is assigned a unique user ID that is stored on your computer. Vivaldi will send a message using HTTPS directly to our servers located in Iceland every 24 hours containing this ID, version, cpu architecture, screen resolution and time since last message.*

As well as sending a bunch of requests to Google to update its extensions right at launch (but hey, I don't have any extensions yet - so what's the justification for it?). Also uses Google for the Safe Browsing threat list downloads every 30 minutes, as many other browsers thoughtlessly do, too. When you finish Vivaldi's setup wizard, it tries to load its start page, which is behind Cloudflare. If you're running Vivaldi through TOR, the CF page will refresh in perpetuity, and never let you in while it keeps making requests - what a blunder! No matter, I don't care about its shitty start page, let's check out some other things. Like the New Tab page being full of crap by default:



You can delete all this, but why should you have to? Let us set up our New Tab pages as we want to - without having to take out the devs' trash first. I can understand having the Vivaldi links in there, but why the others? Moving on to Vivaldi's actual features, let me repeat what I've said three years ago:

> *It's still the most featureful browser out of the box (mouse gestures, screenshots, web panels, notes...) and boasts massive amounts of customizability (in regards to tabs,*

bookmarks, keyboard shortcuts that no other browser can change by default)

Now you can add themes, menu positions which are fully modifiable (very good feature that more software should implement), in addition to the above. Though, it lacks gimmicks like Opera's ChatGPT, so I'm not even sure it's the most featureful now. Bing is the default search engine except for private windows, which use DuckDuckGo (is this an admission that they are violating the users' privacy in the non-private windows? haha...). Many many options, in terms of how it all works, that I don't care about that much, since I won't use this browser. The spyware and shitty defaults (even a PDF reader is enabled) simply take precedence over anything good it might have in terms of features. It also doesn't release the full source code and the phoning home every 24h can't be disabled.

Vivaldi also brings along a mail client and a RSS reader, which I didn't test at all. RAM usage clocks at 290mb with one empty tab. Again, many people will like its features - but they do not cover the other flaws. And most of those are replacable by extensions, anyway (even Pale Moon has a mouse gesture extension). I do like some of the things it's doing though, and wish they could be picked up by others - like the movable menus and modifiable keyboard shortcuts. But it's not enough considering the spywaristic and babifying defaults. Translation offers will even appear when you visit a foreign web page; holy shit, I hate all kinds of pop-ups! Whether they come from websites or the browser itself. Let the user choose when they want to do something.

Also, I have to mention one more thing that really annoys me. It seems that the font sizes for the browser UI itself can't all be modified, so if you sit far away from the screen and use a big font (like I do), you'll have to come near to read the tiny font every so often (like every time you right click). Even if this browser was otherwise perfect, this one flaw would truly ruin

everything, ugh. Anyway, there is clearly some potential in this browser, just brought down by a few bad choices / maybe lack of polish or general care. Minimalists won't like it, either.

Summary

The situation with Chrome forks is better than Firefox ones - there are more of them and they are more commonly updated. We've got more variety in terms of features, included addons, looks (though all require GTK3), philosophies, etc. But something seems to be missing. The ones with more features introduce their own problems such as custom spyware, false advertising, lack of ethics, even less speed, or crashes. The ones removing all the spyware don't introduce anything new. And they all still rely on the Blink engine (and thus Google). And since Google keeps including anti-user changes (archive) (MozArchive), the forks will have to remove / modify those in the code, which some of the smaller teams might not be able to eventually keep up with. **UPDATE January 2026**: I don't care that much about browsers anymore, but just thought I'd tell you that **none of the Chrome forks** ended up resisting Manifest V3. Though Brave hosts forks of four of the affected extensions, it's set to give them up (archive) (MozArchive) - *“This feature will be best-effort: we might have to modify support based on either Google’s plans or what extension authors ultimately decide to do. If extensions become stale or obsolete, we may remove support for them” [...]* at some point. The rest simply fully cucked. **All journalists that talk about "browsers that still support manifest V2"**, or similar things, are misleading you. None of them are commited to actual lasting support; it's either "until Google finally pulls the plug", or "we have an in-built replacement" (but the affected extensions still don't work). Do you now see the problem with relying on a protocol / language / engine controlled by Google (plus its allies Microsoft, Apple, Mozilla, which work together in all major decisions)? What if Manifest V4 is even worse than this? Are we **really** stuck with

desperately trying to patch up the big corpo abominations?

