Fake privacy / security initiatives

"Beware of false prophets, which come to you in sheep's clothing, but inwardly they are ravening wolves."

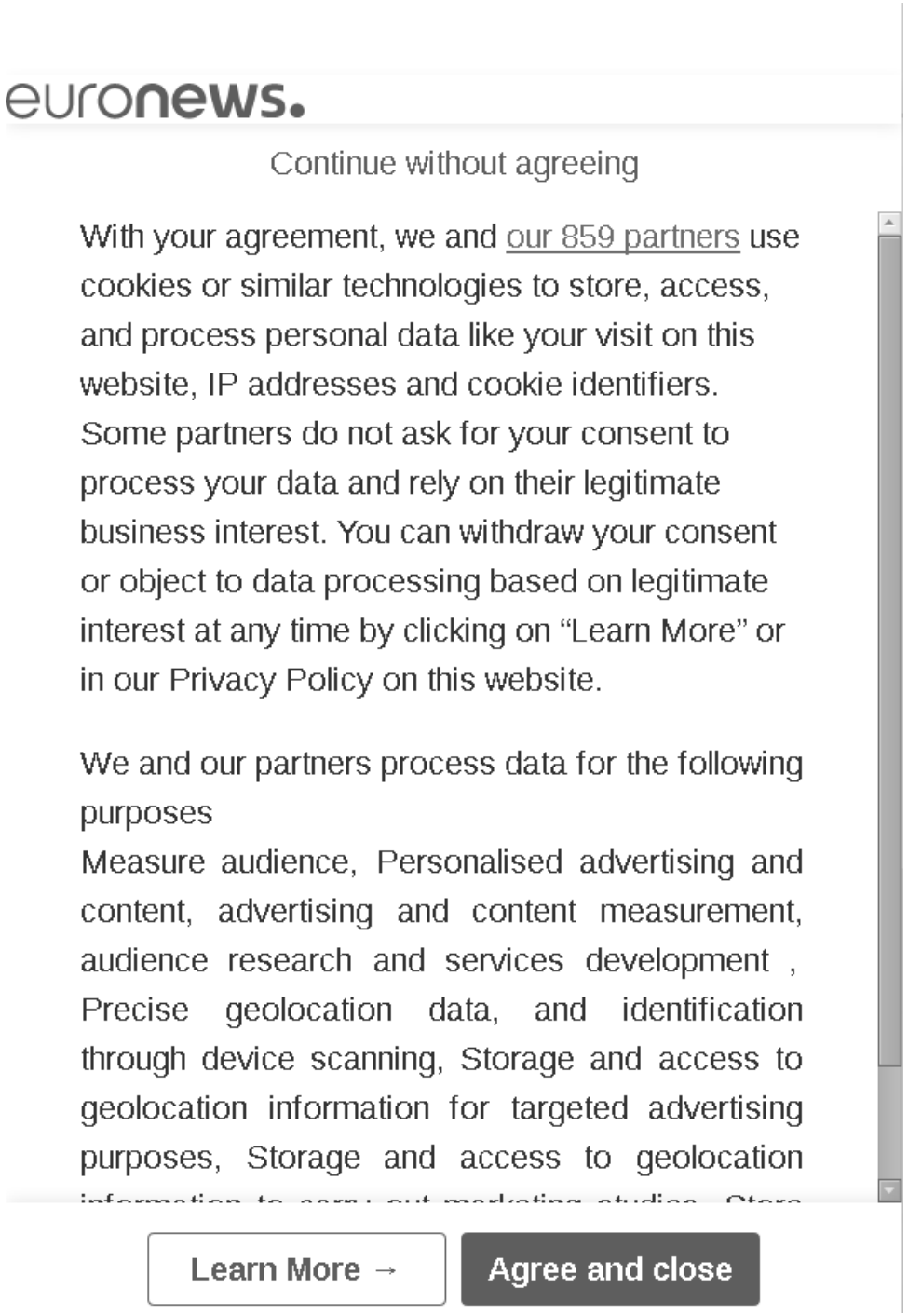
List of initiatives

Do Not Track

Invented in 2009, this browser header tells websites you visit that you do not want to be tracked. 9 years and thousands of articles and discussions about DNT later, and **there is still not even a standard for what "tracking" exactly it is supposed to prevent** - even though they promised to create one long ago. Needless to say, websites can interpret DNT however they want, or even **ignore it altogether**. How much effort has been wasted on this dud - effort that could have been spent on creating and improving browser extensions that actually protect you from tracking. **DNT, on the other hand, just gives the illusion of privacy** to unsuspecting users - which is worse than doing nothing at all. Let's be real here - cooperating with trackers could have never worked anyway - since they don't care about playing fair.

