

Mozilla - Devil Incarnate

- Introduction -
- Mozilla's pretend privacy -
- Mozilla's privacy policy -
- Firefox privacy policy -
- "Lean data" is yet another fraud -
- Firefox account - the master spy tool -
- Hidden tracking with link shorteners -
- Privacy-preserving advertising? -
- Anti-privacy nonsense backfires -
- Firefox will feed your data to AI? -
- Freedom is slavery -
- History of anti-control -
- XUL deprecation -
- Forced updates -
- Bypassing proxy settings -
- Supporting censorship -
- Cucking to Manifest V3 -
- People before profit? -
- Analyzing Mozilla's finances -
- Advertisements in your browser -

- Pocket integration -
 - ProtonVPN partnership -
 - Mullvad partnership -
- Bribing distros to include spyware in their default settings -
- Shady marketing -
 - Blog post analysis -
 - The users have spoken -
 - Summary -
- Shitty developer attitude -
- JavaScript toggle removal issue -
 - PulseAudio enforcement issue -
- Long-time volunteer DISRESPECTED AND BANNED -
- Summary -
- Refuting the manifesto -
- Principle 1 -
 - Principle 2 -
 - Principle 3 -
 - Principle 4 -
 - Principle 5 -
 - Principle 6 -
 - Principle 7 -
 - Principle 8 -
 - Principle 9 -
 - Principle 10 -
- Mozilla's doublespeak -

- What would Mozilla do -
- Mozilla's Endgame -
- Cloudflare partnership -
- DNS over HTTPS -
- Firefox Private Network
- Sacrificing readers at the Cloudflare altar -
- Second head of Google -
- Other "giants" -
- The Hydra -
- Consolidation of power -
- The RSS deprecation conspiracy -
- Summary -
- The death of Mozilla? -

Introduction

If you haven't been living under a rock for the last decade or so, you will at least know Mozilla as the developer of the popular Firefox web browser. Of course, if you've been reading this website a little, you'd guess that **there is a darker story behind Mozilla**. There is no bigger example of a corporation pretending to be your friend while being your worst enemy. And you don't have to dig too deep to prove it (but we will in this article!) - just get past the skin-deep veil of Mozilla's deception and you reveal a greedy, controlling, sneaky, deceptive, abusive, data hoarding, disempowering, doublespeaking, vile **spawn of Satan**. So what makes Mozilla different than Google, Microsoft and such? Well, it's the **facade**, of course; they campaign against all the sins they themselves partake in! And it is this facade which I will smash in this

article, little by little...

Mozilla's pretend privacy

First, the facade - let me show you some quotes and article titles from Mozilla's website:

“Fast. Private. Fearless.” (this is about Firefox)

“Your Privacy Focused Holiday Shopping Guide”

“Latest Firefox Rolls Out Enhanced Tracking Protection”

“When the Facebook breach was revealed, Mozilla had an immediate response – and a Firefox product to support user privacy.”

“Individuals’ security and privacy on the internet are fundamental and must not be treated as optional.”

“In our Webby-winning podcast, IRL, Veronica Belmont gets real about the online issues that affect our real lives, from privacy and filter...”

There is much, much more. That's not even considering the stuff inside their browser, such as the fake initiatives Do Not Track and Private Browsing. If you only saw these quotes, you'd think they must be some champions of privacy; nothing could be further from the truth, though. OK, now let's move on to the fun part - busting the facade! For that, we have to direct ourselves to their website privacy policy (archive) (MozArchive) as well as general privacy policy (archive) (MozArchive):

Mozilla's privacy policy

We care about your privacy. When Mozilla (that's us) collects information about you, our Mozilla Privacy Policy describes how we handle that information.

They are shameless - still trying to keep up the facade even when the same document refutes it later.

We may also use cookies, device information and IP addresses, along with clear GIFs, cookies and third party services [...]

Clear GIFs - that's a common tactic of trackers ([archive](#)) ([MozArchive](#)) (“Website owners use tracking pixels to track visitor behavior, including page views, time spent on the site, and interactions with specific elements.” - so they now recruit others to spy on you as well. Moving along, Mozilla now has its own analytics service:

Mozilla Glean, our first-party telemetry and analytics platform.

I don't know when they've installed it, but you'd think they did it because they wanted to ditch Google Analytics, which is what many other sites do. But no; in their quest for as much data collection as possible, they still have that:

Google Analytics, which places a cookie on your device, to obtain metrics on how users engage with our websites. This helps us to improve site content.

Anyway, let's continue:

Mozilla has implemented third-party technology, Google's Invisible reCAPTCHA [...]

Google is one of the most anti-privacy companies that exist; and here Mozilla is allying with them - proving they are made of the same mold. The really vile thing here is that since the captcha is invisible, you will have your data collected by Google and you won't even know it's happening. Okay, let's move on to the regular privacy policy, which describes how the data gets used:

Your privacy is an important factor that Mozilla (that's us) considers in the development of each of our products and services.

Still continuing the pretense? Anyway, let's check out the section “*when do we share your information with others?*”

For processing or providing products and services to you, but only if those entities receiving your information are contractually obligated to handle the data in ways that are approved by Mozilla.

So, Mozilla is sending your information around to some unknown “*entities*” - but it's fine, since they are obligated to handle the data in a way that Mozilla has approved (does that fill you with confidence after reading the above quotes?).

When we are fulfilling our mission of being open. We sometimes release information to make our products better and foster an open web, but when we do so, we will remove your personal information and try to disclose it in a way that minimizes the risk of you being re-identified.

So, you “*release information*”, but it's fine since you “*minimize the risk*” of me being

identified? Well, “*minimize*” means it's still not zero, so fuck off with that excuse.

When we believe it is necessary to prevent harm to you or someone else.

That can mean absolutely anything. So just expect your information to be thrown around for any reason! Hey, it gets even worse:

If our organizational structure or status changes (if we undergo a restructuring, are acquired, or go bankrupt) we may pass your information to a successor or affiliate.

Not even death is a barrier for the spy masters. Also check this:

We also don't want your personal information for any longer than we need it, so we only keep it long enough to do what we collected it for. Once we don't need it, we take steps to destroy it unless we are required by law to keep it longer.

Can they be anymore vague? There is no mention of a specific timeframe, so we're left to guess just how long they keep your data for. And seeing how much regard (read: zero) Mozilla has so far shown for your privacy, we can safely assume it's longer rather than shorter. And lol at the “*we take steps*” - why not just say "we destroy it" if you actually do so? You'd only say “*we take steps*” if you don't intend to actually finish the job. Holy shit, Mozilla just can't stop mocking its users. How did they earn their reputation as the good guys at all? Okay, now take a deep breath, and prepare for something even worse - [the Firefox privacy policy \(archive\)](#) ([MozArchive](#)):

Firefox privacy policy

That's why we build Firefox, and all our products, to give you greater control over the information you share online and the information you share with us. We strive to collect only what we need to improve Firefox for everyone.

Still lying I see. Okay, now - the section is **very long**, and I don't want to bore you to death here, so I will just list the general data that FF collects, straight from the horse's mouth: *“Interaction data”, “location data”, “webpage data for Snippets”, “webpage data for Pocket recommendations”, “technical data for updates”, “technical data for Add-ons blocklist”, “webpage and technical data to Google's SafeBrowsing service”, “webpage and technical data to Certificate Authorities”, “crash reports”, “campaign and referral data”, “search suggestions”, “Firefox Accounts data”, “Synced data”, “Screenshot uploads”, “Addon search queries”*...and I've skipped much of it anyway. There probably **isn't a single piece of software collecting more data by default than Mozilla Firefox**; at least I - having tested (close to) all web browsers in existence - haven't seen one.

"Lean data" is yet another fraud

I only recently learned Mozilla has [this page \(archive\) \(MozArchive\)](#) - but it has actually been around since 2016. Anyway, here is where Mozilla tries to justify data collection if it's *“lean”*. Of course, *“lean”* is [redefined \(archive\) \(MozArchive\)](#) in an Orwellian way to where it's not really *“lean”* anymore:

Multiple organizations may have access to parts of your data, causing a larger digital footprint than expected.

And why must *“multiple organizations”* have access to our data at all? Why not just keep it to

yourself, instead of throwing it around wherever?

Most sign-up forms ask for first and last name. A valid reason to have this data might be to increase email open rates through customized emails. An equally valuable alternative—that minimizes risk—would be to collect first name only.

And why not go all the way and **not ask for the names at all**? Pseudonyms are enough - really. Many people in the age of the Internet are more attached to their pseudonyms than their "real" (government-assigned) names. This excuse of “*email open rates*” is actually **really fucking stupid**. The receiver will open an email he cares about, and won't if he doesn't. Names don't come into play at all.

Sometimes you need data indefinitely.

Why? Why? **Fucking why?** This isn't “*lean*” at all! This is a whale that has eaten the entire ocean and still tries to pretend it's a beautiful and agile shark. Again, the point of this page is only one: to redefine “*lean*” in a way that makes Mozilla seem like a privacy supporter. To complain about "fat" data collection but then give fake solutions that don't really make it “*lean*”. For example, check [another page \(archive\)](#) (MozArchive) from the “*Lean data*” series:

Give people choices and control over their data. They will trust and respect your brand more when you do.

Not needed if you just don't collect it. And for Moz, the way to do this is to just provide a bunch of **opt-outs**. Some of which require you to make accounts...on different services :D - “*Some Mozilla.org pages use clear GIFs which communicate with DoubleClick to understand*

*the effectiveness of our advertising campaigns; you can control personalized ads from DoubleClick in Google's ad settings (you will be prompted to sign into your Google Account)”. What if someone doesn't want to deal with Google at all? Mozilla **does not provide this option** and calls that “*Lean data*”. What a joke. Don't lecture others about privacy if you can't provide it yourself.*

An effective policy tells people what data you collect, who you share it with, and how you handle it.

And it's easier to do this the less data you collect. Mozilla's [website privacy policy \(archive\) \(MozArchive\)](#) is 1385 words long, while RiseUp's (entire) [privacy policy \(archive\) \(MozArchive\)](#) is only 733 words long - and actually much more detailed. This is what happens when you just don't collect much - there's no need to write a dissertation (e.g the entire third party sharing section can be skipped, since RiseUp doesn't do that). And if you add Mozilla's [regular privacy policy \(archive\) \(MozArchive\)](#), you end up with over 2000 words together. And they have a few more separate policies if you want to torture yourself further - totaling probably over 5000 words if I had to guess. But that's not all - they say this in their policies:

Use of the Invisible reCAPTCHA is governed by the Google Privacy Policy and Terms of Use.

Ha-ha. More thousands added to the pile. And this is supposed to be “*Lean data*”?! How is it in any way “*lean*” to force someone to read **someone else's** privacy policy before visiting **your** website? Funnily enough, in their “*Creep-o-Meter*” Mozilla [complains \(archive\) \(MozArchive\)](#) (MozArchive) about **exactly that**: “*Legalese, ambiguity, and policies that sprawl across multiple documents and URLs are the status quo. And it's getting worse, not better. Companies use*

these policies as a shield, not an actual resource for consumers". Mozilla is using its privacy criticisms of others as a moral shield to distract from the fact they're doing the same things they're complaining about (and worse). How despicably fraudulent.

Firefox account - the master spy tool

Taken straight out of the Google / Microsoft playbook, where one account gives you access to many different "services". But because it's one, it connects everything you do together (or builds a profile) that much easier. I couldn't log in from Pale Moon, which was expected, I guess. Funnily, the confirmation email they send you has links with a bunch of &utm= style tracking. So the disaster starts before you've even logged in. Anyway, the [new Firefox privacy policy \(archive\) \(MozArchive\)](#) has some info about Account privacy:

Your email address is sent to our email vendor, Acoustic

Why does Mozilla even need an “*email vendor*”? It seems they just can't stop throwing user data at random targets. Let's learn more [about Acoustic \(archive\) \(MozArchive\)](#), though:

ACOUSTIC

Here for
the
marketers.

Okay, that's enough. They needed that really big font to make it absolutely clear who they are here for - and it's not the users. Since I'm not a “*marketer*” I guess I have nothing to stay around here for, so let's move back to the FF account privacy policy:

Interaction data: We receive data such as your visits to the Firefox Accounts website, dashboards and menu preferences, what products and services you use in connection with

your Firefox Account, and your interactions with our emails and SMS messages. We use this to understand your use of our products and services and to send you more useful Firefox Account Tips and in-product messages.

Haha. I told you they're going to build a profile of all your activity :D.

Technical data: To display which devices are synced to your Firefox Account and for security functionality, we store your device operating system, browser and version, timestamp, locale, and the same information for devices connected to your account. If you use your Firefox Account to log into other websites or services (such as AMO or Pocket), we receive the timestamp of those log-ins.

What you do and when, all beautifully stored together. Master Google would be proud! And remember, that the FF Account gives access to Pocket - so they know what you really like to read, and when. Relay gives them access to your emails, as well as which websites you want to anonymize yourself from. And the VPN...well, we all know what that does. Look, not even Google runs a VPN. **Not even the botnet master has access to all your browsing history.** Mozilla **really** is worse! BTW, there is one really funny thing inside the account ToS (MozArchive) that I just have to mention:

We may suspend or terminate your access to the Services at any time for any reason, including [...] our provision of the Services to you is no longer commercially viable.

The fuck? If you stop bringing them profit, you're gone. They **really** said that! To me, this is a roundabout admission that your data is being sold. And if it's not worth much (for whatever reason), then you get kicked out.

Hey, I am so used at this point to just shitting on Mozilla whenever they execute yet another violation. But when I take a step back to look at it all from afar, I am absolutely shocked at the extent of it. It is like we have this digital Godzilla walking around, destroying everything - and no one cares, or they even think it's cool. I could get lost in the emotions, but it's time to work, and expose the illusion since no one else dares to.

Hidden tracking with link shorteners

Go to Mozilla's Twitter and click any post e.g this one (MozArchive). The link to the article (the “*foundation.mozilla.org*” part) pretends to be a full link but is actually just a shortening (“*mzl.la*”+an arbitrary string), where you cannot see directly where you'll be going (an evil in itself). But why does Mozilla do something like this, specifically? If you actually click the shortened link, your address bar will contain something like this: “*https://foundation.mozilla.org/en/blog/alexa-help-me-which-smart-speaker-has-the-best-privacy/?utm_source=twitter&utm_medium=social&utm_content=1689999999*”. So, Mozilla will know where you came from and what you clicked to get to the final destination. None of the “*utm*” parameters are necessary for any actual functionality **except to let Mozilla follow you around**. And you cannot know the final destination contains those parameters because Mozilla doesn't let that be seen thanks to their evil shield - showing a **purposeful plan to deceive**. How vile is that? The corporation that speaks so strongly against tracking and has built its entire reputation on that issue, actually tracks you through every single one of their Twitter posts (and probably other social media, too - but I'm not bothering to check) and attempts to hide it.

Privacy-preserving advertising?

Mozilla's new, nice-sounding invention that's supposed to ship in Firefox version 128 (archive) (MozArchive) and presumably all later ones if it succeeds. But what is it even supposed to do? Let's listen to Mozilla itself:

Mozilla is prototyping this feature in order to inform an emerging Web standard designed to help sites understand how their ads perform without collecting data about individual people. [...]

So the point is to “*help sites understand how their ads perform*”. But how does this help the user? Wasn't it supposed to be users first? Continuing...

Attribution is how advertisers learn whether their advertising works. Attribution measures how many people saw an ad on a website and then later visited the advertiser's website to do something the advertiser cared about. [...]

Once again, advertisers - and not users - are being appeased here.

Attribution is very important to advertisers. [...]

Yeah, but not really to the users.

Our hope is that if we develop a good attribution solution, it will offer a real alternative to more objectionable practices like tracking. We are currently testing this approach to see if it can provide advertisers with the information they're looking for.

You want “*to see if it can provide advertisers with the information they're looking for*”? But

what's in it for the user? I know I'm repeating myself, but this is so blatant. Four quotes and four attempts to appease the advertiser, while ignoring the user completely. But surely, there's something in this for the user too. I mean it's “*privacy preserving*”, right? So let's see if there is any substance inside their claims:

1. Websites that show you ads can ask Firefox to remember these ads. When this happens, Firefox stores an “impression” which contains a little bit of information about the ad, including a destination website.

So this data is going to be saved locally for anyone with access to the machine (or just malware) to steal? How is that private?

2. If you visit the destination website and do something that the website considers to be important enough to count (a “conversion”), that website can ask Firefox to generate a report. The destination website specifies what ads it is interested in.