The Fallen Hero - Pale Moon

It used to be **fucking good** - and still has several advantages over FF / Chrome such as independent development, lack of some antifeatures, less vulnerabilities (archive) (MozArchive), XUL addons support, better UI (also the only one that can use GTK2 instead of 3), smaller codebase, and more customizability. **UPDATE**: oh, and it consumes only 100MB RAM with one empty tab. I also want to compliment it on having very little spyware (which sounds funny, when the default in software should be **no unsolicited requests** - but in this fucked world, we have to take what we can get). On launch, Pale Moon connects only to its start page, which is Cloudflared and blocks TOR, so I couldn't reach it anyway - lol. That's nine requests. A while later come the requests for the addon blocklist and the update check. That's it, and it can all be easily disabled. Funnily, it seems **none of those requests end up doing anything if using TOR**, because CF denies them. This sounds like quite the significant flaw, preventing browser functionality because of your attitude towards anonymizing networks. Before we move on to other issues, please realize that this browser is still miles ahead of any of the other major ones due to having actual customizability, XUL addons, not being chained to big corpos (as much as the others, at least), GTK2 support, and actually disabling some "modern" things on purpose. However, it recently went off the deep end so much that I cannot in good conscience call it an "alternative" to anything anymore. Let me give some examples:

- Blocking the AdNauseam extension (archive) (MozArchive) due to allegedly causing *“economic damage”* to websites. But actually, it's the ads and trackers that are causing human damage (archive) (MozArchive) and if extensions such as AdNauseam help kill

the "economy" based on them, they should be praised instead of banned. Re-enabling AdNauseam requires fiddling with about:config.

- NoScript was another extension added to the blocklist with the "rationale" that it breaks sites (that's how it achieves its security and other benefits - same as uMatrix or adblockers). There is a big scary warning (archive) (MozArchive) but fortunately, you could still use the extension.
- Pale Moon's website (including the addon search integrated into the browser) is behind the evil Cloudflare MitM. The CF-loving lead dev thinks it's fine (archive) (MozArchive) for people to be violated by CF without being notified (or worse, a way to **resist**) and goes around sharing that message.
- He also hates the TOR network (archive) (MozArchive) because the people using it dare to protect their identities or stand up to their oppressive governments.
- A contributor created a backup of Mozilla's XUL docs (MozArchive) (that they want to delete in December 2020) and got dubbed an insect (archive) (MozArchive) for it by Tobin, the other main developer.
- He is also insulting long time contributors (MozArchive) even in commit messages for petty reasons (archive) (MozArchive).
- They both have hounded the OpenBSD packagers (archive) (MozArchive) because they wanted to use system libs which would be *“deviating from official configuration”* - something the PM devs hate. They also hardcode compiler parameters, especially with libvpx to use specific opcodes instead of using whatever the user or operating system sets ${CFLAGS}/${CXXFLAGS} to, breaking portability with different CPUs and operating systems.
- Pale Moon now has WebAssembly enabled by default (archive) (MozArchive), the whole point of which (archive) (MozArchive) is pushing cancer such as *“AAA games*

that have heavy assets”, *“VR and augmented reality”* and *“Live video augmentation”* onto web browsers. Talk about scope creep! It pretty much turns your web browser into another operating system since it's literally assembly to which you can compile other languages and run all kinds of "apps". Of course, you can imagine all the new security vulnerabilities coming along with that. And just a year ago it was a not recommended technology (archive) (MozArchive) ...