European Union cookie law

If you've spent any time on the Internet at all, you've surely seen some obnoxious cookie notices, such as:



In 2011, the European Union has created a law which requires websites to inform visitors about

the kind of data that will be stored on their computers, its purpose, as well as the need to get consent from users before storing anything. There were also guidelines for the duration of the cookie's existence. Anyway, a report (archive) (MozArchive) has shown that **most websites do not follow all the requirements properly**. Even if they did, the people who would benefit from this information won't understand it and will click through it instead; while the aware ones have already blocked the cookies - but will still be bothered by the obnoxious notices. It should also be mentioned that **the most important tracking cookies - the social network ones - are exempt from the law!** So you can still be tracked by Facebook and friends; talk about a wasted opportunity.

Private Browsing / Incognito Mode

Almost every browser has this under different names. Let's be clear here - **this does nothing whatsoever to protect you from nosy ISPs or trackers**; and, while most browsers do admit that - some, like Waterfox, have tried to ride the wave of confusion to pretend that their improved private browsing (archive) (MozArchive) does something more. A report has shown (archive) (MozArchive) that many people do in fact believe that this mode guards them from online spying; as far as I'm concerned, browsers should remove this if they want to stay honest - or at least change its name. **UPDATE**: Pale Moon kind of averts this with the Proxy Privacy Ruler addon.

Hooktube / Invidious

Hooktube used to be a YouTube frontend, then it got forced to use Google's API, became useless and died. So let's talk about Invidious. On November 2020, Invidious lead dev left the

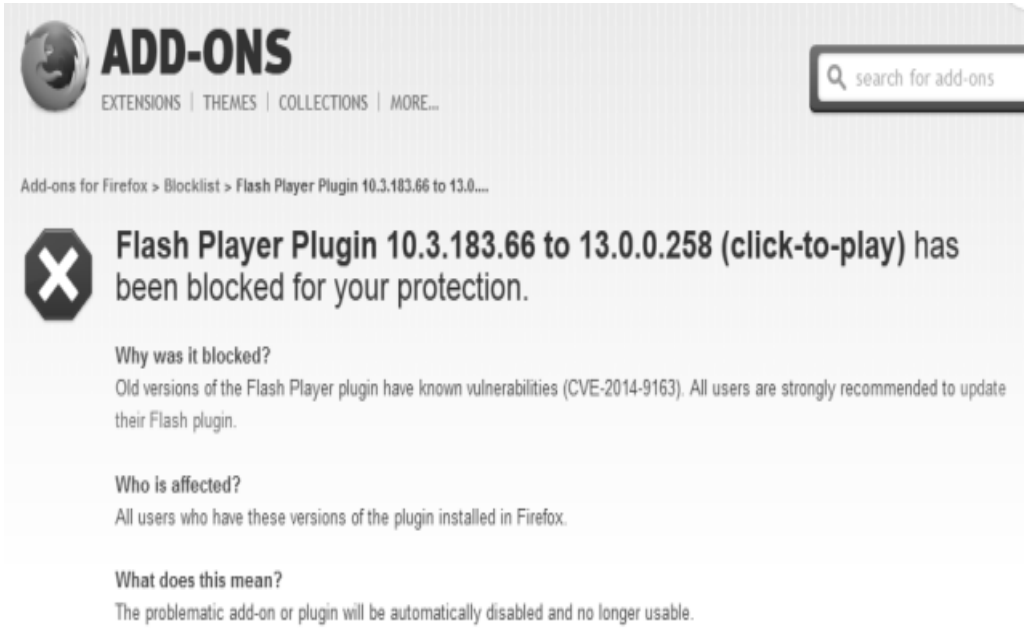
project (archive) (MozArchive) and the other people don't appear to be doing much. Main instance is gone and the others are hit and miss. Errors such as *"Read timed out"* or *"Video unavailable"* (even if it actually is) are commonplace. Invidious, also, still contains most of the bloat of YouTube. I recommend using youtube-dl (there's a crusade against that, too (MozArchive)) to download videos - with it, you can watch them as many times as you want, whenever you want - without ads or slowdown, google connections or any other connections. **UPDATE August 2021**: now youtube-dl fails to download age-restricted videos (**another update**: yt-dlp works, but who knows for how long?). It's the same situation as with search engines that don't use their own index - you're **completely dependent on the violators** you're proxying. Do you like being shielded from *"coronavirus misinformation"* (a codeword for *truth*)? Every so-called content creator should host their shit on alternative platforms. Of course, the major ones (Bitchute, Odysee, Brighteon) are cuckflared or suffer from other major flaws. Hey, why not make your own site and put direct links to your vids there? How radical, I know. **UPDATE June 2023**: now invidious will die completely (archive) (MozArchive). It was already hanging on by a hair for a long time, but now, Google finally decided to spray some cockroach poison and the invidious users will have to scatter. Some are still fooling themselves that they will fix it with yet another tech solution, yawn.