So websites have to agree with this proposal in the first place for it have any meaning at all. Why would they just...not sign up and keep tracking users in the more malicious (and more effective) ways? This is just Do Not Track revisited. Hey, I'm sure some websites will sign up for this and pretend they're doing some great service (while still shoving us their slimy ads); it's going to be good PR. Let's make it clear: the advertisers still hold all the cards with this scheme. They can choose to report their tracking crimes, but don't have to at all, with zero consequence if they don't. And even if they report, they can still perform them just in a less violating way (if you believe it). Maybe they will even be portrayed as heroes in the media, for being some of the first companies to engage in this “*privacy-preserving*” advertising. What a life!

3. Firefox creates a report based on what the website asks, but does not give the result to the website. Instead, Firefox encrypts the report and anonymously submits it using the Distributed Aggregation Protocol (DAP) to an “aggregation service”.

4. Your results are combined with many similar reports by the aggregation service. The destination website periodically receives a summary of the reports. The summary includes noise that provides differential privacy.

So it's anonymized data, but still data, and thus un-private. Besides - again - the data stored locally is not anonymized yet, since well, it's local, so it can be attached to everything that is on your system. Though Mozilla might say it's only sending the ad impressions without connecting it to anything else, that is just a promise that can be violated at any time (and this very article is full of Mozilla's broken promises). Without confirmation from network monitoring, trusting this scheme is foolish.

Mozilla explains how this scheme is supposed to work in detail in this "technical explainer" (archive) (MozArchive). Let's take a look:

Mozilla is working with Meta and other actors on defining an in-browser attribution API. The purpose of this API is to provide a privacy-first design for advertising companies to be able to measure how advertising drives conversions.

Heh. Privacy and ethics giant Meta (AKA Facebook AKA Zuck) is involved in this. The giant that Mozilla was pretending to fight just a few years back. And again, it's advertisers that are targets of this proposal, not the users. But wait! The next section's header reads - wait for it - *“End-User Benefit”*! Is this where we finally get to understand the magic behind this proposal?

Mozilla will now surely reveal itself as the savior of the Internet and the world. I can't wait, so let's not babble any further:

Users largely benefit indirectly from the use of this API. That's a hard fact, but an important one.



Not so fast!

And just what's the evidence for your “fact”?

Any benefit people derive from this feature is indirect. The sites they visit are often supported by advertising. Making advertising better makes it possible for more sites to function using the support that advertising provides.

So what? You could make an analogous argument that we derive benefits from all the products made by child labor, so we should make child labor "better". Then more companies will be able to use it, and we'll get more products. Yay! Except, child labor is bad. And ads are bad. And

they should both be eliminated, not "made better". If the things that depend on them have to die because of it, then so be it. Maybe we don't need them. Basically, **the general idea of this argument allows anyone to justify the most horrible of acts, as long as something - anything - can be found to depend on them** - which is obviously insane. The situation becomes even worse when you consider the fact that **the more a website is focused on making profit, the worse it is**. The best places on the Internet are those that are completely noncommercial. They don't have to care about whether some ad provider out there thinks the place is "appropriate" enough for their ads, they don't have to focus on posting 15 low-quality articles per day to be "relevant" and stay high up on search engines. They will never include shady sponsored articles shilling shitty products. And of course, they don't have disgusting ads clogging them up. I swear, I've checked the source codes for some sites, and it seems half of it is dedicated to displaying ads. **These sites exist only to shove you ads and sell you crap you don't need** with "news" as a Trojan horse. Meaning, to accept Mozilla's argument that "we need the privacy respecting ads to save the Internet" would actually be ceding too much ground already. Even if it was true that ads keep many websites going, they are the exact ones that need to die. So no, Mozilla - your proposal is not saving the Internet, but continues to feed the cancer that infects it while portraying it as healthy tissue.

Our view is that the costs that people incur as a result of supporting attribution is small. Those costs are:

- CPU, network, and battery costs for generating and submitting reports. Here, this cost is negligible, particularly relative to what sites are already able to use. This design could replace some of those costs, which might lead to improvements in some cases.*
- Privacy loss from use of their information. Attribution information will be*

aggregated and will include noise that protects the contribution that each person makes. This design is structured so that advertisers learn about what many people do as a group, not what any single person does.

How could you miss the fact that we have to **see your disgusting ads** and absorb the manipulation inherent in them? The “*costs that people incur*” while having to endure a blizzard of ads day in and day out are obviously not “*small*”; in fact ads are a major source of human dissatisfaction (archive) (MozArchive). So, who are ads **really** for?

In comparison, the indirect benefits are likely to be significant:

- *The value that an advertiser gains from attribution is enormous. Attribution can be the difference between an advertising-dependent business surviving or failing. Advertising-supported content and services can be more equitable than alternative funding models.*

Thanks for admitting it. Advertising vampires suck up “*enormous*” amounts of money from their unsuspecting victims. And if the victims just blocked the ads, the vampires would die. But Moz wants to portray vampires positively so that they are able to keep exploiting you.

- *If advertisers do not need to track people for attribution purposes, it makes it easier for us to identify and stop tracking.*

In this point Moz tries to meet the advertisers halfway by offering them a way to measure ad effectiveness while only tracking sets of people instead of specific people (but it is still tracking, so Mozilla is being dishonest here). But again, the advertisers don't have to take Moz

up on it and can keep tracking the old way, similarly to how DNT ended up working. And it is still assuming that the ad-supported website ecosystem is something that should be kept around at all costs.

Anyway - if you still really like ads despite their proven harms - then you don't need Moz's proposal to have “*privacy-preserving*” ones, as that can already be done easily with only basic HTML tags. With the magic `<img>` tag, you can display your shitty ad like this: `<img src = 'my_shitty_ad.jpg'>`. And boom! You have your perfectly private ad, with no more data collection other than what the client sent to download the image, which of course doesn't have to be kept or sent anywhere or analyzed in any way at all. If Mozilla was serious, they would require whoever joins their program to do ads this way. This wouldn't remove all the problems with ads, but at least they would truly be “*privacy-preserving*”.

But of course, that would be too little tracking for Mozilla, so it adds that “*attribution*” crap to give advertisers the information about which of their ads are more or less effective. Then, it pretends that tracking people in sets with their proposal instead of individually (like it is usually done) makes it not tracking anymore, but it actually doesn't. Your behavior (of which the advertiser is informed with this scheme) still impacts what the business does later; it is absolutely tracking. Why are businesses entitled to knowing how we view or interact with their content at all? **Mozilla bases their entire project on the assumption that businesses absolutely must sell their products**, but doesn't bother to justify it. If your product is truly needed, people will seek it out on their own; if they don't, then it has no God-given right to get sold.

In summary, this is yet another way with which Mozilla pretends to be noble but actually defends the evil foundations of civilization. Their pretend compromise with the advertising vampires seeks to convince you that the reformed version is now an ethical one (even though

the advertisers still hold all the cards), but the fundamental assumption of ads being great and essential is never questioned. As expected from controlled opposition.

Anti-privacy nonsense backfires

It's January 13, 2022, and a terrible bug (archive) (MozArchive) has struck our favorite web browser, Mozilla Firefox. Whenever anyone ran it, it stole 100% of their CPU cycles, affecting all versions. Why did this happen? From what I've been able to discern, some of the unsolicited requests (*Firefox Data Collection* and others) Firefox makes at launch connected to servers that screwed up their HTTP3 implementation. Most of the comments that provided solutions (disabling telemetry / HTTP3 or installing an adblocker) have been hidden (censored). This situation proves not only that Mozilla's staff is incompetent, but that they also hate the users since they hide workarounds for their fuckups and still won't disable telemetry by default, which causes them in the first place.

Firefox will feed your data to AI?

This is what I've concluded from their new Terms of Use (archive) (MozArchive) page for Firefox, whose most important part seems to be this:

When you upload or input information through Firefox, you hereby grant us a nonexclusive, royalty-free, worldwide license to use that information to help you navigate, experience, and interact with online content as you indicate with your use of Firefox.

The specific wording used tells us a lot about Mozilla's intentions. Starting with the *“or input”* part. Why would they use that particular word? Because the *“input”* can be anything. Mouse, keyboard inputs, or anything else that the user submits - not just *“upload”* which seems to be limited to files. So that word should cover everything Firefox is able to grab. What will they do with it, after that? Gain the ownership of it (*“you hereby grant us a nonexclusive, royalty-free, worldwide license”*). For what? Supposedly to *“help you navigate, experience, and interact with online content”*. But what does it mean? How would my uploaded files or inputs help with that? Only if they were then analyzed by something and used to modify your experience. What could it be?

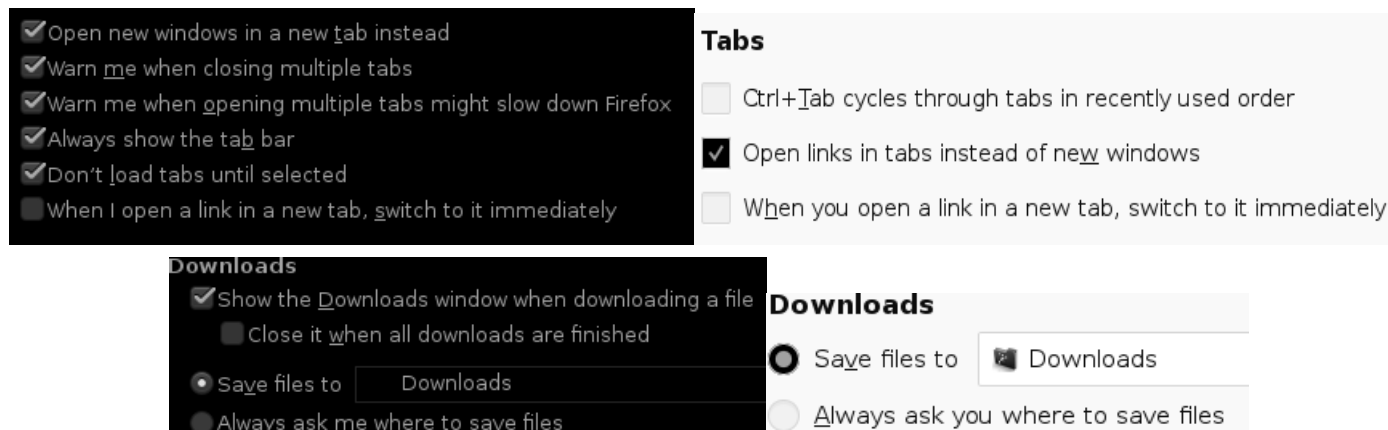
Only AI. This becomes even more obvious when you look at their latest blogposts (archive) (MozArchive). 3 out of 6 "latest mozilla news" are about AI - *“ROOST: Open source AI safety for everyone”*, *“Mozilla, EleutherAI publish research on open datasets for LLM training”*, *“Paris AI Action Summit: A milestone for open and Public AI”*. Even in the *“Welcoming Peter Rojas as Mozilla’s SVP of New Products”* news piece, the guy appears to be related to AI companies, so the full amount could even be 4 out of 6. It is clear that Mozilla is now an AI company. And AI relies on...gigantic amounts of (user-submitted) data. Exactly the amount that Firefox provides, and is trying to protect themselves from legal consequences of its abuse by their new ToU. What will they use the data for? I don't know. I can think of many things, none seem good. Realistically, AI will be yet another part of the technological slavery system, except one that is much more powerful, encompassing, and harder to resist. And you - by your natural usage of Firefox that spies on almost all interactions with it - will provide the data required to fuel it.

Freedom is slavery

- *“Individuals must have the ability to shape the internet and their own experiences on it.”* (archive) (MozArchive)
- *“Firefox Puts You in Control of Your Online Life”* (archive) (MozArchive)
- *“We created Firefox to give people choice and control of their Web experience and we’re always adding more ways to personalize your Firefox.”*
- *“Celebrating Choice, Control and Independence On the Web”* (archive) (MozArchive)
- *“Ten years ago, we made Firefox to keep the Internet in each of our hands — to create choice and put you in control of your life online.”*

History of anti-control

To get a big picture view of this one, it's necessary to go back in history quite some time. Let's put the *Settings* menus of Firefox 17 and 63 side by side:



As we can see, the trend has been to remove options - so **less control for the user**, contrary to the claims of Mozilla. But these are pretty minor - wait until you see the really vile things. In

version 23 (which came out in 2013), Mozilla removed the ability to disable JavaScript from the Settings menu. Now, you could say "just use an addon to handle JS permissions!" and I agree - but that is no reason to remove the in-built option for the people who want it. An adjacent problem also throws a wrench into that plan - namely the fact that Firefox **does not allow installing unsigned extensions** anymore! Here is the history of this:

- **Firefox 40-42:** Firefox warns about signatures but doesn't enforce them.
- **Firefox 43:** Firefox enforces the use of signatures by default, but has a preference that allows signature enforcement to be disabled (*xpinstall.signatures.required* in about:config).
- **Firefox 48:** (Pushed from Firefox 46). Release and Beta versions of Firefox for Desktop will not allow unsigned extensions to be installed, with no override. Firefox for Android will enforce add-on signing, and will retain a preference — which will be removed in a future release — to allow the user to disable signing enforcement.

Notice the slippery slope? First it was just a warning, then disabling unsigned extensions by default but still letting you enable them; and finally removing the option to install the addons without Mozilla's approval completely. Firefox will also disable any unsigned addons you might already have. The *“Choice, Control and Independence”* is truly off the charts...Just imagine - one day they might decide to disable your AdBlocks and NoScripts - and there will be nothing you can do whatsoever. This might be coming sooner than expected. Mozilla's [new addon blocking process \(archive\) \(MozArchive\)](#) literally starts with a section called *“Security Over Choice”*, which was not in the old one. So, they have now provided us with a **direct, undeniable admission** that **your choice doesn't matter**. Thanks, Mozilla! The criteria for a *“hard block”* were also way expanded - I think we can expect a wave of addons (that Mozilla doesn't

like) to get buried soon.

UPDATE: Aaaand **literally the next day** my predictions came true: all Firefox addons have been disabled (archive) (MozArchive) due to an expired certificate. And so, people got silently hit with stuff like this when turning their "private and secure" browser on. It was only a matter of time until Mozilla's extension prison backfired, and it did so spectacularly. Though the BugZilla comments were already predictably closed, they will not be able to contain the armageddon this time, no matter how much PR they spew. The whole /r/firefox front page is filled with threads about this, with many people moving to Chrome-based browsers. Hacker News (archive) (MozArchive) is also booming. Tech sites are running with the news (archive) (MozArchive) too. The funny thing is, the whole point of the extension prison was allegedly to increase security - and yet today, **all security addons got disabled** because of it! Shows how freedom always has to trump over security or it ends up in a disaster like this. RIP Mozilla, you won't be missed. And let's use this as a reminder that **evil eventually loses** not only in cartoons! With this out of the way, let's list some other anti-choice decisions Firefox has made before moving on to the most vile one:

From Firefox version 23 (archive) (MozArchive) and up you cannot disable images from the UI anymore - *"Load images automatically" and Always show the tab bar* checkboxes removed from preferences" (ensuring that the *"clear GIFs"* from Mozilla's tracking allies get loaded?). 44 has removed (archive) (MozArchive) the option to *"Ask you every time"* whether you want to allow a website to store cookies (and hid the removal (archive) (MozArchive) from the release notes page). 52 brought a PulseAudio requirement to play sound on Linux - even though the ALSA code is there **even now**, so the decision was made entirely to **remove user choice**. 57 no longer supports XUL addons. Since version 60, Firefox does not allow (archive) (MozArchive) deleting singular cookies anymore - only all of them for a chosen website;

Mozilla describes the change (archive) (MozArchive) like this: *“Redesigned Cookies and Site Storage section in Preferences for greater clarity and control of first- and third-party cookies”*...hahaha. 68 removes yet another option - disabling multiprocess (archive) (MozArchive). It seems they even plan their anti-control changes two versions ahead, because the removal of userchrome.css (archive) (MozArchive) customization is coming in 69. **UPDATE April 2024:** oh, and I don't usually cover phone issues, but Firefox for Android lacks an about:config (archive) (MozArchive) in all versions after 68.11.0.