- And the icing on the cake - they've now started forbidding direct addon downloads (archive) (MozArchive) - much to the dismay of many (archive) (MozArchive) users (archive) (MozArchive). Tobin has called wanting to actually have control over your extensions *“obsessive packrat tendancies..”* and Moonchild followed with *“hoarding addiction”*. Now contrast that attitude with the quotes on their main page - *“Your browser, Your way”* or *“offering full customization”*. Doesn't this sound familiar?
- **UPDATE Nov 2020**: the straw that finally broke the camel's back - the **removal of global custom user agent**. Whereas the other malicious changes can be kind of justified with some twisted reasoning, this one is absolutely impossible without going directly against Pale Moon's stated goals, such as customization (the main page mentions it **three times**). See, Moonchild thinks (archive) (MozArchive) that the global override is *“a terrible Web Compat footgun”* that the users shouldn't have access to. Of course, it's somehow fine to allow UA setting per site or request, despite it being terribly inefficient. Even then, a **global custom UA actually helps web compatibility** by sneaking past those UA-sniffing sites (which will not stop existing anytime soon). All of this is besides the point though - what matters is that **the users should be able to shoot themselves in the foot** if they so desire, and this recent change goes against that. For honesty's sake, let me say that Moonchild reverted the change - but only because of the huge backlash (archive) (MozArchive) on the forums. The fact that this was an idea in

his mind for even one second proves he **doesn't give two shits about freedom, customizability, or user respect**.

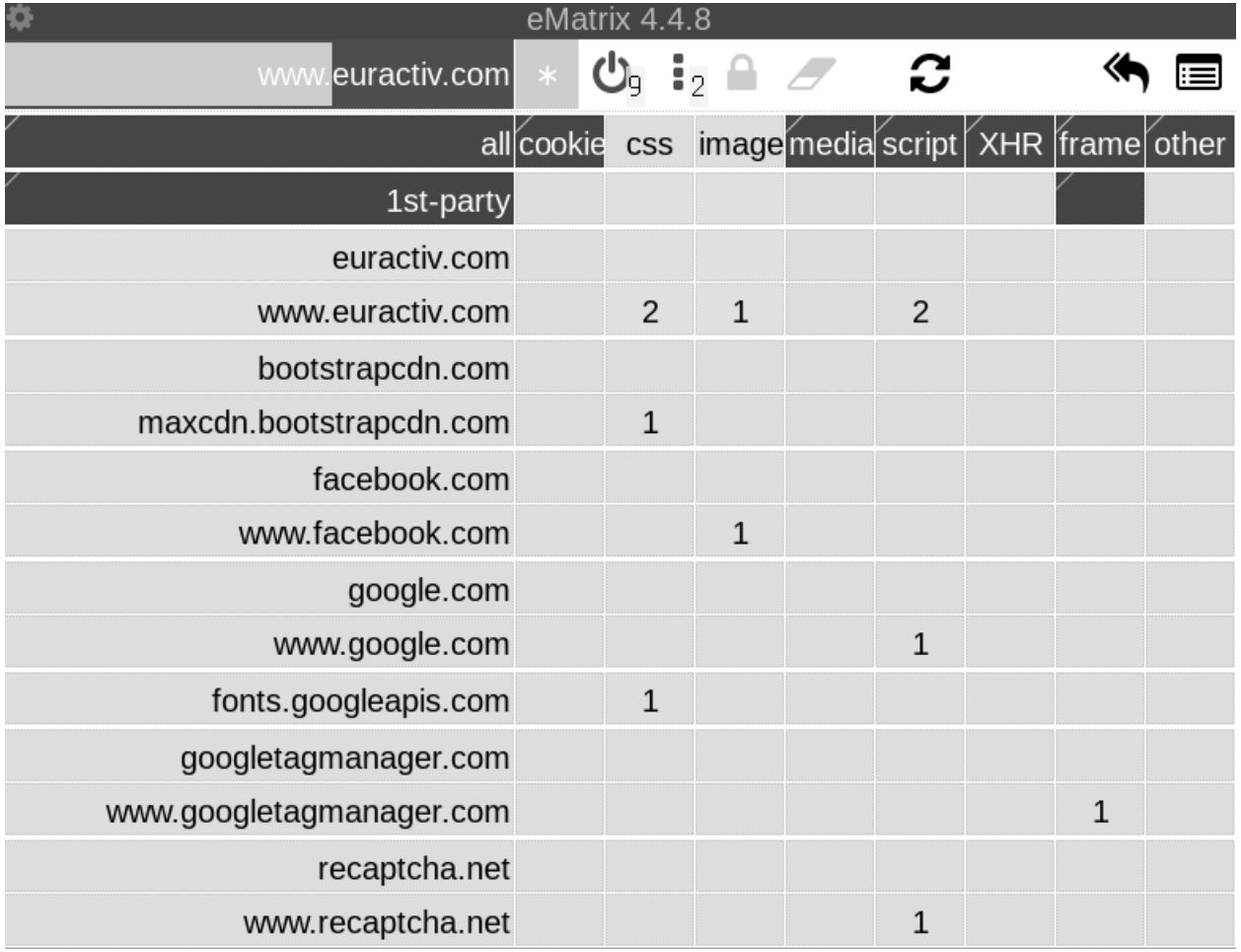
- **UPDATE April 2021**: so I called Pale Moon a *"sinking ship"* some time ago. I hate to be the bearer of bad news but it's clear it has actually sank now. The reason? You cannot install (archive) (MozArchive) extensions from the Classic Addons Archive anymore - just because Sensei Moonkid decided so. Hope you got out in time!
- **UPDATE March 2022**, Tobin left (archive) (MozArchive). Is this the event which sends Pale Moon to the grave?
- **UPDATE March 2023**: Pale Moon addons store is now Cloudflared, and you cannot install extensions through TOR (**2026 edit**: not anymore). Sure, Moonchild, go ahead and kill your browser if you're so eager to do so.