"End-to-end" encryption

For the last few years, services which have traditionally been famous for their spying (such as Skype, Viber, or the Facebook operated WhatsApp (archive) (MozArchive)) have been loudly announcing their support of "end-to-end" encryption - which **should** mean that only you and the person you are communicating with can see the content of your messages. However, **it is still them generating the keys**, and therefore relies on their trustworthiness. Many allegedly

"private" E-mail providers also suffer from this flaw - read my report. The moral of the story - if you don't manage the encryption yourself, it's not truly end-to-end, and shouldn't be relied upon.

Forced "protection"



This is simply a huge slippery slope - first it was plugins, then addons, then browser settings kept getting dumped into about:config or the abyss. What's next - deciding what sites you can or can't visit? Isn't Google SafeBrowsing just that? Maybe one day, they will block all "insecure" HTTP websites. Surely that's going too far - or is it? In fact, both Firefox (archive) (MozArchive) and Chrome (archive) (MozArchive) have been trying to get rid of HTTP for a long time. Great, thanks Mozilla and Google for "protecting" me from all this malicious stuff -

but **who will protect me from you**? That is the real question. Of course, people don't realize there is an issue until something they use regularly breaks. The solution, of course, is to only use software that actually respects you instead of treating you like a baby; **security will always be the responsibility of the user** - you cannot "protect" people from everything. Even if you could, it would not be desirable; there is always a trade-off between security and functionality, and people should be able to choose at which point of the spectrum they want to be.

Silent or forced updates

An extension of the above; they are the truck through which undesirable changes get dumped onto unsuspecting users. UI modifications, configuration option removals, the aforementioned blockages, additional spyware, or actual malware; regardless - **auto-updates transfer control of the software from the users to developers**. And there is no excuse to at least not ask the user before proceeding. The horror stories of updates breaking things are numerous - for example:

- Firefox freezing the computer (archive) (MozArchive)

  My Firefox was updated to it yesterday. It froze when I tried to use it and froze the computer to where I had to use the power button to get out of it. I tried Firefox in safe mode and it still froze. I see messages in Mozilla Zine saying the same thing.

- Firefox changing the user's settings (archive) (MozArchive)

  I would appreciate very much if Firefox update informed me about changes it does to my settings in detail. I want to have the chance to not be surprised by a

new default search engine or a disabled https feature for example.

and

I first noticed it when it first introduced the "do not track me" setting. I enabled that and the next time I checked, it was disabled.

- Another example of the same (archive) (MozArchive)

Jern informed me that Firefox reset the block lists setting of the browser's Tracking Protection feature from strict to basic when the browser was updated to version 50 from Firefox 49.0.2. Basic protection is the recommended and default value of the setting. It does not block as many trackers as the strict blocking list.

and

Michel told me a week later that a recent Firefox update (to 50.0.1 or 50.0.2) did reset another preference. This time an URL string that Michel modified on Firefox's about:config page.