XUL deprecation

The XUL issue is really important and requires further elaboration. With version 57, Mozilla decided to end XUL support and replace it with the gimped WebExtensions which they knew would kill many addons (the others would have to be rewritten). If you check out Mozilla's site (archive) (MozArchive), you will see that **the vast majority** of functionality available for XUL addons can't be done with WebExtensions. It is actually really tough to find relevant information (as in, not Mozilla's propaganda) about this; we have to hunt down addon developers unhappy with the change, such as Classic Theme Restorer's dev (archive) (MozArchive). Check out these quotes:

WebExtensions will never do everything XPCOM does, so feature parity is not a goal. Some top add-ons can't be completely ported (DownThemAll and Firebug come to mind) and we're accepting that risk.

So, Mozilla doesn't care that some addons considered essential by their numerous users will die. Nice *“choice”* and *“control”* they've got there.

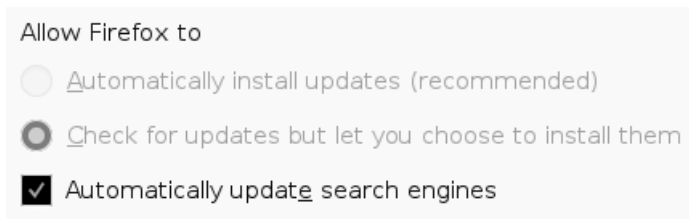
pretty much all the APIs that it makes sense to implement have been done. What remains is undocumented, deprecated or we've thought not worth bothering with (we could be wrong).

According to Mozilla, some functionality isn't worth bothering with. All that “*control and independence*” probably overwhelmed them. And the most important and revealing quote:

The only reason why CTR does not work in Firefox 57+ is Mozillas decision to take away add-ons almighty power over the browser, not because add-on features are incompatible to modern techniques or Firefox 57+ in general. A simple CSS loader would allow over 80% of CTfRs features to be available for Firefox 57+. This is proven by all userChrome.css/userContent.css tweaks available [here](#).

So, Mozilla not only doesn't care about user choice and the other slogans it spews - but is **actively working against them**. “*Spawn of Satan*” wasn't an exaggeration! Another good resource for WebExtension information is [DownThemAll's site \(archive\) \(MozArchive\)](#). This topic is so extensive I have barely scratched the surface - and the developers of the killed addons explored it way better than I could - so read those links I've provided if you want to know more. For now, let's move on to the last - and perhaps the most disgusting - anti-control scheme of Mozilla:

Forced updates



Yes, you saw it right! There is **no way to disable auto-updates** since version 63! The option has even been removed from the dumpster known as about:config. Therefore, Firefox will at least check for updates (privacy issue) and graciously let you decide whether to install them. But it remains to be seen if that's still available in the versions to come; remember, **the trend is towards less user choice**. So it is quite likely that you will soon be completely at the mercy of Mozilla in regards to the software you run on "your" computer - unless you stick with an ancient Firefox version, or switch browsers (the sane choice).

UPDATE February 2025: in case you were wondering, simply keeping your Firefox version old is **not possible anymore**. At least without having your functionality be disabled remotely ([archive](#)) ([MozArchive](#)):

On March 14, 2025, a root certificate used to verify signed content and add-ons for various Mozilla projects, including Firefox, will expire. Without updating to Firefox version 128 or higher (or ESR 115.13+ for ESR users, including Windows 7/8/8.1 and macOS 10.12–10.14 users), this expiration may cause significant issues with add-ons, content signing and DRM-protected media playback.

If you don't update, Firefox features that rely on remote updates will stop working, and your installed add-ons will be disabled. DRM-protected content, such as streaming services, may also stop playing due to failed updates. Additionally, systems dependent on

content verification could stop functioning properly.

"You will update your Firefox, and you will be happy"! Yes, the Mozilla Firefox that pretends to support freedom is now literally slave software which will be crippled unless you always run the newest version (absorbing all the new spyware, ads, etc. coming with it). There is no more way to deny it, **choice has been completely removed**. Let's be clear here, **these people are complete psychopaths** for whom communication is only about baiting, about manipulation. They don't mind using the word "freedom" while acting the complete opposite to it; their respect for the user is absolute zero.

And since you're now totally forced to update, you'll have to deal with the fact that these updates also **frequently change settings** you've set up for yourself. So, Mozilla knows better what your Firefox preferences should be than you do. Their bugzilla page is full of these intrusions being reported. For example changing the order of extension buttons (archive) (MozArchive), removing bookmarks (archive) (MozArchive), bookmarks again (archive) (MozArchive), removing pinned tabs (archive) (MozArchive), reenabling of the Pocket spyware (archive) (MozArchive), deactivating addons (archive) (MozArchive), and many, many others including on their support site (archive) (MozArchive) and elsewhere (archive) (MozArchive). Of course, not all of these can be proven to be malicious, but some - like the Pocket thing - seem very likely. And regardless, a changed setting is a changed setting, and takes away user control - which is what this section is all about.

Bypassing proxy settings

From <https://www.bleepingcomputer.com/news/security/mozilla-blocks-malicious-add-ons->

installed-by-455k-firefox-users/ (archive) (MozArchive):

Starting with Firefox 91.1, Firefox now includes changes to fall back to direct connections when Firefox makes an important request (such as those for updates) via a proxy configuration that fails. Ensuring these requests are completed successfully helps us deliver the latest important updates and protections to our users.

Yes, this means that, even if you've configured your Firefox to use TOR, and that fails to connect, **auto-updates will still be executed in the clear**. How malicious. This also means that mitmproxy - my favorite method for fishing out unsolicited requests - **is not guaranteed to catch them all** anymore (unless using proxychains). I suspect Mozilla will soon bring in more requests that they consider “*important*” enough to ignore the users' wishes and bypass the proxy.

Supporting censorship

On January 8, 2021, Donald Trump (then president of USA) was banned from Twitter (archive) (MozArchive). Mozilla - of course - immediately jumped to defend the ban (archive) (MozArchive), almost as if they were already prepared. Anyway - since this has wider implications than just Trump - let us analyze their blogpost:

The title “*We need more than deplatforming*” already shows that they **do support** kicking out undesirables, but that (they think) we need to do **even more** to control the discourse effectively. Before we move on to the actual quotes, let's realize what this means. The only way to censor in the manner Mozilla thinks is appropriate, is by **relying on the so-called Big Tech - the same Big Tech which Mozilla has pretended to rally against!** The elephant in the room is this:

Turn on by default the tools to amplify factual voices over disinformation.

They want to algorithmically decide which content is allowed to be posted, and which isn't. This is especially relevant in the context of the fake pandemic, during which the whole world has been enslaved exactly thanks to the propagation of the “*factual voices*” over the so-called “*disinformation*”. The “*disinformation*” here includes mentioning the factual harm done by COVID vaccines or even proven alternative treatments for COVID itself. So, Mozilla supports a world where people are harmed without being able to defend themselves.

These are actions the platforms can and should commit to today. The answer is not to do away with the internet, but to build a better one that can withstand and gird against these types of challenges.

As I said earlier, the only platforms that can do so are those that have enough resources to develop and implement algorithms that will check every comment posted there against their criteria for “*disinformation*”. Which just happen to be the Big Tech that Mozilla allegedly hates (but in reality is apart of them). Another censorious thing they've done one time is releasing a version (archive) (MozArchive) of Firefox **entirely to remove Russian search engines**. Mozilla is fully on board with the West's sucking of Zelensky's private parts and supporting his ongoing robbery of Europe and USA (archive) (MozArchive) and sacrifice of most of Ukraine's male populace. That is why they are hiding some of the only places where you'd be able to find any information opposing that. Anyway, let's finish up with an analysis of another one (archive) (MozArchive) of their pro-censorship blogposts.

In short, Mozilla is really bothered that YouTube's recommendation algorithm brings up conspiracy theory or anti-LGBTQ videos. So bothered that they even want to create laws to

combat the issue. Fortunately, that won't be necessary as YouTube already has policies against hate (archive) (MozArchive) and conspiracy theories (archive) (MozArchive). What Mozilla - then - wants, is **even more** control over allowable content than YouTube already provides. And since they are in bed with Google (and Twitter, Facebook, Microsoft...) they will surely get their wish. **All of this has been planned with full knowledge of all the participants involved**, including the pretense that Mozilla is the David fighting against the transgressions of the Big Tech Goliath. And what The Hydra wants, is full control of what you can do, say, and even think.

Cucking to Manifest V3

Manifest V3 is a new set of internals governing how browser extensions will work, that was envisioned by Google in 2018. It was supposed to (archive) (MozArchive):

create stronger security, privacy, and performance guarantees

In practice, this of course means **reducing what extensions are able to do**:

More narrowly-scoped and declarative APIs, to decrease the need for overly-broad access and enable more performant implementation by the browser, while preserving important functionality

Here is what gorhill - the developer behind uBlock Origin and uMatrix - has had to say (archive) (MozArchive) about it:

The fact that they are planning to remove a proper blocking webRequest API with no

word of an equivalent replacement is a sign of intent, that is, reducing the level of user agency in their user agent (aka Google Chrome).

Many uBO features are still not available in the new system 4 years later:

One of the biggest issue at this point is the inability to implement the overview pane in the popup panel, thus also preventing the implementation of the advanced-user mode and the ability to point-and-click to set dynamic rules.

The no-large-media-elements feature can't be implemented as this requires to inspect response headers on the fly.

There is no concept of exception modifier filters in DNR, i.e. `csp=/removeparam=` exceptions cannot be accurately translated to DNR rules. For a specific example, all the `removeparam=` filter exceptions from AdGuard URL Tracking Protection, meant to override the main `*$removeparam=utm_source` filter, can't be converted to DNR.

Given that cosmetic filtering is declarative, it's not possible to have an element picker to create cosmetic filters.

In January 2024, Google will completely cease to host (archive) (MozArchive) extensions made in the previous Manifest V2 system:

In January 2024, following the expiration of the Manifest V2 enterprise policy, the Chrome Web Store will remove all remaining Manifest V2 items from the store.

Even earlier, the ability to run them in the browser will be denied:

Starting in June in Chrome 115, Chrome may run experiments to turn off support for Manifest V2 extensions in all channels, including stable channel.

This is literally a repeat of what has happened during the switch from XUL to WebExtensions. And what is Mozilla's reaction (archive) (MozArchive)?

In 2018, Chrome announced Manifest v3, followed by Microsoft adopting Chromium as the base for the new Edge browser. This means that support for MV3, by virtue of the combined share of Chromium-based browsers, will be a de facto standard for browser extensions in the foreseeable future.

Of course, they jumped from excitement at the opportunity to swallow the new “*standard*” Google had shat out. Let's realize it is considered a “*standard*” only because **Google has decided so**. And Mozilla won't dare to oppose their master. Though Mozilla pretends to keep the relevant functionality of the old API:

Mozilla will maintain support for blocking WebRequest in MV3. To maximize compatibility with other browsers, we will also ship support for declarativeNetRequest.

Anyone that's paying attention will know it's all a temporary part of their boiling frog controlled opposition scheme. Same tactic they've used to enforce extension signing back in the day. Hell, they pretty much admit that if you read between the lines:

We will continue to work with content blockers and other key consumers of this API to

identify current and future alternatives where appropriate.

They will be trying to get adblock developers to move away from the powerful webRequest features to the gimped Manifest V3 ones. And slowly, the webRequest features will be deprecated more and more, and we'll end up with content blockers that are heavily restricted in their functioning. Another sentence that betrays where their true convictions lie:

Unfortunately, that power [for extensions to have access to more of the browser's functionality - addition mine] has also been used to harm users in a variety of ways.

Power is bad, because someone might hurt themselves by installing a "malicious" extension. AKA the standard Mozilla fare. This is despite the fact that Mozilla already has ([archive](#)) ([MozArchive](#)) an addon review system that's supposed to prevent exactly that. As well as the reality on the ground, where websites keep hurting people with ads, tracking, viruses, long loading times, paywalls, cookie notices, Cloudflare, etc - and powerful extensions are the antidote for all of that. Why is Mozilla fine with those types of harm, but really bothered about the mostly imaginary harm of "malicious extensions"? It is obvious that extension safety is just an excuse to take away control from the users (in this case content blocking extensions are targeted specifically because [The Hydra](#) wants to control what you see, think, and do). Yet Mozilla is determined to keep the slavery train chugging along:

At the same time, we'll be encouraging extensions to use models that don't require permanent access to all websites, by making it easier to grant access for extensions with a narrow scope, or just temporarily. We are continuing to evaluate how to best handle cases, such as privacy and security extensions, that need the ability to intercept or affect all websites in order to fully protect our users.

How about **stop fucking gimping extensions** again, just because Google is doing so?! If Mozilla was really the people's company, they'd stand up to their master for once. They could do what Pale Moon did - which was to stick to the old standard (XUL; or in this case Manifest V2) forever. But of course Mozilla won't do that, because they can't.

People before profit?

“Mozilla makes browsers, apps, code and tools that put people before profit.” (archive) (MozArchive)

“Mozilla puts people over profit in everything we say, build and do.”

“Motivated by creating public benefit versus commercial gains” [...] (archive) (MozArchive)

Analyzing Mozilla's finances

It just so happened that as I was beginning to write this section, I visited Mozilla's site and this greeted me:



So let's check out how Mozilla is actually financed - does it really need our donations? It seems Mozilla has made their financial report as hard to understand as possible - but let me try to make sense of it anyway:

<i>Years Ended December 31,</i>	2017	2016
Unrestricted Net Assets:		
Revenues and other support:		
Royalties	\$ 539,168	\$ 503,677
Subscription and advertising revenue	2,653	
Interest and dividend income	4,919	3,018
Net realized and unrealized gain (loss) on investments	819	1,076
Contributions	6,438	5,440
Other	553	191
Foreign currency exchange gain (loss)	2,409	(1,241)
Loss on sale of assets	(43)	(124)
Net assets released from restrictions	5,363	8,336
Total unrestricted revenue and support	562,279	520,373

In 2017, 96% of Mozilla's revenue came from “*Royalties*”; in 2016 - 97%. What are these “*Royalties*” made up of?

Mozilla has entered into contracts with search engine providers for royalties which expire through November 2020. Approximately 93% and 94% of Mozilla's royalty revenues were derived from these contracts for 2017 and 2016, respectively, with receivables from these contracts representing approximately 75% and 79% of the December 31, 2017 and 2016 outstanding receivables.

97% from 93% is 90%; that is the percentage of 2017 income Mozilla gained from having certain search engines as defaults in Firefox. What were those search engines?

we decided that the default search providers would be Yahoo in the US, Baidu in China, Yandex in Russia, Belarus, Kazakhstan, Ukraine, and Turkey, and Google for the rest of the world.

Amazing, isn't it - **90% of Mozilla's income comes from having anti-privacy search engines as the defaults**. Truly, thanks for putting “*people over profit*”, Mozilla. There isn't much space left for donations to fill. I'm assuming they go under the “*Contributions*” section - that would mean **donations made up a measly 1% of Mozilla's entire income** in both 2016 and 17. According to [Wikipedia \(archive\)](#) ([MozArchive](#)), this situation is going back at least to 2005! So, their "we're funded by donations!" shtick is just a shameless lie and a ploy to fill their pockets as much as possible. It does not end at the search engines, of course - I had to hunt down an [obscure wiki page \(archive\)](#) ([MozArchive](#)) to reveal these quotes:

Invest in sustainability to grow diversified revenues this year [...] Our goal is to strive to hit meaningful diversified revenue by December 2014 [...] After reviewing over a dozen revenue opportunities for Mozilla, we have isolated a few that we are pursuing this year.

OK, so they want money from another source - because **500 million \$** from Google (and the others) just isn't enough for those greedy fucks. What are the ways they're going to get more?

Advertising in your browser

Tiles: There are a few opportunities that we plan go to market with in 2014 the first of which is to provide sponsored content on Firefox Tiles. Mindful of our values, we'll then evaluate the program and look to develop enhancements that benefit users and generate revenue.

Okay, so what is hiding behind those mysterious “tiles”? From <https://blog.mozilla.org/advancingcontent/2014/02/11/publisher-transformation-with-users-at-the-center/> (archive) (MozArchive):

Directory Tiles will instead suggest pre-packaged content for first-time users. Some of these tile placements will be from the Mozilla ecosystem, some will be popular websites in a given geographic location, and some will be sponsored content from hand-picked partners [...]

What this actually means is **you will see advertisements** anytime you open a New Tab page. The blog post mentions many times that this initiative “*puts the users first*” - hell, it's **even in the title**. So let's check out if that is actually true:

While we have not worked out the entire product roadmap, we are beginning to talk to content partners about the opportunity [...]

Oh, so you already **ran to the advertisers** to get them on board. How about talk to the **fucking users** first, if we're allegedly “*at the center*”? Anyway, it gets worse - on some obscure google group (archive) (MozArchive) I hunted down this quote:

Darren's team looked at that, and realized that we could make this better for users and generate income for Mozilla if we were smart about it.