And with that, it's obvious that **Pale Moon is a sinking ship**. A few months ago I've said that the browser is in the *"beginning stages of degradation"*. Now, the stage is clearly advanced, the cancer has metastasized and cannot be removed anymore. Pale Moon **has become exactly what they've fought against for so long - Mozilla-lite**. It's still a good enough piece of software (and the only decent one for browsing the modern web) - but one I **cannot recommend anymore** due to violating the most important principles (which for years have defined it). **UPDATE February 2022**: this used to contain a recommendation for *Web Browser*, a Pale Moon fork - but it's pretty much abandoned and the lone developer never went far enough with mitigations, anyway. Therefore I'm deleting the section but you can still check out the project here.

Why "minimalist" browsers suck

Since many people have asked me to review their favorite "minimal" browser, I will just cover

them all in one fell swoop. By default, a browser will load all the content that it supports, including cookies, scripts, CSS files, frames and videos. The majority of modern websites rely on lots of third party stuff which is either useless to display the website, or can track you. Here is an uMatrix grid of Euractiv:



all	cookie	css	image	media	script	XHR	frame	other
1st-party								
euractiv.com								
www.euractiv.com		2	1		2			
bootstrapcdn.com								
maxcdn.bootstrapcdn.com		1						
facebook.com								
www.facebook.com			1					
google.com								
www.google.com					1			
fonts.googleapis.com		1						
googletagmanager.com								
www.googletagmanager.com							1	
recaptcha.net								
www.recaptcha.net					1			

In an unmitigated browser, all the tracking scripts, CSS and images will be loaded - sending your data to Facebook, Google and others - and also slowing down the loading times. This is

despite the fact that the site works perfectly well without any of that stuff. It does look ugly though, and enabling the bootstrap CSS file fixes it. And here we encounter the problem with all minimalist browsers - **they cannot block stuff they load per domain**. Either they load everything from a certain category (that is, if they even support it) or nothing. So, in such browsers, if you wanted to make Euractiv look as it is supposed to, you'd have to enable all CSS - including the tracking ones from Google.

Let's look at suckless surf. You can run it with options that tell it to disable images or scripts. Disabling images means you will see pure text, enabling them shows all the images including the 1px tracking ones from dedicated spy corpos. A site could have one image needed for understanding the content, and 10 tracking ones; or one script needed to run the site and 10 advertisement spreaders, crypto miners, etc. - **and the minimalist browsers can't distinguish**. The only tool that can do so, is uMatrix - and **the only browsers that support that are the fat ones**. With minimalist browsers, **you have to choose between functionality and privacy / speed** - uMatrix gives you both. And that is why minimalist browsers suck, my friends. The only time I'd recommend them would be if you only visit sites that make no third party requests. This used to be common in the early Internet, now it is almost unheard of.