- Windows 10 updates are famous for breaking shit (archive) (MozArchive)

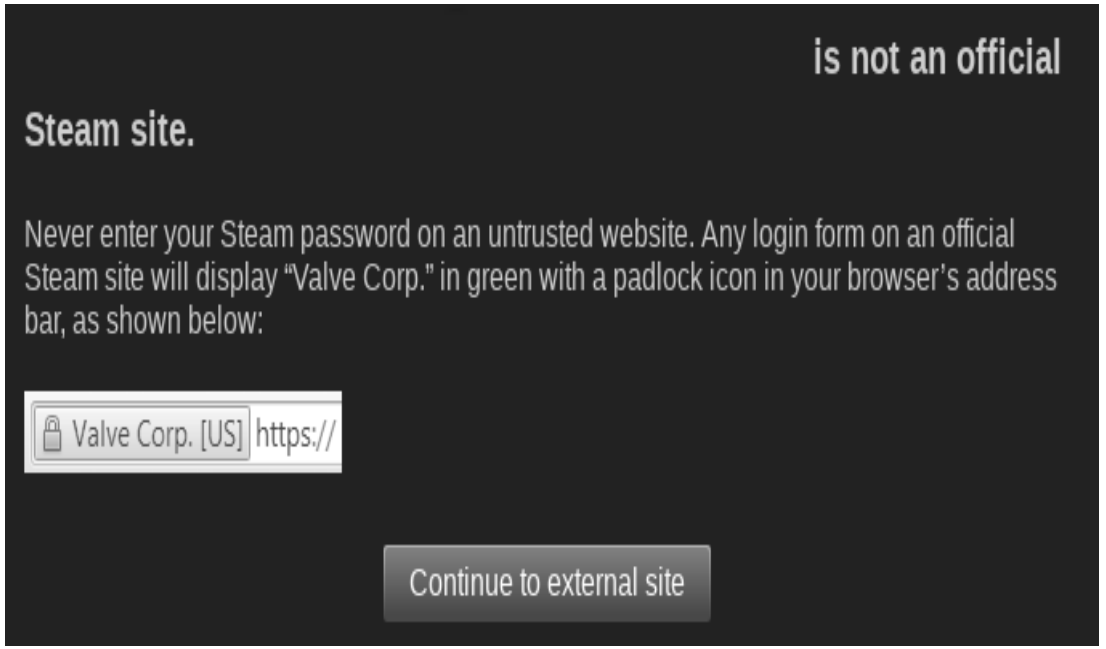
The most common complaints after updating to Windows 10 were software compatibility issues, such as programs not working properly, or at all (21 percent), followed by hardware problems, such as printers and speakers no longer working (16 percent). Members also struggled with issues such as email accounts

no longer syncing and personal files being inadvertently deleted, said Which? "Some consumers suffered PC slowdown and, in some cases, members reported complete PC failure. Of those in the survey who experienced this, 46 percent said they had paid someone to fix it, at an average cost of £67 each," noted the consumer group.

- And finally, my absolute favorite (archive) (MozArchive):

  Miller added code that would delete the file system of any computer with a Russian or Belorussian IP address. Then, its maintainer added the module as a dependency to the extremely popular node-ipc mode. Node-ipc, in turn, is a popular dependency that many JavaScript programmers use. And it went from annoying to a system destroyer.

External link filters



Didn't know whether to put this here or in Principles of bad software design - but the alleged point of it is security, so it's here. How does this work? Briefly - certain sites, whenever a link is posted to them - will NOT let you go there directly but only through their special redirect. If this actually improved security I would just consider it as simple babying - similar to the auto-updates; but the reality is much more malicious as usual. Not only are the link filters annoying, but they **make tracking easier** by putting the website you're leaving to into the URL. Also, people can **actually fucking see** the link they're clicking on, so the security benefit is doubtful at best. Twitter goes even further and **prevents users from knowing where they're going to** - every web address is replaced by their t.co shortener. They even admit this is used for censorship (archive) (MozArchive):

> *A link converted by Twitter's link service is checked against a list of potentially dangerous sites.*

Don't bother looking at those links, son - Mommy Twitter will protect you! But maybe they should first focus on their own security than that of others; Steam, for example, had a breach (archive) (MozArchive) where:

> *users were able to access other people's game libraries, and were able to see sensitive information including names, home addresses, email addresses, purchase history, Paypal account information, and even partial credit card numbers.*

Twitter had an even worse one (archive) (MozArchive) where up to 250 000 accounts were compromised. As I said earlier - **security should be the responsibility of the user**; we're not babies and treating us like them always results in disaster.