Anyway, they had to end this failure of a project just 8 months later, since it didn't bring in enough money. From <https://blog.mozilla.org/advancingcontent/2015/12/04/advancing-content/> (archive) (MozArchive):

Advertising in Firefox could be a great business, but it isn't the right business for us at this time [...]

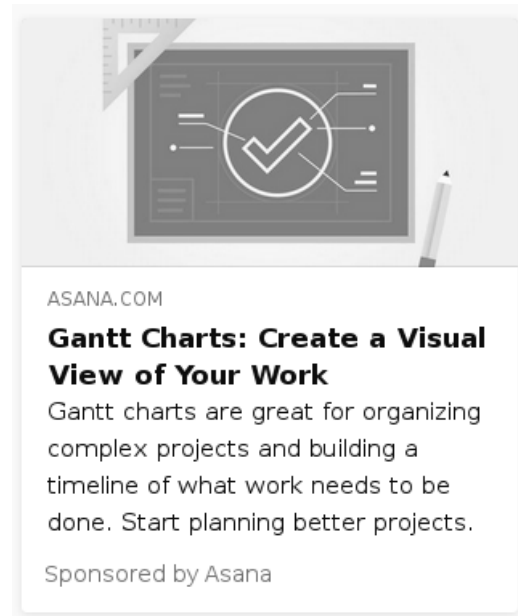
Okay, so you have to wade through a bunch of PR-bullshit before finding this gem of a quote. Directory Tiles were a business decision all along - and ending them was, as well. However, one failure isn't going to stop Mozilla from trying to shove ads down your throat to get rich (or richer than they already are):

Mozilla will continue to explore ways to bring a better balance to the advertising ecosystem

By the way, I've retested Firefox in 2023, and the Directory Tiles are back there. So, their removal was a **tactical retreat** executed probably because the opposition was too strong back then (the comments on the blogpost were overwhelmingly negative). But in the end, they couldn't give up abusing their users for money, so the ads are back in your New Tab page.

Pocket integration

The last quote from the above section was just PR-talk for "we'll find a way to make money from ads - just watch!". And it turns out they're back at it. Pocket is a service which allows you to *“Save articles, videos and stories from any publication, page or app”*. Firefox has been integrated with it since 2015, and acquired it in the beginning of 2017 (for 30 million \$, so they had to get it back somehow). And, thanks to *“recommendations from Pocket”*, they've been able to resurrect Directory Tiles (archive) (MozArchive) in another form. As they say, *“a picture is worth a thousand words”*:



As you can see, they're indistinguishable at all from regular suggested tiles until you get to the bottom to see *“Sponsored by”*. Of course, these tiles are also tracking you - this is how Mozilla is earning money from them in the first place. Since it started this year, we will know how much when their financial report comes out, I guess. And when this becomes another project

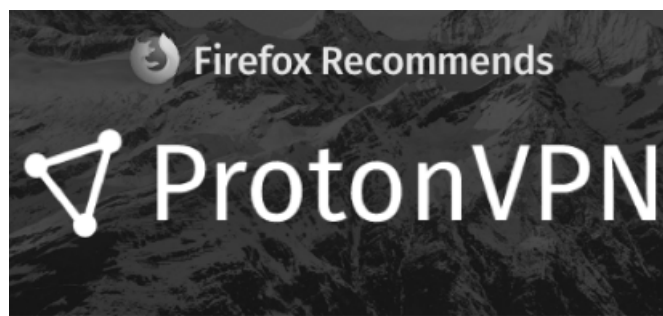
supposedly “*improving the user's experience*” that is ditched a few months later - it will again be shown as a purely **business decision**, not an user-centered one. I mean, let's be real here - they're working with advertisers; how can it be said that this is about the users? Did the users ask for ads in their New Tab pages? No? Then it's advertisers first, users second - refuting the “*People before profit*” slogan.

ProtonVPN partnership

Recently Mozilla has partnered with ProtonVPN (archive) - of course to keep you **safe online**. Actually, I'm impressed by them this time - it only took until the second paragraph to tell you it's about the money:

We believe that an innovative, vibrant, and sustainable Mozilla is critical to the future of the open Internet, and we plan to be here over the long haul. To do that with confidence we also need to have diverse sources of revenue.

Anyway, whenever you browse using a public Wifi, this ProtonVPN advertisement will appear:



It appears you are browsing on
an unsecured wireless network.

Firefox has teamed up with ProtonVPN
to provide you with a private and secure
internet connection, no matter where
you are.

☐ Don't tell me about this again.

Dismiss

Tell Me More

Has Mozilla suddenly had a change of heart towards caring about the users' privacy? Doubtful - just read the [first section](#) again. Anyway, it takes a visit to [ProtonVPN's blog \(archive\)](#) ([MozArchive](#)) to reveal the fact that:

*These subscriptions will be billed directly by Mozilla and **the majority of the revenue from these subscriptions will go to Mozilla**, directly supporting Mozilla's mission.*

So the greedy fucks will take most of the money even though it's ProtonVPN that provides the actual service. If Mozilla cared so much about the users' privacy as they claim, they could just

create their own VPN and give it away for free (they are surely rich enough to do that). But they cannot even stop including an avalanche of spyware into their flagship product - showing that it's about **satisfying their endless greed** instead of the user.

Mullvad partnership

Mullvad is one of the best VPNs on the market in terms of data collection, payment options, servers, speed, etc. Mozilla's partnership with Proton has failed so I guess they had to find another victim. In July 2019, Mozilla has started running a frontend for Mullvad (archive) (MozArchive) for twice the price and worse performance. Since it's using Mullvad for connections - but also connects to their own servers - it will be slower than Mullvad alone, by definition. More importantly, it adds the usual spyware (archive) (MozArchive) on top of it that Mozilla is famous for:

Campaign and referral data. This helps Mozilla VPN understand the effectiveness of our marketing campaigns. Upon installation of the app, Mozilla may temporarily receive your IP address in addition to campaign data and referral data like what ad campaigns you engaged with and your operating system, device type, and operating system version. Mozilla shares this with Adjust, but we do not share or store your IP address.

Interaction data. Mozilla receives data about your interactions with Mozilla VPN, including when you log in and when you request the server list.

There's also the fact that the VPN requires a Firefox account (the perils of which are described here), that it's available only in certain countries, and that it only accepts payments from anti-privacy services (*“Stripe, Apple, PayPal, or Google Pay”*). Analyzed honestly, you have to

admit that this is **the worst VPN to have ever existed** - seriously, try to find me a single commercial one that collects as much data or has all these other flaws. Mozilla is **literally scamming people** by inserting themselves as a middleman in front of a respected service, ruining it and charging twice the price (unless you pay for the whole year straight up, then the price per month is the same as Mullvad's). They do not even bother to mention that they are just a frontend to Mullvad on their main VPN page - you have to click the Privacy page. And yet, Mullvad has somehow agreed to this deal (bribes?). Still, it's obviously only a ploy for money since people do not gain any additional privacy by using their VPN (let me repeat, Mozilla's VPN has zero advantages over using Mullvad directly). If Mozilla respected the user, at least they'd have left Mullvad's great privacy untouched - but no, they just had to add a bunch of data collection. You'd be hard pressed to find such a horrible villain even in fiction.

Bribing distros to include spyware in their default settings

I am refering - of course - to the [Linux Mint "partnership" \(archive\)](#) ([MozArchive](#)) which changed users' Firefox search engine from DuckDuckGo / Yahoo / StartPage to the spywaristic Google:

The default search engines no longer include Linux Mint search partners (Yahoo, DuckDuckGo...) but Mozilla search partners (Google, Amazon, Bing, DuckDuckGo, Ebay...)

Even if you have explicitly chosen the more private options, they will be burned with the new update, and Google's jaws will devour you:

No, these were core engines in the Linux Mint configuration. They no longer are present

in the Mozilla version of Firefox. The default engine will switch to Google.

Though the Mint team gave excuses like “*simplification in terms of maintenance and development*”, it is obvious big money was involved (they admit later it's a “*commercial*” partnership). So, Mozilla will pay you to ship Firefox with Mozilla's chosen settings, which include the spyware search engines and all the telemetry etc. To be honest, this is partially a FOSS issue, where projects eventually realize they need money and end up giving up their principles in order to gain it. But Mozilla still takes the blame for having bullshit default settings and bothering distros to include them, with the money working as the carrot and lawyers as the stick:

We can't continue to keep using Mozilla's trademarks and brand identity if they don't agree with our changes.

Shady marketing

I've thought for a long time on how to structure this section (actually - the whole article!), since anything Mozilla touches is full of shady marketing - and I don't want to write an encyclopedia here! Maybe let's start with explaining how marketing actually works. Imagine Mozilla wanting to do something that they know their users will hate, so they recruit their public relations team to present the issue in a more positive way. Misdirection, confusion, replacing certain words with more acceptable ones, including a lot of "fluff talk" to bury the real relevant points, and even outright lying are some of the ways this is accomplished. Let's present some examples here, and hopefully you too will be able to **unspin Mozilla's web of deception** soon. We will take [this post \(archive\)](#) ([MozArchive](#)) to the chopping block:

Blog post analysis

Introducing Extension Signing: A Safer Add-on Experience

Mission: make a walled garden of addons. Now how to get there? The blogpost starts with a title containing the buzzword “*safety*”. This is supposed to “prepare” you in a certain way - you know, first impressions have an impact. Since people (usually) want safety, if you hit them with that right at the start, they will be more willing to lose some things in exchange. Of course, the marketing team will skip mentioning those at first - a title like “We will decide which addons you can use - for your safety!” would be a PR disaster.

This year will bring big changes for add-on development, changes that we believe are essential to safety and performance, but will require most add-ons to be updated to support them. I’ll start with extension signing, which will ship earlier, and cover other changes in an upcoming post.

“*Safety*” again. Repeat it until it sticks! And finally add another alleged benefit - “*performance*”.

The Mozilla add-ons platform has traditionally been very open to developers. Not only are extensions capable of changing Firefox in radical and innovative ways, but developers are entirely free to distribute them on their own sites, not necessarily through AMO, Mozilla’s add-ons site. This gives developers great power and flexibility, but it also gives bad actors too much freedom to take advantage of our users.

In preparation for the upcoming reveal, Mozilla reminds you that they are the good guys and

have been so for so long.

Extensions that change the homepage and search settings without user consent have become very common, just like extensions that inject advertisements into Web pages or even inject malicious scripts into social media sites.

Problem - reaction - solution. First, imagine a problem - malicious addons floating around! By the way, this is disproved by Mozilla's own data (hey - telemetry can be useful after all ;D). The most common extensions are adblockers, which are the opposite of malicious:

Rank	Add-on	Usage
1	Блокировщик рекламы Adblock Plus	8.899%
2	uBlock Origin	3.163%
3	Video DownloadHelper	2.652%
4	Cisco WebEx Extension	1.448%
5	Візуальні закладки	1.249%
6	Search Extension by Ask	1.219%
7	AdBlock	1.063%

Only these seven addons go above 1% of usage, and **65% of Firefox users do not use any!** By the way, Pocket used to be just an extension once, instead of an integrated part of the browser - and it is very intrusive privacy-wise, but it was allowed. So, Mozilla has **lied twice**: first about the severity of the problem, then their interest in solving it.

To combat this, we created a set of add-on guidelines all add-on makers must follow, and we have been enforcing them via blocklisting (remote disabling of misbehaving extensions)

Click [here \(archive\)](#) ([MozArchive](#)) if you want to analyze these guidelines; they are very long - the gist of it is: extension developers are complete slaves. Anyway, with this quote Mozilla reminds you that they have already dabbled into the addon slavery business, to get you ready for the cuffs getting tighter (the "Boiling Frog" strategy again):

Furthermore, malicious developers have devised ways to make their extensions harder to discover and harder to blocklist, making our jobs more difficult.

See? We've been trying so hard to protect your safety, but those damned malicious developers just keep bypassing all our schemes. Clearly, we need something better! So, the capability of imagined "enemies" is way overstated in order to get you to accept the "solution" easier.

We're responsible for our add-ons ecosystem and we can't sit idle as our users suffer due to bad add-ons.

Mozilla reminds you again that they're your friend, and want to save you from the suffering caused by the freedom to install whatever extensions you want!

An easy solution would be to force all developers to distribute their extensions through AMO, like what Google does for Chrome extensions

Look, we could do it the wrong way - like those evil Google guys over there - but we're your friends! And then - with the reader already conditioned in several different ways - comes the reveal of the whole addon slavery system. I've skipped it since that part is pretty honest - and we're analyzing bad advertising here. Moving on...

One important improvement that signing brings about is that the extension install experience will be renewed and improved.

Our prison is pretty comfortable though, so don't worry about it! So, since you might be a little worried after knowing their "solution" - they've had to recondition you. Anyway, as usual with spinning the narrative - it's as much about what you include as what you skip. And they've carefully avoided mentioning the fact that the browser **isn't yours anymore** - you don't decide which extensions can run in it - that's controlled by Mozilla now. This directly contradicts their stated mission, manifesto, and all the stuff about *“independence and control”* they keep spewing on their site. Fortunately, **the users have spoken** on the blogpost comments, and they realize what's up - which is the only good thing about this extension signing business. I hope they don't mind me quoting them:

The users have spoken

LuckyBastard wrote on March 12, 2015 at 4:52 am:

The end of freedom comes under the guise of safety. Thanks for the years of freedom, but I don't need or want your “safety”. SELLOUTS!

Gary5 wrote on February 10, 2015 at 1:09 pm:

[...] Goodbye Firefox, it's been a nice few years.

Mathieu wrote on February 11, 2015 at 7:35 am:

The problem is that Mozilla is gonna become the next Apple or Google, moderating away add-ons on subjective reasons. Even if you use the “do no evil” argument, it would be pointless, as it used to be Google’s argument.

Will wrote on February 11, 2015 at 5:04 pm:

Why is there this control-freak fetish going around these days? Apple and iOS, Microsoft and Modern, Chrome and their addons. Now Mozilla? Come on guys, don’t be so freaking unilateral.

Mike wrote on February 11, 2015 at 7:50 am:

Yeah, not being able to disable this is the nail in the coffin.

And many, many more. Surprised Mozilla didn't disable the comments there (like they usually do), knowing how freedom-hating they are. Was this a strategic decision or a moderation fuckup? Regardless, these should at least fill you with some hope; though there are also other comments which - unfortunately - show how some people have fallen hook, line and sinker for Mozilla's marketing. Anyway, time for a summary:

Summary

Okay, that's it for this blogpost. Now, you should be prepared to do the same kind of analysis elsewhere on Mozilla's site (and even other PR pieces, since Mozilla certainly isn't the only corporation using these tactics). Honestly, once you know the ways marketers use their gimmick, it's so transparent - like a magician pulling a rabbit out of the hat, or a cheap card

trick - you will not be taken in anymore. A good way to test your capability to recognize PR-bullshit are the "advancing content" blogposts from the Freedom section.

Shitty developer attitude

Let's get straight to the meat of it. How do the developers respond when users challenge their terrible decisions? Let's look at the removal of JavaScript toggle (archive) (MozArchive) first:

JavaScript toggle removal issue

Some clarifications: - This preference is still available in about:config.

Also known as "the dumpster" - where the dirty options you are not supposed to touch - go. Do you want to dumpster dive in order to change a basic browsing preference? This guy thinks you should.

- There are add-ons such as NoScript or SettingSanity that will do what you want with more easily accessible UI.

Again - according to their research - 65% of Firefox users **do not use extensions**. So they know very well the setting will be unchanged for most people. Why pretend otherwise then?

Turning JS off completely is the wrong security/usability tradeoff for the vast majority of users.

This guy thinks it's **up to him** to decide where you should put yourself on the security / usability spectrum.

The ability to shape your experience (including turning of JS) is offered in many different ways. Not everything needs to be in primary browser UI. We did not actually remove a choice, just reduced the visibility of that particular choice. That does not go against either of these principles in the manifesto.

I'm struggling to find words here to describe this utter contempt for the user. They just threw the most basic browser option into the dumpster, forced you to dive in there if you wanted to find it, and then told you it's not that important and they **did not take away your freedom**. What's next? Having to recompile Firefox to be able to create a New Tab? That would be a "choice" too, according to this dev's logic. Now look at how he replied to a person that didn't like her preferred setting getting changed, without her consent:

Note that if we removed the preference from the UI but left it disabled, this would make life really hard for non-expert users that accidentally changed this, because they're a lot less likely than you are to be able to find out where to change this back.