Don't get me wrong, the minimal browsers **do have advantages**. They usually don't spy on you (no unsolicited requests), they are more configurable (having keybindings by default, for example), they lack some antifeatures, sometimes they have their own engines so don't depend on big corpos, take up much less disk space and use less CPU / RAM etc. However, most of the evil of the web comes from the websites themselves. And the only tool that can handle that properly is uMatrix, which the minimal browsers don't support. And unfortunately, that one single disadvantage overshadows all other advantages these minimal browsers might have. This isn't going to change, either - sites are not suddenly going to become minimal - which would

have to be the case for these minimalist browsers to be viable. Of course, the "major" browsers will eventually become even worse, "modern" websites even more bloated and malicious. Therefore, long term, we will need to create our own web which is usable with minimal browsers. I have written this article with the assumption that engaging with the modern web is still necessary and / or worth it for the reader. Since even the minimalists still keep around a modern browser for certain websites, I am trying to show the best / least harmful way of doing so. And that - in my opinion - is still Pale Moon with the proper addons.

UPDATE November 2022: qutebrowser is somewhat of an exception, since it does have jMatrix available (CF warning). You can lift a config file from uMatrix / eMatrix and just drop it there; there is no graphical UI / grid for fixing sites though. I have no experience with it but someone told me it works. But not all of it, apparently:

> *Right now, all we do is block incoming requests. uMatrix does a bit more than this, such as spoofing noscript tags when js is blocked. It also means we cannot block cookies (so those rules will be ignored).*

It is possible to block third party (or all) cookies in qutebrowser, but you lose the per-site functionality of uMatrix / eMatrix, then. **Note**: qutebrowser isn't quite "minimal" either way, being dependent on the Blink (Chrome) engine. Just know what you're signing up for.

Summary

Pale Moon is still the only decent way to browse the modern web that's actually relevant - but **it's slowly rotting from the inside**. Firefox is dying and will soon bring down all its forks

alongside itself, surrendering the Web to Google whose abomination of a browser is just as worthless. Promising projects such as Otter Browser or suckless surf suffer from small dev teams, no / low addon support and don't have their own engines - so depend on Google / Apple, anyway. The only reasonable choice is Pale Moon. Or, just try wean yourself off the modern web by sticking to websites such as the ones on Neocities, wiby.me, etc. which are functional in NetSurf or terminal browsers. I hate to kill the positivity of yet another summary, but if reality forces me to - what can I do?

Browser / Feature	Spying	Engine	Extensions	GUI library	Source code	RAM usage
Mozilla Firefox	High	Gecko	WebExt	GTK3	Yes (Full)	~260MB
GNU IceCat	Mild	Gecko	WebExt	GTK3	Yes (Full)	~300MB
LibreWolf	Mild	Gecko	WebExt	GTK3	Yes (Full)	~260MB
Waterfox	Medium	Gecko	WebExt	GTK3	Yes (Full)	~300MB
SeaMonkey	Medium	Gecko	XUL	GTK3	Yes (Full)	~120MB
TOR Browser	Mild	Gecko	WebExt	GTK3	Yes (Full)	~260MB
Google Chrome	High	Blink	WebExt	GTK3	No (or not full)	~170MB
Iridium Browser	Mild	Blink	WebExt	GTK3	Yes (Full)	~170MB
Ungoogled-chromium	None	Blink	WebExt	GTK3	Yes (Full)	~170MB
Brave Browser	Medium	Blink	WebExt	GTK3	Yes (Full)	~170MB
Dissenter Browser	Medium	Blink	WebExt	GTK3	Yes (Full)	~170MB
Opera	High	Blink	WebExt	GTK3	No (or not full)	~260MB
Vivaldi	Medium	Blink	WebExt	GTK3	No (or not full)	~290MB

Pale Moon	Mild	Goanna	XUL	GTK2	Yes (Full)	~100MB

RAM listings are rough, do not take them as gospel, just take note of the ratios with a grain of salt.