Firefox Send

Mozilla's allegedly private file upload service - analyzed in more detail here.

Firefox Lockbox

Mozilla's password storage service - analyzed in more detail here.

EFF's "Who has your back?"

They've made many of these over the years - the most recent one as of writing is https://www.eff.org/wp/who-has-your-back-2019 (archive) (MozArchive). Briefly, the report rates the big corpos' censorship policies, but **the most important criterion - that is, how much**

they actually censor - is completely ignored. Instead, they focus on whether the censors graciously tell you that you've been suspended or that a government has requested a takedown. And so a known violator like youtube gets 4 fucking stars out of 6 - what a joke. They even got a point just for having an appeal system that doesn't even work. **There is only one aim of these reports - to justify the big corpos** so that naive / inexperienced people don't abandon their services which don't respect them.

Facebook Container

A Mozilla-created (hey, a red flag already!) extension which - in Mozilla's words - *"helps you control more of your web activity from Facebook by isolating your identity into a separate container"*. There are several problems with this:

1. It does not prevent Facebook data collection while you're on it. It is trying to give a compromise between privacy and the convenience of the violators' services, which of course doesn't work.
2. Even for its stated purpose, it doesn't really work (archive) (MozArchive). Inspecting the source seems to reveal that it's using a blacklist to decide which sites contain facebook elements that are then blocked.
3. It is completely outclassed by uMatrix, which can contain not only Facebook (in a way that actually works), but any other sites you'd like in addition to many other benefits.

The same kind of logic applies to all other "container" extensions. Just learn uMatrix, my friends, and you will look down on pretender addons such as this one.

Total Cookie Protection

Another piece of trash from the evil Moozilla. First of all, **it's not fucking "Total"**. Look (archive) (MozArchive):

> *In addition, Total Cookie Protection makes a limited exception for cross-site cookies when they are needed for non-tracking purposes, such as those used by popular third-party login providers.*

So, the "protection" is "total" EXCEPT when it concerns services that Moozilla thinks should be exempt - such as Facebook. Does Moozilla realize that - when you log in to a forum through Facebook - they are **tracking you then**? Of course, they can't be so stupid as to not understand this. Therefore Total Cookie Protection is simply a way to distract from real privacy solutions. Such as uMatrix, which does everything TCP does plus much more - without (by default) compromising with violators like Google and Facebook.

Other privacy sites

I really didn't want to do this, but some of those pretending to give advice and help people have no business doing so and need to be exposed. So let's get on with it:

Privacy Guides

UPDATE February 2022: I'm just going to rewrite this, since some things have changed and / or became irrelevant. The old report is here (MozArchive).

Formerly *Privacy Tools* (what is currently Privacy Tools is run by different people). The website equivalent of Mozilla - pretends to be your best friend but pushes you off a cliff when you're not looking. TOR Browser is literally their main browser recommendation (archive) (MozArchive), even though it is unusable due to how many websites block TOR. They also think you should not change anything in it:

> *We recommend that you do not change any of Tor Browser's default configurations outside of the standard security levels.*
>
> *You should never install any additional extensions on Tor Browser, including the ones we suggest for Firefox. Browser extensions make you stand out from other Tor users and your browser easier to fingerprint.*

This ignores two things. First of all, fingerprinting can be blocked by extensions such as uMatrix, which will deny the requests that fingerprint you in the first place. Second, Moonchild has provided (archive) (MozArchive) a much better way against fingerprinting than what TB tries to do, without the inconvenience of being unable to use browser extensions (some of which do in fact help resist fingerprinting).

Privacy Guides' second browser recommendation is Firefox, which is totally not private. And not a word is said about the truckload of data FF leaves with, even though they do admit it in a roundabout way by recommending Arkenfox user.js, which disables most of the violations. Then they continue with their extension hating:

> *We normally do not recommend installing any extensions, as they have privileged access within your browser. We make an exception for uBlock Origin, a popular content blocker*

and Recommended Extension by Mozilla.