"We will change your settings for your own good, because you are too stupid to know what you want".

More generally, "add more dialog boxes/infobars" is practically never a solution.

This is in response to a guy that thought there should be a dialog box warning you that a setting has been changed upon update. So the dev thinks he can freely change your settings and does

not need to inform you in any way. And, of course, there wouldn't need to be a dialog box if you just didn't touch the fucking setting!

Mikko and Blake, thank you for your support - keep on rocking the free web!

And then shamelessly suggesting Firefox supports your freedom.

Anyone else who would like to comment: please note that this change was not made lightly; if you believe you have convincing arguments against it or would like it changed, instead of posting here please post to the firefox-dev mailing list: <https://wiki.mozilla.org/Firefox/firefox-dev>

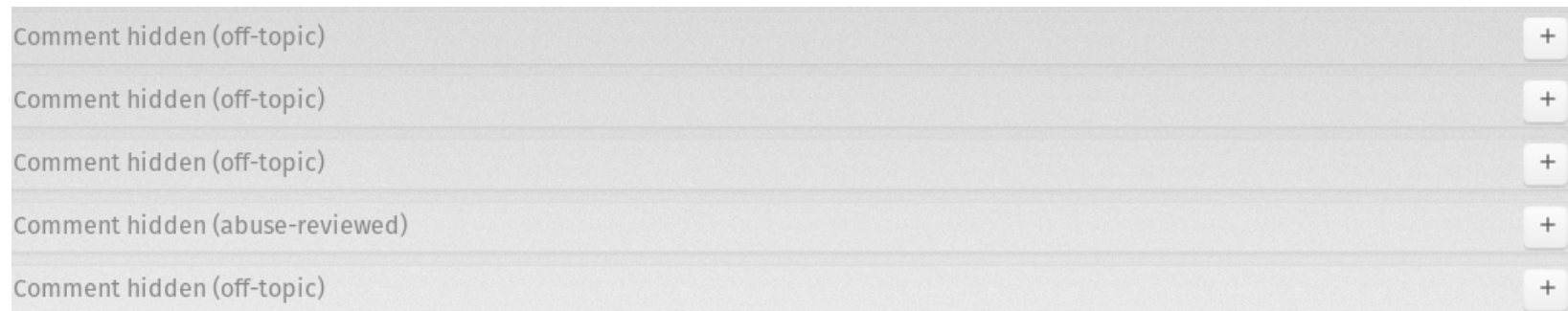
Well, you certainly don't have any convincing arguments **for** deleting the option to disable JavaScript. Stop sending your users to wherever the fuck (that list has a really **shitty moderation policy**, by the way) and actually address the issues! Of course this vermin would rather crawl back under the bed:

I believe at this point, there isn't much point in repeating the same objections that have been voiced previously (see also the points I made in comment 15), and considering some of the language used I will go ahead and restrict commenting to users with editbugs.

Complaining about the **fucking language**? How about your total disregard for the users' feedback, implying they are stupid, lying and shifting the blame? Now let's check out [the PulseAudio requirement \(archive\) \(MozArchive\)](#) complaint, with another dev:

PulseAudio enforcement issue

First, let me tell you what this is even about (though it should be obvious from the title). Version 52 of Firefox had disabled the ability to play audio if you lacked the PulseAudio package installed in your system - even though the **ALSA support code wasn't actually deleted**. And of course, ALSA-only users were angry about it. What was Mozilla's response? Right at the start you are hit with censored comments:



If you're wondering, those comments are not at all offtopic, and the allegedly abusive one is simply in Russian. Anyway, the person responsible for the idea posted this:

What is preventing you from installing Pulse Audio?

Why should someone be required to install your preferred piece of software, just because you have arbitrarily decided to disable the alternatives? When ALSA has worked perfectly for all these years, and the code is still in there, so nothing had to be done to keep having the support for it. This is nothing more than blaming the victim.

The issue is that people may forget that they're using ALSA and not know why their audio doesn't work.

Yeah, a person that **chose to** uninstall PulseAudio would surely forget that they did it. And the

audio doesn't work because you disabled the fucking functionality!

If there are issues with Pulse Audio then please file them with steps to reproduce in a separate bug.

First, we force you to use a certain piece of software that breaks things if you want basic functionality in your browser, then expect you to do our jobs for us and fix its problems. Even single developers of software like ungoogled-chromium or Otter Browser give the user more respect - and this big corpo cannot muster basic human decency. Ethically, they should have either ensured the Pulse backend actually worked properly, or kept the ALSA one available.

TL;DR We're trying to do what is best for Linux and Firefox, so please file bugs if you have Pulse Audio issues.

Why not do what is best for the people - allegedly part of Mozilla's mission? And again, relying on the users to fix your stuff - the same users who **you've ignored** when you created the problem in the first place...

You must be looking at different numbers to me. At the time of making the decision, only 3% of Linux users were missing Pulse Audio.

The source for those statistics is telemetry, which is unreliable, because people (or even distro maintainers) often disable it. One commenter said this:

I am just wondering if you are aware that Firefox telemetry is turned off by default in the version of Firefox supplied to Ubuntu users? Ubuntu does not provide PulseAudio by

default, but relies on ALSA. Since Firefox is the default Ubuntu browser, this decision broke the default browser for all Ubuntu users, a significant number of users, globally.

Even if we took those statistics at face value, it would still be tens (maybe hundreds) of thousands of people for whom Mozilla shamelessly and pointlessly disabled audio functionality in their browsers. Perfectly showcasing the hubris of their developers. Hey, later some big fish came in and said this:

This is a reminder that Bugzilla is our professional working environment, not a place to vent your displeasure.

Then closed the topic:

For the time being, however, I've elected to restrict comments on this bug to Bugzilla users with "editbugs" access.

So, Mozilla doesn't care about the users' opinions at all, even while breaking thousands of working systems. Now for something even more vile, let's check out how they treat **actual long-time volunteers**:

Long-time volunteer DISRESPECTED AND BANNED

I hope he won't mind me writing about him. Filipus Klutiero has been a Firefox user since 2003 and - as I understand it - a Mozilla volunteer since 2004 (his [bugzilla account \(archive\)](#) ([MozArchive](#)) seems to support this). In 2016, he [submitted a bug \(archive\)](#) ([MozArchive](#)) in which he dared to suggest that bugs should not be marked as RESOLVED and WONTFIX at

the same time. This was enough to send the Mozilla bullies after him:

To put it another way, we have firmly decided that we do not view this report as a bug, and hence we will not be fixing it.

let me make this clear: we will NOT be making the change you suggest here, or in bug 1285748. there is nothing you can say that will alter that. pushing on this issue further may result in your account being disabled.

We're right, you're wrong, shut up or we will ban you. And they did:

unfortunately your activities here have left me with little choice but to disable your account. it's great that you're passionate about some things, but you have to pick your battles and stand down when given clear answers and resolutions.

“Stand down”! A fucking military term. Could they have been any more patronizing? Later he posted a report about all the issues he found with Mozilla's project to their [governance mailing list \(archive\) \(MozArchive\)](#). Let's see how they reacted. This is in response to the the above ban:

That said, a disabled account is typically a sign that someone was argumentative or abusive to the point where interacting with them was not being productive at all

By “argumentative” you mean he dared to challenge Mozilla's nonsense. And the actual abusers were the hyenas who first threatened him with a ban, and then finally executed it. Another person commenting on the ban:

When someone disagrees, pace down and come back to it later; don't keep working on them (or the issue) in frustration. From my observation failing to do this has contributed to a majority of bans on the Internet.

Disgusting blaming of the victim. Why not have the bullies “*pace down*” on their banhappy hands?

But just on the off chance that you really are missing something instead of being willfully obtuse

“*Willfully obtuse*”. Now the insults are starting to fly. Who's the abuser here? And then this gem:

This is not a mailing list for disputing decisions made by bugzilla administrators.

What the fuck is it for, then? Again the dirty tactic of hiding under the cover instead of facing the issues. It should also be mentioned that Filipus submitted the report to another list as well, but it didn't appear there. The moral of the story is: there is nowhere to go if you want to complain about Mozilla's bullshit. You can read his take on the issue [on his site \(archive\)](#) ([MozArchive](#)).

Summary

And those are the guys deciding what does or doesn't go into Firefox! I could cite many more examples, but the point should be clear by now. First, Mozilla makes a shitty anti-user decision, then disregards direct feedback (preferring unreliable telemetry), disrespects the users in many

different ways, sends them to some other places if they still have a problem and finally closes the topics or even disables their accounts. Doesn't matter who you are, the hyenas will devour you regardless. But remember, **Mozilla is your friend!**

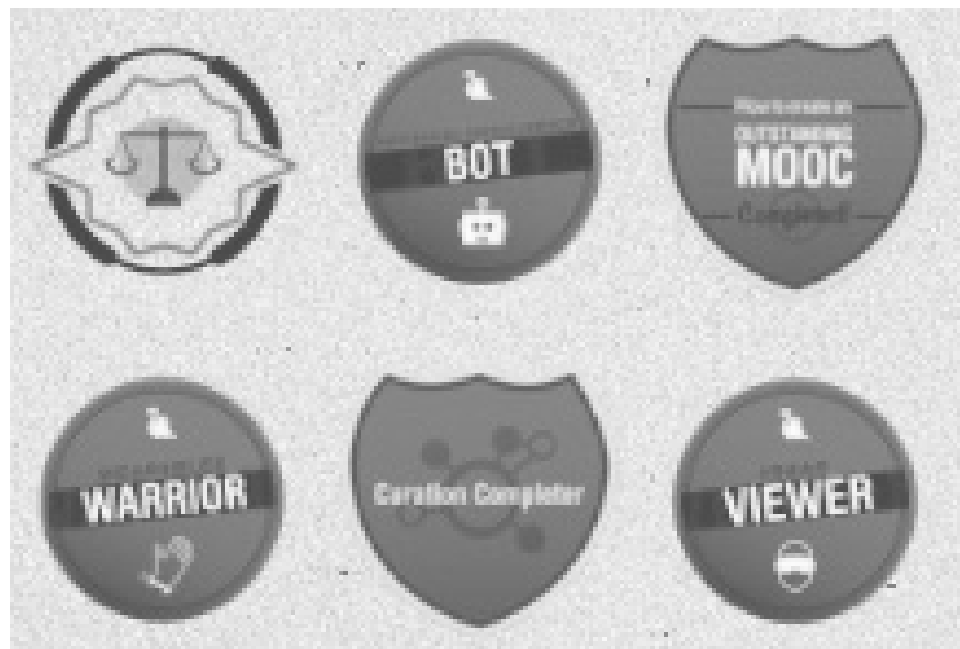
Refuting the manifesto

UPDATE August 2023: by the way, I failed to actually [link to it \(archive\) \(MozArchive\)](#) for all this time. Well, there you go. It seems all the supportive links have disappeared somewhere along the way; I'm keeping the responses though. I guess Mozilla doesn't anymore think that they actually have to fulfill their manifesto principles with anything other than empty claims. Enjoy:

Principle 1

The internet is an integral part of modern life—a key component in education, communication, collaboration, business, entertainment and society as a whole.

That's obvious. And what about it? The “*Learn More*” section on the right contains some useless projects. I don't think I've ever seen someone bragging about his "Open Badges", for example. Even then, it seems these badges are centralized in Mozilla's database ("backpack"), so if Moz goes down, so do your badges. Anyway, for completeness' sake, let's check out the actual badges:



Not very meaningful, are they? Needless to say I don't foresee a good future for this project. Then there is the *“Explore how the web impacts science”* thing. They could have just linked to SciHub if they really wanted to support science, instead of organizing some useless meetups. Wasted opportunity.

Principle 2

The internet is a global public resource that must remain open and accessible.

It is unknown what does Mozilla mean by "open". *“Read about open internet policy initiatives and developments”* links to [this blog \(archive\)](#) (MozArchive), which contains posts such as:

- [The future of online advertising – Mozilla panel discussion at ICDPPC \(archive\)](#) (MozArchive)

- [Getting serious about political ad transparency with Ad Analysis for Facebook \(archive\) \(MozArchive\)](#)
- [Contributing to the European Commission's review of digital competition \(archive\) \(MozArchive\)](#)
- [Mozilla reacts to EU Parliament vote on copyright reform \(archive\) \(MozArchive\)](#)
- [EU Code published: another step forward in the fight against disinformation \(archive\) \(MozArchive\)](#)

The first two are still trying to work with advertisers (the enemies). Next two - with politicians (another group of enemies). And the last one is particularly dangerous, since *“fighting disinformation”* is just another way to call **censorship**. A cursory look at this blog reveals nothing useful there. If Mozilla really wanted to keep the web "open" (whatever that means) - they would do it alone, instead of relying on organizations that don't care about you. Like I am (hopefully!) doing here with this website. What about the other link, [Explore how to help keep the web open \(archive\) \(MozArchive\)](#)? It contains mostly some useless tutorials and then:

Open Practice Competencies

Distinguishing between open and closed licensing.

Contributing web resources using the appropriate licensing to give others credit.

Making web resources available under an open license.

Advocating for the web as an open and public resource.

So, one part of Mozilla's "openness" is the focus on FOSS licenses, which are nice but they don't necessarily ensure quality software. See, FOSS can still be spyware, adware, lack

customizability, have unnecessary features, etc. - and it just so happens that both Firefox and Thunderbird **do suffer** from those flaws. Neither do FOSS licenses ensure being open to user participation in the development - they might let you fix bugs, but try to get them to remove the Firefox spyware and count the seconds until you get told to fuck off (forking doesn't work, you are always playing catch-up, and your fork won't get popular due to the lack of brand name and not being a default in distros). Anyway, basically the only justification for making your source code unavailable is to sell the binary later - therefore, if Mozilla wants an "open web" in the FOSS kind of way, **they should work towards killing capitalism**, since that is the source of the "closed practices". But of course, they are not going to do that - they are mostly funded by Google which obviously benefits from closed source software. They also work closely together with other corporations that also don't care about FOSS. But we don't need to dig that deep - Mozilla includes closed source components ([archive](#)) ([MozArchive](#)) in their mobile browser, so they don't even care about FOSS absolutism themselves.

Principle 3

The internet must enrich the lives of individual human beings.

It already does without your "help", Mozilla. I mean, people can find information about whichever topic they want to. They can communicate with their friends from another continent. Watch movies, play online games, make websites...all without Mozilla's dubious initiatives. Like the Medic Mobile ([archive](#)) ([MozArchive](#)) thing they link to, which would allegedly “connect remote communities to health care” through features like “scheduling maternal health visits” and “monitoring of medicine stock”. Medicine has worked well enough without that stuff, so the usefulness of this is doubtful; regardless, Firefox OS **is now dead**, and the

partnership with Medic Mobile was through it! So this initiative is already gone, and the only other one is [Explore how the web works \(archive\) \(MozArchive\)](#) - and I doubt knowing that “*enriches the lives of individual human beings*”. Hey, the *learning* subdomain is even dead now, so they clearly didn't think they were enriching people's lives that much. Nevermind, there are many tutorials about how the Web works available already, and have been way before Mozilla came along with their initiative.

Principle 4

Individuals’ security and privacy on the internet are fundamental and must not be treated as optional.

Mozilla's alleged privacy focus is refuted thoroughly in the [first section](#) of this article. What about security? Usually, that is a "buzzword" used to bait people into giving up their freedom - read the [relevant section of this report](#), as well as the [fake initiatives article](#), especially the last three sections of it. How about the stuff Mozilla links to on the side of the principle? Needless to say, it's the usual bullshit which has very little to do with real privacy - in fact it distracts from it. Just one example from [the first link \(archive\) \(MozArchive\)](#):

User Control: Deciding who can collect your data

We should all be able to choose – with clarity and confidence – what information we share with what companies, understanding the tradeoffs we’re making when we do.

Right now, we all lack meaningful choice online – privacy policies are often miles long

and hard to read, we don't understand what information we're sharing or when, and opting out is seldom on the menu.

Deciding **who** can collect my data? How about **no one**. Next paragraph is just the same shit - “*what information we share with what companies*”? **Fucking none** is the privacy-focused answer, instead of Mozilla's bullshit. And “*opting out*”? How about opting IN, which simply means **not making data hoarding the default** - exactly what a privacy-supporting organization would encourage - clearly not Mozilla.