Compatibility at all costs?

During the writing of this entire article, I have made a certain assumption. That browsing the modern web is worth it and a browser must have full compatibility with it. But maybe it is this assumption that needs questioning in the first place. When you have this requirement, you suddenly become dependent on one of the big evil corporations (Apple, Google or Mozilla) - which are the only ones who have enough manpower to be able to sustain the engines that support the web standards fully. In fact, the standards themselves are now unashamedly controlled (archive) (MozArchive) by the same corporations that develop the major browsers. No conflict of interest there, at all. Of course, the goal is to make the standards so complex that an independent browser developer cannot stand a chance of implementing them, and so the internet user must settle on one of the big corpo browsers. The Pale Moon devs tried to avert this, but did not manage to do it completely, so compatibility issues still exist with some sites. But is this actually a disadvantage?

The websites have gotten way too complex for their own good, and we shouldn't seek full compatibility with them. I was hoping really hard that the Pale Moon devs would go against the trend of including everything possible and at least deny WebAsm, but of course they ended up cucking. It's not just WebAsm, either; new standards include a lot of complicated stuff that's useless, violates privacy (e.g CSS media queries (archive) (MozArchive)), makes websites

slower, kills compatibility with older browsers and / or makes code way harder to understand for someone who wants to learn web development. I mean, you can't honestly tell me that this abomination (local) is somehow desirable! During the development of modern web browsers, no one bothered to ask himself - what do we want them to actually do? No, everyone just jumped into the feature train, rode full speed ahead and rammed into a brick wall. Now all that remains from the Web is a pile of rubble from the crash.

But the train's still chugging along. Those corporations won't hold themselves back and will keep inventing more crap. Since they control both the standards and the major browsers, webdevs feel no inhibitions in including all the new technology on their sites. A popular VPN company even told me in an E-mail that they *“won't support those outdated browsers”* - refering to Pale Moon, which despite being separate from the Google / Mozilla duopoly (really a monopoly), is still a modern browser. One way we can attempt to fix the situation is by making sites that promise to be compatible with all browsers (archive) (MozArchive). However, I feel like these days, that might be not quite enough. That site itself appears quite dated in that it refers to Netscape and IE as if they were still the top dogs. A regular person will also probably misunderstand the campaign since they assume "all browsers" just means Chrome, Firefox and perhaps Safari. Eventually we have to say "no!", and start making and using browsers that are less compatible (support less new crap) on purpose (and not just because we lack manpower to reach the ideal of full compatibility). This will also put pressure on webdevs to design their websites more sanely. Again, I thought Pale Moon might have been that browser, but it didn't turn out that way.

What should be supported and what should be discarded? I don't know. That remains to be decided - but no one even asks that question today, believing full compatibility with big corpo standards to be the unquestionable ideal. I cannot anymore pretend that that is the case, though,

and that minor browser differences are a big deal. And compared to the compatibility issue, every other feature is minor. Today's "minimal" browsers are not even "minimal" - they just lack an UI and extension support, with the decidedly not minimal Blink or Webkit under the hood. Sometimes people mention NetSurf as a viable alternative; forget it - despite being independent, it blindly hopes to absorb (archive) (MozArchive) the entirety of WhatWG's abomination:

> *There are many web standards. HTTP, HTML and CSS are just a few of them, and new specifications appearing all the time. The NetSurf team is devoted to implementing these standards.*

On the other hand, a truly "minimal" browser would proudly reject useless modern "features". NetSurf doesn't care and already includes the CSS spy queries, for example - with the other stuff coming up. If you are dead set on the modern web, Pale Moon is still the best option available. But long term, our only option is a rejection of the modern web and the creation of our own, at least if sanity is a goal. I will still leave up this comparison of modern browsers, since there are significant enough differences to warrant consideration. The section Why "minimalist" browsers suck still applies, since "minimal" browsers only work for a "minimal" web.

Back to the front page