So if you *"make an exception"*, why not do it for an extension that is actually good, like uMatrix? But anyway, with this, Privacy Guides proves they **do not really know what to believe in**. On Monday extensions are bad and ruin your fingerprint, on Tuesday uBlock Origin is so great the fingerprint suddenly doesn't matter.

Their E-mail recommendations (archive) (MozArchive) are even worse. Proton - one of the worst possible choices - is literally listed first. Then other trash like Tutanota and CTemplar that do not even support mail clients (this should be a dealbreaker).

Their mali client (archive) (MozArchive) page recommends insecure Thunderbird and ignores the much more secure and overall better Claws Mail. Search engine recommendations (archive) (MozArchive) list StartPage second, despite it being owned by an ad company, blocking VPNs and TOR and relying on heavily censored Google for its results.

Not all the advice on Privacy Guides is terrible - they do recommend VeraCrypt, for example. But **we as privacy supporters should have high standards and not tolerate shilling violators like Firefox, ProtonMail or StartPage**. Another fundamental problem with Privacy Guides is that it simply **recommends too much stuff**. A newbie will be confused by the six or seven options in each category; a good site would only mention one or two absolute best ones. Then, Privacy Guides also fails to mention quality alternatives like XMPP, Pale Moon or RiseUp mail. And completely ignores uMatrix, the best browser extension and strongest single privacy tool on Earth. And just like that, Privacy Guides should also be ignored.

Privacy Spy

UPDATE May 2023: site is dead so here's an archive. This will be short since this fake doesn't deserve much more. A member of our chat posted them and I immediately spotted the red flags. In Bypassing the privacy chase, I've said that the most important thing while rating a provider's privacy policy is what it stores and for how long. There, I also listed the most important specifics to look for (IP address, system info, etc). **Privacy Spy, however, completely ignores all that and bases its ratings on useless stuff**. And so, violators like FastMail get a grade of 8 / 10 just because they graciously tell you why they collect personal data (if the reasons are shit, that does not lower the rating), the policy's history or allegedly notify you when it's changed. Of course, Privacy Spy plays fast and loose with most of its definitions, so the ratings become totally useless. For example, about the notification thing, here's what FastMail's policy actually says:

> *If we make fundamental changes to this privacy policy, we may take additional steps to notify you including by posting on our website(s), through pop-up notices or via email.*

"MAY" take additional steps to notify you. And because of this *"MAY"* (and not **WILL**), FastMail gets the best rating. Or check this about the deletion of personal data:

> *Even if there is a reasonable delay before the data is fully deleted (as is common), the data still counts as "permanently deleted" and satisfies the parameters for this question.*

So, the fact that this data stays around on FastMail's servers for **180 fucking days** is completely ignored, and the violator earns the best rating again. Clearly, Privacy Spy's criteria are worse than useless - since they justify clear transgressions while also not caring about what actually is stored and for how long. I could go on for a long time about this fraudulent rating site (there are many more issues - e.g, Privacy Spy is fine with collecting personal data for allegedly *"critical*

uses"), but as I said, it doesn't deserve it. **Avoid and forget it exists!**

Arkenfox

I will not be rating his user.js here, as that isn't the point (browsers that require user.js to be unfucked shouldn't be used, anyway). He repeats the same extension-hating nonsense (MozArchive) that Privacy Guides does. Yet he recommends extensions like uBlock Origin or Skip Redirect anyway. More importantly, he **shits on the King of extensions - uMatrix**:

> *No longer maintained, the last commit was April 2020 except for a one-off patch to fix a vulnerability*

It does not need maintenance, since everything that's supposed to be there, already is. Unlike trash extensions like uBlock Origin that need constant filterlist updates. Besides, the Pale Moon version of uMatrix is still being maintained. And then this disgusting lie:

> *Everything uMatrix did can be covered by prefs or other extensions: use uBlock Origin for any content blocking.*

This argument is refuted in depth here, but briefly: the uBlock Origin grid mode only has a few of the categories uMatrix does, while the *"prefs"* do not have per-site functionality.

It might seem weird how I've put this in here. Arkenfox isn't a big site - it's not even a site at all. Its only focus is providing an user.js file to unfuck your Firefox browser. But, if someone attacks the single most important privacy and control tool in existence, I have to react.

Back to the front page