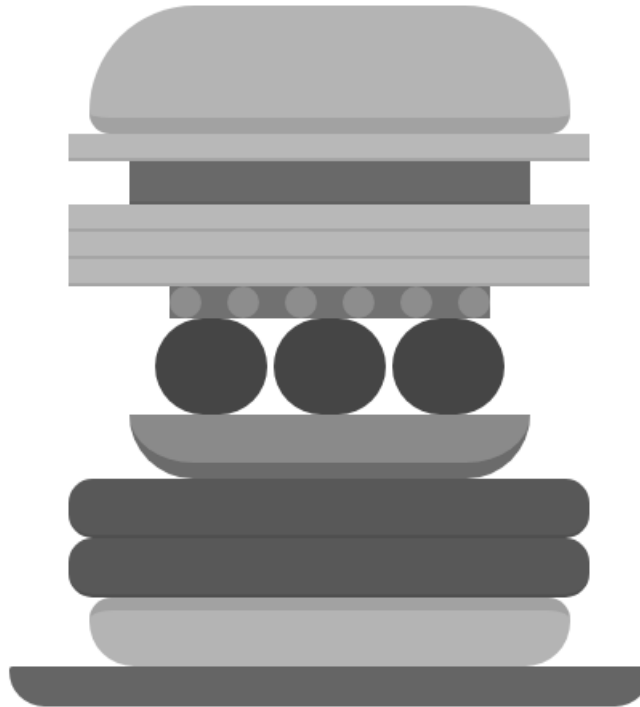
Principle 5

Individuals must have the ability to shape the internet and their own experiences on it.

Yeah, they must, but Mozilla doesn't care about it - as shown in the section Freedom is slavery. And look at the kind of nonsense they link to on the side:

The Best Burger

Only \$9.99



Seriously? **Burgers?** **That's** supposed to teach HTML and CSS? Why not just link to a regular tutorial? Or even to Neocities, so people can actually put their sites up online? And regardless, the fact is that most people will not bother making their own sites, and even those that do will still browse others - so the *“shaping the internet”* should consist of **deciding how those other pages will be displayed**. And Mozilla **absolutely hates** the idea of letting the users control that, as described in the Freedom is slavery section.

Principle 6

The effectiveness of the internet as a public resource depends upon interoperability (protocols, data formats, content), innovation and decentralized participation worldwide.

Wonder what do they actually mean by “*interoperability*”? There's no need to guess anymore - they just tell us [here \(archive\)](#) (MozArchive). As usual, I was too forgiving originally:

The terms "compatibility" and "interoperability" are typically distinguished by browser vendors, where compat refers to site compat, and interop refers to two or more browsers behaving the same. In that terminology, this effort is about interoperability and so the project has aligned with that naming.

Remember when I said that Gecko and Blink might be merged eventually? Well, here's a step towards that. To Mozilla and its big corpo friends, “*interoperability*” means having all browsers work the same. And by all browsers they mean all of **their** browsers - “*agreed on by representatives of three major browser implementations*”. This is yet another attempt of Mozilla to present something negative as a positive. Because - even though e.g the [Wikipedia definition \(archive\)](#) (MozArchive) of “*interoperability*” includes “*producing web pages viewable with nearly every device and browser*” - **Mozilla's Orwellian definition skips the small guy** to focus only on big corpo abominations. What they want to do is to have a single set of web standards that only their own browsers can manage to implement, locking people inside their ecosystem. And since small dev teams can't even begin to follow all the new shit that's being pushed into standards every day, they are forced to base their projects on Gecko / Blink. Giving big corpos full control of the web, which is the goal of this “*interoperability*” scheme.

What about “*innovation and decentralized participation*”? Well, if we used the above definition of “*interoperability*”, that would actually go against innovation and decentralization - since the

standards themselves are centralized. Anytime they come up with a new HTML element, or a new meaning for an old one - it forces the browser devs to keep up. If enough webdevs start relying on these updated elements, older browsers **will not display sites correctly**, forcing the usage of a "modern" browser. Therefore, you can have either *“interoperability”* or *“innovation and decentralization”* - but Mozilla, shady as they are, tries to use as many positive-sounding buzzwords as possible to hypnotize people. They link to a Do Not Track page which is a fake privacy initiative - and it doesn't seem to have anything to do with innovation or decentralization anyway. How about Understand the web ecosystem (archive)? Is this where we finally find innovation or decentralization? Doesn't seem so if it doesn't teach people to actually create and deliver their own websites. Why don't they link to Neocities, IPFS or even the Tor Project? Since those actually support decentralization. But then we're talking about a corporation that's in bed with the heavily centralizing Google, so...

Principle 7

Free and open source software promotes the development of the internet as a public resource.

The openness issue has been covered in Principle 2.

Principle 8

Transparent community-based processes promote participation, accountability and trust.

They sure do, **if they actually exist** - which they clearly don't at Mozilla, as Filipus from the

previous section unfortunately learned. Signing up for the linked governance forum (archive) (MozArchive) seems to **require a Google account**, already discouraging many users from participating (those that don't want to bow down to the botnet master, at least). Of course, you can't just get in - it requires **admin approval** - *“Once confirmation is received, your request will be held for approval by the list moderator.”* Last post has been written 15 days ago at the moment of me typing this, so not many people seem to be getting through. Even if you do manage to do so, there doesn't seem to be much you can affect there. For example this thread (archive) (MozArchive) criticizing Mozilla's usage of Google Analytics - which was posted over a year ago - has been completely ignored. You also have an "opportunity" to *“Volunteer with Mozilla”*- which really means you do the dirty work of localization or organizing events, but still don't get to take part in the decision-making processes. Thus Mozilla - despite claims to the contrary - ends up being governed by a few people at the top.

Principle 9

Commercial involvement in the development of the internet brings many benefits; a balance between commercial profit and public benefit is critical.

What kind of *“commercial involvement”*? The advertisers and trackers you've worked with in many ways? Those bring absolutely no benefit and thus can **fuck right off**. In fact, this whole principle seems to be about easing people into accepting spying - they link to the Lightbeam Firefox extension (archive) (MozArchive), which shows you a nice live graph of all the trackers following you, but **does not block** any of them. If you've read the Shady marketing section, you should notice how the principle quickly changes from *“commercial involvement”* to *“commercial profit”* - read between the lines and you can see that the principle is hiding profit

from ads and tracking behind “*many benefits*”, which are of course never elaborated on.

Principle 10

Magnifying the public benefit aspects of the internet is an important goal, worthy of time, attention and commitment.

We all know the benefits of the Internet and don't need to be told about them. However, you, Mozilla, seem to be doing everything possible to destroy those - like all the stuff described in the sections about privacy and freedom. The most important benefit of the Internet is, of course, **being able to read independent information** - something alien from the world of TV and newspapers. Would you be surprised if I told you that **Mozilla intends to kill that**? They have this thing called Mozilla Information Trust Initiative (archive) (MozArchive) (see the manipulation there?) which will allegedly “*battle disinformation and fake news*” - but around here, we call that **censorship**. They intend to use their own inventions “*like Pocket, Focus, and Coral*” to push certain stories and block others. By the way, that's the kind of thing I've predicted in the Technological slavery article, way before this was done by Mozilla - we will see if this gets used to control the narrative on issues such as GMOs, as I suspect (and fear) it will.

Mozilla's doublespeak

- “*Privacy*” - we collect more data than anyone out there, but...(it's anonymized, you can opt out, we need the data, it's for our mission, it's only used for X, and a thousand other excuses)

- *“Security”, “safety”* - protecting you from yourself, babysitting, we want to push an anti-user change and need an excuse
- *“Tracking”* - what these other bad guys are doing; ours is fine since (it's anonymized, you can opt out, we need the data, it's for our mission, it's only used for X, and a thousand other excuses)
- *“Sustainability”* - we need more money and will exploit our users to get it
- *“Publisher transformation”, “sponsored content”, “relevant content”, “personalized browsing experience”* - (targeted) advertisements
- *“Improve your experience”* - Take away user control
- *“Disinformation”, “fake news”, “propaganda”* - any information which hurts the so-called "elites", to whom we submit
- *“Transparency”* - we will inform you on how we screw you over...sometimes
- *“Openness”* - censorship and digital ID (archive)
- *“Decentralization”* - centralization of the kind we approve of
- *“Choice”, “control”, “power”, “independence”, “shaping your experience”* - choose between options graciously provided by us; as in, red or green apple with all other fruit stacked away
- *“Competition”* - one evil or the other
- *“Volunteer”, “Mozillian”, “activist”* - useful idiot
- *“Interoperability”* - forcing certain standards
- *“Balance”* - add some badness to a good thing, compromise with your enemies (such as advertisers or trackers)

What would Mozilla do

...if they actually cared about the stuff they claim to?

- Allow the installation of whatever extensions you want; XUL or WebExtensions, signed or unsigned, malicious or not.
- Have StartPage, DuckDuckGo or Metager as the default search engine.
- Do not have any data collection in your browser and don't do "experiments" on the users. If you want feedback, just ask for it.
- Actually listen to user feedback. Open up the comments on all the blogposts. Allow free posting on all the mailing lists and respond to the issues raised. Do not close bug reports just because someone challenged an anti-user decision of yours.
- Stand up to the advertisers and trackers instead of allying with them. Make it clear: their nonsense has no place in a healthy internet.
- Include uMatrix-like functionality by default in the browser, with sane defaults.
- Bring all the about:config options back to the UI, where they belong.
- Challenge JavaScript overuse; encourage lean, static sites.
- Provide a hosting service or link to a good one like Neocities.
- Fight censorship instead of alleged *"fake news"*.
- Create private, censorship and control-free alternatives to services people commonly use like E-mail, social media and instant messaging.
- Provide a free Mozilla VPN for every Firefox user.
- Write in-depth articles about encryption, anonymity, advertisement and tracker blocking, browser customization, IPFS, bitcoin, TOR, and everything else that's allegedly part of your mission. Even better - do video tutorials!.

Mozilla certainly has the resources to do all that and much more. There are already groups that

provide much of it while being funded entirely by donations - such as Disroot, Autistici or RiseUp. Even Otter Browser - run by one guy - manages to have absolutely zero tracking, much more customizability (keyboard shortcuts!), and content blocking functionality by default. Mozilla, then, has no excuse whatsoever...except, of course, that they **do not actually care** about all the stuff they spew about, because:

Mozilla's Endgame

This is Mozilla's public image:



This is how they really are:



This is them laughing in your face at the fact that you believed their nonsense:



Don't mind me, I just needed an excuse to use these gifs. And you know the saying - *“a picture is worth a thousand words”*. Anyway, why does Mozilla do what they do? And why do they pretend to do the opposite? To understand that, we will have to focus our attention on another video game - *Deus Ex: Invisible War* (a really good one, by the way - don't listen to the grumpy Deus Ex fans that didn't get exactly what they wanted from the sequel). The game had two factions you could do missions for - The World Trade Organization - the cold-hearted, rule-loving government guys; and The Order - rule-defying, nature loving, spiritual people. Of course it's obvious that different kinds of players would ally themselves with whichever faction is closer to their beliefs. And then, at the end of the game, it was revealed that **both of these organizations were run by the same people**.

I suspect you realize now where this is going. **Mozilla is controlled opposition!** In DX: IW, the Illuminati knew that many people would rebel against the WTO's rule, so they had to create a "good guy" The Order to oppose the "bad guy" WTO. This way, they would direct the opposition where they wanted them and prevent the loss of control. The exact same thing is happening here in the real world - Google (and Apple, Microsoft, etc...) are the "bad guys" - anti-privacy, anti-freedom, pro-centralization, caring about profit and ignoring the user; while Mozilla are the "good guys" pretending to oppose them but really following the same principles. Of course, they have to throw you a bone sometimes, such as *“Do Not Track”* - so the facade is kept and you don't totally rebel - but contributing little to any actual positive change.

This explains everything Mozilla does and doesn't - the focus on marketing, pretending to have a *“mission”*, recruiting *“Mozillians”* to do their bidding. In fact, their tactics are similar to those of religious organizations (such as Invisible War's The Order!) - with repeating certain phrases like it was a freaking prayer (privacy, freedom, openness...) and having meetings and podcasts

which could be considered the equivalent of churches. Except The Order could keep up the facade until the end of the game - they were truly believable. Mozilla - on the other hand - must think you're **dumber than Invisible War's characters**, since it's so much more obvious what they are doing. In addition to all the stuff I've written above, let us consider the more direct evidence:

Cloudflare partnership

Cloudflare is one of the biggest current Internet evils. What is Cloudflare? There is a great overview on [this site \(archive\)](#) ([MozArchive](#)):

It is the world's largest MITM proxy(reverse proxy). It sits between you and origin webserver, acting like a border patrol agent. The origin webserver administrator allowed the agent to decide who can access to their "web property" and define "restricted area".

So, if a site is sitting behind Cloudflare, you will be connecting to it before reaching your chosen destination, all while being unaware that all your information, **including your passwords**, is being decrypted and collected by a third-party on the fly. More than that, it can be used for censorship:

The operator of this CDN possesses great power. In a sense, they control what the end user ultimately sees.

This is just scratching the surface of the issues with CloudFlare. They are often blocking Tor, VPNs, doing invasive "browser checks", forcing people to solve recaptchas, installing tracking

cookies, etc. I highly recommend reading through the above linked site. Anyway, let's check out how Mozilla ended up in bed with this company:

DNS over HTTPS

Mozilla has been planning to do include Cloudflare's DNS in Firefox by default for a long time ([archive](#)) ([MozArchive](#)), and it seems it's finally being pushed ([archive](#)) ([MozArchive](#)). But what is this all about?

Let's first briefly explain how the Web works. Every computer on the Internet has an assigned IP address (such as 198.51.233.100) which tells your machine how to connect there (similar to a physical address if you want to go somewhere). You can actually copy that right now to your address bar and visit the site which has that IP address assigned. Remembering these numbers would be tough for people so we use **domain names** such as neocities.org to surf the 'net instead. However, these are not understood by the network, which is where the DNS servers come in. The DNS server takes the domain name and turns it into an IP address, allowing seamless traveling through the Web. By default, you will be using your ISP-assigned DNS servers (so people from different parts of the world all have a different one). Mozilla, however, seeks to change this.

DNS over HTTPS would make every Firefox user use the same DNS server by default. So, whether you're browsing from the Faroe Islands, India or Cameroon, all your requests will be routed through Mozilla's chosen DNS. Which just happens to be **Cloudflare's**. This means **all your requests will be routed through it** (see above for the explanation for why that is bad). Cloudflare allegedly has a privacy agreement ([archive](#)) ([MozArchive](#)) with Mozilla, which will

prevent them from storing certain data. However, this is the same company that has **no problem with storing your plaintext passwords**, and Mozilla is untrustworthy itself (as this report aims to prove), so the value of this agreement is negligible.

Cloudflare is now powering over a tenth of the Internet's websites ([archive](#)) ([MozArchive](#)). For those sites it gets access to **all the information** flowing in and out of them, including - again - your decrypted passwords, private messages, etc. But it wasn't enough for the spy company, so they are now trying to make their DNS more popular through the Mozilla partnership, and **collect info for all sites**, not just those behind Cloudflare. They've also graciously provided us with the exact data they will put their dirty hands on:

Timestamp, IP Version (IPv4 vs IPv6), Resolver IP address + Port the Query Originated From, Protocol (TCP, UDP, TLS or HTTPS), Query Name, Query Type, Query Class, Query Rd bit set, Query Do bit set, Query Size Query EDNS, EDNS Version, EDNS Payload, EDNS Nsid, Response Type (normal, timeout, blocked), Response Code, Response Size, Response Count, Response Time in Milliseconds, Response Cached, DNSSEC Validation State (secure, insecure, bogus, indeterminate), Colo ID, Server ID

The main take-away is that the traffic of every Firefox user will now be collected by the honeypot Cloudflare. Since DNS servers are also traditionally used to block sites, and Cloudflare has deplatformed sites before ([archive](#)) ([MozArchive](#)), we could expect them to become a kind of government, deciding which sites you can view or not. Again, this is just the tip of the iceberg, so read this site ([archive](#)) ([MozArchive](#)) to know more. A browser-based DNS would also bypass the system-wide hosts file, which is used to block ads (among other things) by a lot of people. Mozilla - as usual - pretends that their anti-user choice actually benefits you, and also assures you there's an about:config option to disable the DNS. But as

explained in [Freedom is slavery](#), it's not likely to remain there, so don't rely on it. An OpenBSD contributor has gone so far as to **remove the offending code change** from their Firefox package. Here's what he [has had to say \(archive\)](#) ([MozArchive](#)) about Mozilla's decision:

Disable DoH by default. While encrypting DNS might be a good thing, sending all DNS traffic to Cloudflare by default is not a good idea. Applications should respect OS configured settings. The DoH settings still can be overridden if needed.

Firefox Private Network

Another thing Mozilla wants to integrate into Firefox is the **Cloudflare "VPN"**, shamelessly called the *“Firefox Private Network”*. Let's look at how Mozilla advertises it:



So the point is to guard you from those damned “*hackers*”. However, what Mozilla neglects to mention is that with their "private" network, **Cloudflare takes the place of the hacker**, whom you directly connect to and who has much more resources at their disposal than a random "hacker". In fact, hacking is Cloudflare's **entire modus operandi**, breaking your SSL and serving you modified websites:



According to Mozilla, there are other reasons to use their network, such as:

Internet Protocol (IP) addresses are hidden so it's harder to track you – Your IP address is like a home address for your computer. One of the reasons why you may want to keep it hidden is to keep advertising networks from tracking your browsing history. Firefox Private Network will mask your IP address providing protection from third party trackers around the web.

Of course, this is a **total lie**. Do they really not have any actually security-aware people working there? Hiding your IP alone does **nothing whatsoever** to block trackers - all the scripts and requests can still happen, just that they're going through Cloudflare first (which is a tracker in itself). And then:

Toggle the switch on at any time. By clicking in the browser extension, you will find an on/off toggle that shows you whether you are currently protected, which you can turn on

at anytime if you'd like additional privacy protection, or off if not needed at that moment.

So they're doing nothing than an extension such as Browsec VPN doesn't already do. Except Browsec is likely more trustworthy than Cloudflare - but nothing replaces a real, system-wide VPN, of course. To make matters worse, Mozilla will be **making the feature paid for**, right after their lab rats...oops, I mean *"loyal group of users"* provide enough data / feedback (filling surveys) for Mozilla to "offer" the "service" to everyone else. This quote at the end sums it all up:

Sign up now for a Firefox account and join the fight to keep the internet open and accessible to all.

Is this their slick marketing again, or do they really believe their own bullshit? Cloudflare integration is easily explainable not by a dubious privacy or security gain, but by the fact that it's **another head of the hydra** - providing a unique central point for much of the Internet's traffic, allowing undetectable mass collection of plaintext passwords, private messages, etc. And Mozilla aims to increase its influence by redirecting Firefox's traffic to them.

Sacrificing readers at the Cloudflare altar

A few months ago (maybe at the end of 2022, or beginning of 2023), many of Mozilla's subdomains such as *foundation.mozilla.org*, *hacks.mozilla.org* and *blog.mozilla.org* became CFed. Annoyingly, this means I cannot MozArchive their blogposts directly or even read them by RSS. Either way, with this, **all of Mozilla's alleged principles** (such as freedom, openness, privacy, security) **went out the window**. Openness is killed because CF blocks anything non-mainstream. Security - because it does MitM. Freedom - because it can censor (archive)

([MozArchive](#)) or modify sites. And privacy because it does data collection. Hey, we always knew Mozilla doesn't care - but now it's literally in your face. Remember when I told you Mozilla was a bridge? Now we have another proof. It's the model head of the Hydra, designed to lure you in and throw you towards the other heads that ultimately eat you. Now the process became more automatic - with no sign-ups, downloads or anything like that. They simply throw their users right inside the abuse train anytime they stumble upon a Mozilla page. Oh, and this makes the deprecation of HTTP or old TLS versions take on an entirely different meaning. It wasn't ever about security, just control; since by whoring themselves to CF here, they are entirely killing SSL - yet it doesn't bother them at all.

Second head of Google

BIG BROWSER
IS WATCHING.

BROWSE FREELY WITH 

CLEAR CHANNEL



If you knew nothing about the situation, you'd assume that Google is the bad, spying guy and Mozilla is your privacy-loving antidote. There are several other places where Mozilla seems to oppose them, like in [this anti-Google piece \(archive\)](#) (MozArchive), or [another one \(archive\)](#) (MozArchive). Have some quotes from the first article:

With roughly 90% of the global market share for search across all devices in 2017 [...] Google Search is bolstered by its mobile operating system Android and browser Chrome [...] Because it can leverage its market dominance to advance its commercial strategy [...]

And the other one:

Google's primary source of revenue is displaying and selling ads. [...] A lesser known effect of Google's dominance is that the company has the power to define and implement features of how the Web works for everyone [...] This is an unfortunate vector of competition, because Google can push for standards or formats that other browsers can't or don't want to deliver on

Mozilla sounds really bothered by Google's domination of the Internet. And yet:

- They, for many years, have had Google as the default search engine
- They have an active YouTube (owned by Google) channel
- They include Google Analytics on their about:addons page
- They use Google's invisible reCAPTCHA on some of their pages
- They have DoubleClick ads (Google-owned) on their Download Firefox page

So, their opposition to Google is by words only. Their actions seem to show complete

allegiance to them. And it's not like they have to do this - there are alternatives to all of those listed things. DuckDuckGo, Metager or StartPage as the search engine, Rumble for videos, text-based captchas or none at all. They could help make some of those small guys popular, but they would rather ally with the big guy. Almost as if that was **part of the plan**...Okay, enough with Google, let's move on to the others:

Other "giants"

Some quotes from various articles:

These touch points are opportunities to position Mozilla as a trusted independent body on the internet that's challenging the tech giants (archive) (MozArchive)

[...] thus consolidating the power of existing tech giants [...]

It turns out, the web is not the open road many of us imagine — it's full of private lanes, cul-de-sacs, toll roads and sneaky detours designed to divert traffic where tech giants guide it. (archive) (MozArchive)

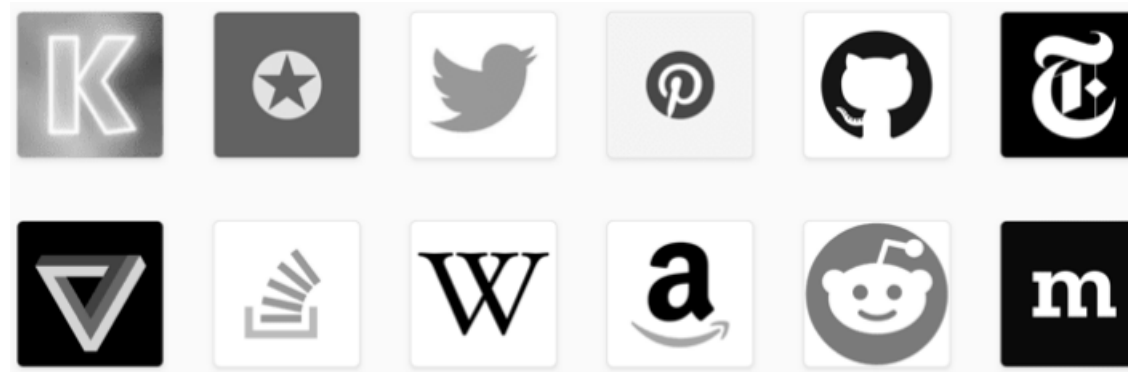
[...] thus allowing a relatively small organisation like Mozilla to compete with corporate giants [...] (archive) (MozArchive)

We know we're up against billion-dollar giants [...] (archive) (MozArchive)

Social media giants Facebook, Tencent, Google reign (archive) (MozArchive)

Monopolies are growing in influence, with a handful of tech giants acting as gatekeepers to access and information. (archive) (MozArchive)

The implication is that Mozilla is the small guy challenging the “*giants*”. Who are those giants and what is Mozilla's real relationship with them? Let's look at their main page:



What do we see here? A bunch of “*giants*” including Twitter, GitHub (recently acquired by Microsoft, remember!), Amazon, Reddit and...themselves (are they sneakily admitting they are also a giant?). They have **two Twitter channels**, an Instagram account (Facebook-owned), and their source code is hosted on GitHub. I don't have to tell you the alternatives to all these things, right? If the centralization of the Internet in the hands of the “*giants*” bothered them so much, don't you think they'd use some of those? Now look at their [holiday shopping guide \(archive\) \(MozArchive\)](#). Already at the top we see products from “*the giants*” described as “*Not Creepy*”, even though Mozilla themselves admit that they share “*your information with 3rd parties for unexpected reasons*”. Now what does Mozilla do when one of the “*giants*” does something that they allegedly oppose? Let's check it out:

- [Amazon Echo Kids \(archive\)](#) device has a [problematic policy \(MozArchive\)](#) in regards to collecting children voice recordings. For example: “*voice recordings are also*

used to improve your child's experience and our Alexa and FreeTime services, for instance by training our speech recognition and natural language understanding systems". What is Mozilla's response? They ask them to clarify ([archive](#)) ([MozArchive](#)) how they're *"safeguarding kids' privacy"*. No warnings about the actual policy. And they claimed victory because Amazon now **graciously explains** how their device spies on kids. How shameless.

- *"50 million Facebook users had their information used by Cambridge Analytica, a private company, without their knowledge or consent"*. And what was Mozilla's response? A fucking petition ([archive](#)) ([MozArchive](#)). As if those have ever worked! Then they created an extension called Facebook Container ([archive](#)) ([MozArchive](#)) which prevents FB from tracking you through like buttons on third-party sites and such. But all the data collected directly by Facebook remains untouched. And look at the manipulative title: *"Being open and connected"* - as if FB was the only way to accomplish this!
- When Microsoft changed the users' settings through their Windows 10 auto-update (sound familiar?), Mozilla wrote a fucking letter ([archive](#)) ([MozArchive](#)) trying to get them to *"respect people's right to choose"*. As an aside, how hypocritical of them when they've done the exact same thing with Firefox updates many times...

Three sins of the *"giants"*, and three times Mozilla has tried to work with them instead of boycotting them. And they've had such good opportunities to get people to try some of the alternatives out. But that's the one thing they absolutely could not have done, because...

The Hydra

Okay, it's time for the final conclusion. Google, Microsoft, Apple, Facebook, Twitter, Amazon, Cloudflare and Mozilla are all **different heads of the same hydra**, looking to control the Internet and the world. And Mozilla's job in all of this is to **be a bridge** between the rebels - those people who would at least consider not using Google and co - and the controllers, to keep them in the web of slavery. They lure users with promises of privacy, freedom, openness, whatever - and they try to make the other parts of the control scheme seem more palatable, with stuff like the Facebook Container or pretend compromises with them. All while neglecting to mention any of the alternatives so that you keep being trapped in the web of slavery. For the final proof, let's look at the times all the heads of the hydra have worked together for common aim:

- <https://www.euractiv.com/section/digital/news/eu-code-of-practice-on-fake-news-tech-giants-sign-the-dotted-line/> (archive) (MozArchive) - *“A group of tech giants including Google, Facebook and Mozilla have agreed to abide by landmark new standards set out by the European Commission in the battle against the dissemination of fake news across the EU.” “The industry is committing to a wide range of actions, from transparency in political advertising to the closure of fake accounts and demonetisation of purveyors of disinformation”*. So they are working together to end *“disinformation”* - in other words, **cancel the Internet**. And they will *“demonetise”* you if you engage in the spread of so-called *“disinformation”* - so you won't be able to earn advertisement money if you dabble in alternative, unapproved content.
- <https://redmondmag.com/articles/2017/07/25/adobe-ending-flash-support.aspx> (archive) (MozArchive) - Mozilla, Facebook, Google, Microsoft, Apple and Adobe have agreed to end Flash support. They have also worked together to create a new codec (archive) (MozArchive).
- <https://arstechnica.com/gadgets/2018/10/browser-vendors-unite-to-end-support-for->

20-year-old-tls-1-0/ (archive) (MozArchive) - Apple, Google, Microsoft and Mozilla end TLS 1.0 support. Maybe this isn't so terrible, but still shows they DO make plans together. Google and Mozilla are also looking to kill HTTP entirely, as described in my Fake initiatives article.

- The “giants” have also staged a net neutrality protest - <https://www.washingtonpost.com/news/the-switch/wp/2017/06/06/amazon-kickstarter-reddit-and-mozilla-are-staging-a-net-neutrality-online-protest/?noredirect=on> (archive) (MozArchive).
- In August 2022, Mozilla has recruited (archive) (MozArchive) a dude with a past at Twitter, Facebook, and 14 fucking years at Microsoft for their “*product officer*” position. If this is not absolute proof of Mozilla being a bridge, then what is?
- An even better proof came around in November 2023. I'll just let Mozilla's quote (archive) (MozArchive) speak for itself: “*You can now sign in across Mozilla’s products with your Google or Apple ID. Using your Google or Apple ID makes it easy to authenticate your identity and recover access to your account*”. They are totally fighting the “giants”...while cucking to them.

There is more but you get the idea. Especially the first link is telling - they're conspiring to censor the Internet - it's simply out there, clear as the sun, undeniable. Anyway, the true endgame is **consolidating the control of the Internet and computing in a few hands**. Here are some recent examples of this happening right in front of your face:

Consolidation of power

- Yahoo, since October 2007, is part of Oath company, which also owns Tumblr, AOL

and others (and itself is just a division of Verizon) - <https://policies.yahoo.com/ie/en/yahoo/privacy/eu oathnoticefaq/> (archive) (MozArchive)

- Microsoft dumps its EdgeHTML rendering engine in favor of Chrome's Blink - <https://blog.mozilla.org/blog/2018/12/06/goodbye-edge/> (archive) (MozArchive).

Therefore, there are now realistically only two big players for displaying the web: Gecko and Blink - and considering the closeness of Mozilla and Google, the two might be combined eventually.

- Microsoft acquired GitHub in June 2018 - <https://news.microsoft.com/2018/06/04/microsoft-to-acquire-github-for-7-5-billion/> (archive) (MozArchive). This is the same company that has abused Windows users for years with their malicious auto-updates. The deal will be finalized at the end of the year; we will then see what it means for GitHub. **UPDATE October 2024:** some things it now includes are a brutal captcha just to register, forcing JavaScript for most functionality, and mandatory two-factor authentication for repository owners (AKA you need to give them your phone number).

- SystemD is an init system for the Linux kernel whose aim is to *“unify basic Linux configurations and service behaviors across all distributions”*. Now Linux has historically been a "create / choose your own" kind of system, and this changes everything. [Here](#) (archive) (MozArchive) is a list of "features" that SystemD has swallowed plus other arguments against it. Many packages are now dependent on it, and pretty much all except some niche distros have adopted SystemD by default. Here are some quotes from various articles about the dangers of it:

[Linus Torvalds and others on Linux's systemd](#) (archive) (MozArchive):

But as systemd starts subsuming new functions, components like network-manager will only work on systemd or other components that are forced to be used due to a network of interlocking dependencies; and it may simply not be possible for these alternate desktops to continue to function, because there is [no] viable alternative to systemd supported by more and more distributions

Why I dislike systemd (archive) (MozArchive):

There is no one thing about it that makes it bad software, but taken as a whole, I believe it creates more problems than it solves. Sadly, many of those problems will take years to become apparent, by which time all the major Linux distributions will have fully integrated it.

systemd: Please, No, Not Like This (archive) (MozArchive):

To be blunt: My personal verification step is over. I do not like systemd, its design, its implementation, how it is maintained, how (some of) its developers and proponents intentionally alienate whole groups of people, how even valid criticism of it is often declared irrelevant, and I have real trouble with the attitude of many of the people associated with its ecosystem. The whole thing annoys me more than it makes my work simpler, and the situation makes me feel like the things I value in open source and software engineering are being actively undermined.

Another problem with SystemD is that it is controlled by Red Hat - a corporation recently acquired (archive) (MozArchive) by the hardware-producing giant IBM. This

makes Red Hat an *“Linux oligarchy, a narrow circle of developers, mostly located in corporations and working on Linux full time, who "knows best" what is good for the community, and which does not care about interests of Linux "deplorables"”*.

The RSS deprecation conspiracy

Look closely and tell me the most important difference between these two images (the first is an unidentified, pre-2011 Firefox version; the second - version 91):



If you guessed the suspicious disappearance of the orange rainbow button right at the end of the address bar, congratulations - you win (no prizes though). What does this button do, you ask? Well, it allows you to subscribe to an Internet page so that it is able to notify you of the updates for it in a program called an "RSS client". Anyone who is aware of this technology knows it is absolutely indispensable for efficient internet browsing. This screenshot of QuiteRSS should explain it better than a thousand words:

TorrentFreak - QuiteRSS

File View Feeds News Browser Tools Help

TorrentFreak

Find in News

Star	Check	Title	Author	Published
★	✓	Nintendo v. Pomelo: Yuzu-Based iOS S...	Andy Maxwell	15.11.24
★	✓	Men Arrested in Magis TV Piracy Raids ...	Andy Maxwell	14.11.24
★	✓	FMovies Piracy 'Mastermind' Confesses...	Andy Maxwell	13.11.24
★	✓	Dutch Court Orders ISP to Block Torrent...	Ernesto Van der Sar	13.11.24
★	✓	Google's "Negligent" Piracy Response ...	Andy Maxwell	12.11.24
★	✓	Piracy Kingpin Behind 'Noonoo TV' and ...	Ernesto Van der Sar	12.11.24
★	✓	Per-Song or Per-Album? Record Labels...	Ernesto Van der Sar	11.11.24

Dutch Court Orders ISP to Block Torrent Site TorrentGalaxy 13.11.24 12:42

Author: Ernesto Van der Sar | Comments | Piracy

Pirate site blocking is one of the entertainment industry's favorite enforcement tools. In recent years, it's become a common practice in many countries around the world.

In the Netherlands, it took over a decade for the first order to be approved. After detours through the Supreme Court and the EU Court of Justice, the final order was issued in 2020, targeting The Pirate Bay.

With all the legal paperwork in order, the doors were open to more blocking requests, especially after rightsholders and local ISPs signed a covenant to streamline the process. If a court orders one company to block pirate sites, by agreement the other ISPs will follow suit.

Categories

Unread: 80 All: 95

A single look at this should make the extreme increase in efficiency obvious. All you need is to click the *“Update All Feeds”* button (double-orange arrows) to learn of everything that has

happened on your chosen websites (or podcasts, forum threads, youtube / reddit profiles, etc...) since the last time you checked. You can then look at all the recent news headlines and fully read the ones that interest you. Perfect for busy people who still want to know what's going on in the world.

Now imagine trying to do that **without** using RSS. You'd have to either remember all your favorite sites, or bookmark them in your browser. Then visit them separately and wait until they graciously load their bloated menus, social media buttons, spy scripts, advertisements, and other frills. Usually, only a few news headlines will fit on the screen either way, so you'd have to switch pages to learn anything that has happened before today (assuming the website's interface even allows you to do that). This will quickly get boring and you will probably stop after doing this with one or two sites. While the RSS Chad already knows everything that has happened in the world during the last few days in just a few minutes, the web browser virgin is only **maybe** getting finished with one website, and has to ignore the other 20 he'd like to check, because it's taking too long and the frills are already becoming annoying.

Coming back to the Firefox address bar screenshots, somewhere in 2010, Mozilla had decided (archive) (MozArchive) to kill the button. This was the "rationale" of *Alex Limi (:limi)* — *Firefox UX Team*:

The reason is that RSS as a user-facing feature isn't really used much, and pretty much all sites that want you to subscribe to their feed will have dedicated icons/links on their website to do this.

Later commenters have proven an about 10% usage rate; so yes it is indeed “*used much*”. And the real usefulness of the feature will be underestimated, because just looking at it teaches you

that RSS exists (and that the website supports it), and this won't be tracked by stats.

Having it as a top-level UI element (especially when it isn't clear what it's really for) doesn't make a lot of sense. We see people clicking it erroneously — and even when they click it on purpose, they don't understand what it does, and it becomes one of those buttons they just "stay away from".

If someone clicks the button “*erroneously*”, then he can just close the menu that appears. No pain will be incurred during the procedure. But maybe the person will get interested in trying something new and useful. As kids, we did all kinds of interactions with computer software, and our brains did not explode. Why assume that the average Firefox user is somehow incapable of the same?

I use the button myself as a convenient shortcut (just so you don't think I'm any kind of RSS hater ;), but it's hard to justify the prominent placement it currently has.

"The RSS button for me, but not for thee". What a joke. The “*prominent placement*” is justified by the fact that you instantly know if the page you're on has an RSS feed available. Anyway, Mozilla's plans were already criticized early on in the very same thread they were suggested. For example, *Marco Bonardo* said:

What's the need of hurrying in removing that small icon? locationbar has usually a lot of blank space and it doesn't look like cluttering the UI. Even if web pages give their own ui to subscribe feeds, it's often hard to find it, there is no standard in presenting that, and we are assuming user wants to lose time searching for a small icon in the page, when we were giving him a fixed point where to look to discover feeds. If I should vote, it'd be a

"no thanks".

Please Ignore This Troll (Account Disabled) said:

wowowow, guys, please don't remove RSS button - it also serves us as an indicator whether the page has RSS feed or not. If you hide it behind the bookmarks - people will have to click it everytime they need just to check whether the site has an RSS feed or not. [...]

Yes, I think the better solution would be to enlighten and educate people what is RSS used for, instead of hiding it, like it is something evil that should be kept away from users.

Since I know mozdev management doesn't care about users' opinion - could you at least not cut this feature but just use the "display:none;" for it, so users like me could easily enable it by a userstyle?

Sucks how someone with such sane takes got banned. I guess Mozilla really doesn't like it when you bluntly expose their stupid and malicious behaviors. Presumably, they also changed his name after the ban (since I doubt he'd call himself a troll) - an evil I've literally never seen happen anywhere else. Continuing - *Oleg* said:

Sorry, but it is very stupid decision. Please don't remove this button. We don't need yet another add-on like Element properties, Go Button, etc.

VeRtex said:

Please do not remove the RSS icon in the location bar! And if so want to remove, then do in the Preferences another tab "RSS", which among other settings, the output feeds, was able to return the icon in the location bar.

It's funny how regular people can figure out what's the right course of action, but Mozilla's supposedly professional “UX Team” keeps chasing its own tail. Here is another insane argument in favor of the removal (by *Dave Garrett*):

[...] I would personally like the button to stay, yes, be we, us here, people who know how to use a computer, are not the only audience to aim for. This is the one button in the top level GUI that is remotely "advanced", i.e. not immediately figure-out-able by someone who doesn't know what they're doing. They need to use the Internet too. [...]

Again, the standard "if your grandma doesn't use it, we are trashing it" Mozilla illogic rears its ugly head. She could still use the Internet, and simply ignore the button. While the tinkerers have something new to play around with. What's the problem?

*Firefox's raison d'être is addons. At least one addon will be created to add this back, probably with new and better features. As was said prior, this you can count on, always.
;)*

Mozilla knows very well that this doesn't work. 60% of people do not install any extensions, while those that do, focus almost entirely on adblockers and additional languages. And they will never install an RSS extension if they don't even know what RSS is. The most installed RSS addon clocks at only 48775 users (November 2024); the second - at 14715. The others have a few thousand installs at most, and together they all add up to under 100k, which is less

than 0.1% of Firefox users, or about one hundred times less than the in-built button's usage stats. Mozilla has access to all this data and perfectly realizes how removing this feature from the UI was basically equivalent to removing it from the public consciousness. Anyway, after the standard "just use addons!" Mozilla excuse to delete features, *Alex Faaborg* [:faaborg] (*Firefox UX*) has appeared and said this:

I would to once again provide a calm and polite reminder for everyone to debate this change on its merits, as opposed to personal preference and personal attacks.

You have repeatedly ignored the “*merits*” and stuck to your moronic anti-user decisions, as usual. That's the opposite of “*polite*”. In fact, the only impolite posters were the supporters of this change, who called any criticism “*spamming*” or told the critics to “*shut up*”. And to say that there have been no arguments aside from “*personal preference*” is simply gaslighting.

Anyway, partial RSS support (through menu options) still remained in Firefox after this circus show, but due to the lack of indication that the website you're on supported RSS, it was basically useless. Yet, they couldn't stand to keep including even the gimped implementation and killed it entirely (archive) (MozArchive) 8 years later:

While we still believe in RSS and support the goals of open, interoperable formats on the Web, we strongly believe that the best way to meet the needs of RSS and its users is via WebExtensions.

The old adage of judging people by their actions - and not grand pronouncements - applies perfectly here. If you really cared about “*open, interoperable formats*”, you would not have touched the address bar button in 2010 in the first place. Now RSS support is completely gone

from Firefox, and a young person just getting onto the Internet for the first time today, will not even get reminded that it exists. Especially since Google's, Microsoft's, and Apple's web browsers also now lack the support ([archive](#)) ([MozArchive](#)) (proving yet again their cooperation behind the scenes).

What does the RSS deprecation conspiracy accomplish? Again, it heavily decreases efficiency at reading and thus makes people less educated, which helps the psychopaths running this world. Additionally, it puts the control of the Internet browsing experience into the hands of the corporations, forcing you to view their ads and run their spyware scripts while they gain profit from the collected data. And - since RSS / Atom are real standards ([archive](#)) ([MozArchive](#)) and not fake big corpo "living standards", you are not required to install the newest piece of software just to view a page, and in fact will be fine with a two decades old client - *“Therefore, the RSS spec is, for all practical purposes, frozen at version 2.0.1”* (which came out in July 2003). By the way - Pale Moon, SeaMonkey, Otter Browser, and other niche browsers still support the button, but obviously are not defaults pretty much anywhere and won't reach more than 1% of people, who probably already know of this technology. That is why the conspiracy between the "big four" of browser companies is so effective.

Summary

I could go on, but you get the idea. The amount of hands controlling the Internet, computing and the world is becoming smaller and smaller. Or, it is simply being **revealed** to us at the so-called "elites" chosen pace. And Mozilla's job in this is to use the boiling frog strategy to keep you content. They are the real world's The Order. In Invisible War, one of the main characters even **cried** when you told her that the WTO and The Order were two faces of the same

organization. I hope you won't cry when I tell you the same. Except in this world, it goes much further. **All the "competition" between the corporations is FAKE.** Like left vs right, black vs white, woman vs man, Mozilla vs Google - all manufactured so that you're fighting useless wars while The Hydra uses its many heads to accomplish its aim of controlling the world. In Greek mythology, you had to burn the hydra's neck to kill it - if you just focused on its heads it would simply regrow new ones. And that is what we have to do here, if we want to change the situation.

The death of Mozilla?

I suspect you have heard of the US government looking to inhibit Google because of their monopoly on browsers, searches, etc. Well, one way this is supposed to be accomplished is for Google to be banned from paying browser companies to put their search engine as the default (archive) (MozArchive) - *“Perhaps the most straightforward request is a ban on Google striking exclusionary contracts for preferred placement of its search products on browsers and phones. Google would be banned from entering revenue-share agreements to distribute its search product or offer anything of value to Apple, Android phone-makers, or browser companies for any kind of default preinstallation or preferred placement”*. Mozilla is now complaining about it (archive) (MozArchive) so it seems to be coming closer. They wrote to court (local) trying to prevent them from implementing their ideas:

As detailed in its motion seeking leave to file the instant amicus brief, Mozilla has a strong interest in this litigation because the remedie ordered by this Court could force Mozilla to exit the browser and browser engine markets, as well as significantly impair the ability of Mozilla and its parent company, the Mozilla Foundation, to achieve their

public oriented mission.

The last twitches of the dying fox desperate to escape the jaws of the crocodile. Nice for them to admit that Google has kept them alive for the entire time though. Yet they don't mind bullshitting even the courts, that is how shameless they are:

For two decades, Mozilla—a wholly owned subsidiary of the non-profit Mozilla Foundation—has fought for an open and healthy internet ecosystem that promotes the public good. 1 Among other things, Mozilla has developed open source products that foster innovation and prioritize user privacy and security over profits; advocated for web standards and legislation that promote competition and enable users to control their online experience; and spoken out against unfair and deceptive business practices.

This is all a joke. But I don't want to repeat myself, so let's continue:

As Mozilla's Chief Financial Officer, Eric Muhlheim, testified, the Proposed Distribution Remedies, if applied to Mozilla, would present an "existential threat" to Mozilla's business and public oriented mission. This testimony is fully corroborated by the uncontroverted evidence before this Court, which shows that the Proposed Distribution Remedies would eliminate approximately 85% of Mozilla's U.S. annual revenue by preventing Mozilla from being compensated for setting the highest quality and user preferred search engine, Google Search, as the default in its Firefox browser.

Another admission that they will die if the Google money faucet is turned off.

Importantly, the Proposed Distribution Remedies would also drastically impair Mozilla's

ability to maintain and improve its open source Gecko browser engine, which is “the heart of Firefox,” powers other independent browsers, and the only non-Big Tech browser engine. If Mozilla exits the browser engine market, this will give Apple and Google, as the owners of the other two browser engines, greater control over web standards.

You are Big Tech, too. Besides, WHATWG had long agreed that all the major browsers are supposed to work the same. So there is no **actual** competition in engines either way. As I wrote earlier, the "HTML living standard" is cancer that keeps out independent browser engine devs, and Mozilla is in favor of it.

As detailed below, these competitive harms to the browser and browser engine markets can be avoided by exempting Independent Browser Developers like Mozilla from the remedies entered in this litigation, which would not sacrifice the efficacy of this Court’s ultimate remedies in any way.

How are you “Independent”, when you are on life support called Google?

Ironically, if Plaintiffs’ remedies force Mozilla to exit the browser market, users will be left with fewer browser choices.

Not necessarily. When the controlled opposition is gone, people might actually seek out true opposition.

Consistent with the Mozilla Foundation’s mission, Mozilla has managed Firefox in a manner that places people and societal benefits above profits. 6 For example, based on its

belief that “privacy is fundamental to a healthy internet,” Mozilla collects limited user data 7 and has integrated market leading privacy and security features into Firefox, including:

Lol! I hope the judges don't buy this. I mean, the fact that this legal situation even exists disproves it. Because Mozilla would rather keep an anti-privacy, for-profit (ad-driven), censorious (anti-user) search engine as the default, than cut their earnings but put something actually respectful.

This Court has rightly noted that the Proposed Distribution Remedies could force Mozilla to exit the browser market because “Firefox [] depends on Google’s revenue share payments for its very survival.” 1/27/25 Order at 18. 29 Such a result would give Big Tech browsers greater control over the browser market and leave privacy conscious users with fewer browser choices.

Actual privacy conscious users are not using Firefox.

Plaintiffs have attempted to downplay the competitive harm that the Proposed Distribution Remedies will cause in the browser and browser engine markets by suggesting that Mozilla could easily replace its lost Google search revenue. The uncontroverted evidence proves otherwise.

Once again Mozilla admits to being sustained (almost) entirely by Google.

If Yahoo—a company owned and backed by a private equity firm with \$785 billion in assets under management—concluded that it could not sustain a browser without Google

Search as the default, there is absolutely no reason to believe that Mozilla, a much smaller company owned by a non-profit, would have more luck doing so.

Similar things have come up quite a few times, and my reply to all of those is: then so be it! As I've said in the section about "privacy-preserving advertising", we shouldn't keep something evil up (Google search and / or Mozilla) just because some other, less evil things depend on them (but are they really less evil if they chose such "sponsors" ?). Let's fix our problems at the foundations. But again, survival instinct is primary, and in this quote the evil fox is simply gasping for its last breaths.

Maybe we shouldn't celebrate yet, though. After all, none of this has been applied yet, as far as I can see (though Mozilla is - or pretends to be - very scared already). Being a conspiracy theorist, I wonder if this isn't some kind of a game. Maybe Mozilla has just ceased being useful (at least in the form it has existed in, so far). Maybe the world so-called "elites" realized that search engines are slowly being deprecated in favor of AI. They will throw us a bone and "break up" Google while it's already becoming irrelevant (archive) (MozArchive) (*"In 2024, around 15 million adults in the United States claimed to have used generative artificial intelligence (AI) as their primary tool for online search. By 2028, this number is projected to reach over 36 million online users"*), and pretend the legal system sometimes works in our favor. But it will all turn out to be theater as the new monopolizer will be the AI companies, which are - of course - much more effective (archive) (MozArchive) in convincing people of the "official versions of events" (*"To evaluate this possibility, we leveraged developments in generative artificial intelligence and engaged 2190 conspiracy believers in personalized evidence-based dialogues with GPT-4 Turbo. The intervention reduced conspiracy belief by ~20%. The effect remained 2 months later, generalized across a wide range of conspiracy theories, and occurred even among participants with deeply entrenched beliefs"*). And Mozilla -

by [getting integrated with them \(archive\)](#) ([MozArchive](#)) - will lead us to them and keep serving the role of controlled opposition this way. Don't you think this situation is suspiciously convenient? Right as the legal circus is being finalized, Mozilla is moving towards AI. So they might not be that bothered by the restrictions on Google if AI companies will fund them instead. And it is very obvious the so-called "elites" are going all in on AI, so they won't let Mozilla die. This is my prediction.

[Back to the front page](#)