

Search Engines - which one to choose?

- Introduction -
- The problem with no own index -
- List of providers -
 - SearX -
 - Brave Search -
 - Wiby -
 - Swisscows -
 - StartPage -
 - DuckDuckGo -
 - Qwant -
 - MetaGer -
 - Jive Search (DEAD) -
 - Mojeek -
 - Ecosia -
 - Oscobo -
 - Discrete Search -
 - Gibiru -
 - Gigablast -
 - Peekier -
 - Presearch -

- Right Dao
- 4get -
- Freespoke -
- FindX -
- Stract -
- Marginalia -
- You -
- WebCrawler -
- Search my Site -
- MillionShort -
- Spyda -
- Excite -
- 4Conservative -
- GoodGopher -
- Summary -
- Lyrics search engines -

Introduction

Most of us will use these every day (usually several times, in fact), so it's important to carefully consider your selection of choices. Not only do we want great results, but - since we will often share some really sensitive data with them (such as medical, travel, or even that we're interested in loli or shoplifting) - they better not be doing dirty stuff with it. There are also various additional functions that we'd like our search engines to provide. Now why did I use the phrase **selection of choices**? Because - as you will see - the situation with search engines is not as good

as with E-mail providers, so we're forced to switch around since there isn't a single one that has everything we need. Without further ado, let us check what is available:

The problem with no own index

A while after finishing this article I've had a "revelation" - the situation with search engines is even worse than I thought before. Aside from Wiby (which has very few searchable sites in it) and Mojeek, the search engines mentioned here **depend on others** for their results. By "others" I mean either Google, Bing or Yahoo - **three massive privacy violators**. When you search through, say, Swisscows - the query is first sent to Swisscows, which forwards it to Bing, which then returns the result to Swisscows and finally to you. There are several problems with such a setup:

1. Regardless of the engine's policy, the search terms are being stored on the violators' servers, and those can contain sensitive information.
2. The engine needs to enter an agreement with the violator in order to proxy their results, and the contents of that agreement are not revealed to you and can include data collection. Unless they do it the Scroogle way... ([archive](#)) ([MozArchive](#)) (hint: it died).
3. The results will still be censored if that is the violator's policy.
4. The engine can be blocked at any time by the violator.

This is not that different from using Invidious, Nitter, Facebook Container or custom Discord clients for their respective services - the violator still calls the shots. And we - like the wives dependent on their abusive husbands - keep coming back for more in hopes we can prevent some of the damage. But - as we rely more and more on the violators - it gets harder to dump

them. Keep this in mind while reading through the below recommendations.

List of providers

🔍 SearX 🔍

UPDATE June 2022: rewritten. SearX allows you to choose the search engines used, and proxies your queries to them through itself. It has no own index so all the issues from the relevant section still apply. Still probably the best option to use these days, if you find a good instance. The level of support for different search engines can vary heavily. Bing, in particular, doesn't seem to work anywhere, and all other options aside from Mojeek (which will almost always block SearX) and Gigablast, censor. Yandex is not able to be proxied by SearX, either. Still, most of the relevant search engines are supported. So you might be wondering why use anything other than SearX. Well, it's because this happens more often than not:

Error! Engines cannot retrieve results.

brave (timeout)

duckduckgo (Suspended: access denied)

gigablast (timeout)

mojeek (Suspended: access denied)

qwant (timeout)

startpage (timeout)

wiby (timeout)

wikipedia (timeout)

Please, try again later or find another SearXNG instance. (Public instances)

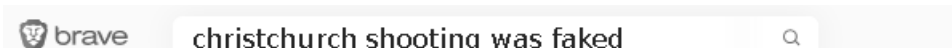
However, using SearX instead of the engines directly obviously provides superior privacy, not giving the proxied engines your IP or loading their trackers. Remember, though, that instances could still choose to collect data (read privacy policies if they exist). The best option is to spread your searching over several instances. SearX provides very useful Web Archive integration as well, helping avoid Cloudflare. Onion domains are possible if the instance has installed them. Searching itself works without JavaScript, even with images. NG has seemingly improved the image results, as well. I recommend using one instance for images and another for regular results; this allows adding both as different shortcuts to the address bar, and without getting image results stuck in between your regular ones.



UPDATE: I don't want to call it "decent" anymore. Even though it apparently has its own index (archive) (MozArchive), it clearly deranks alternative content in favor of mainstream trash (results similar to Google's), even if the latter is barely relevant to what you searched for. That's in contrast to DuckDuckGo or Qwant, whose results are more in line with what you've actually typed. **Edit:** I was too lenient. **The censorship is exactly like Google's** - meaning you will **never** find the truth about the moon landing or COVID vaccines there even if the query asks for exactly that. What you **will** find - though - is a bunch of irrelevant "fact check" or "science loving" sites, or ones shitting on "conspiracy theorists". I am now doubting if they truly have their own index instead of lifting everything from Google - unless they chose to index only the evil sites and ignore all the good ones, which would be even worse. They lie about it, BTW:

No, Brave Search does not filter, downrank, or censor search results. Nor will we change our search algorithm to increase or decrease the prominence of results in response to current events or anyone's political, religious, ethical, or other beliefs. Brave Search—like Brave itself—is intended to be a user-first portal to the web, free of Big Tech's manipulation.

But everyone can easily verify the censorship for themselves, with a query such as "9 / 11 was done by the government". And just with that, this brainwashing facility pretending to be a search engine should be trashed. **UPDATE June 2023:** if you want proof, here are the first 6 results for *"Christchurch shooting was faked"* - my favorite query for testing these kinds of things:



● Christchurch shooting conspiracy theori...
[smh.com.au](#) > world > oceania > chris...

March 19, 2019 - **The surge of disinformation comes as the technology companies have been criticised for the ease with which the video of the slaughter were disseminated online.**

● Disinfo: Christchurch shooting was a fal...
[euvsdisinfo.eu](#) > report > christchurc...

August 5, 2019 - **The Christchurch shooting was a false flag operation with the purpose of restricting gun laws in New Zealand.** ... This claim is a conspiracy theory presented without any evidence. Alleging false flag operations is a common tactic of pro-Kremlin disinformation. The Christchurch shooter, a man named Brenton Tarrant, was a white supremacist who espoused racist and anti-immigrant views, which were detailed in a manifesto that he sent to numerous people just a few minutes before the shooting.

● Conspiracy theorist claims police have v...
[stuff.co.nz](#) > national > christchurch-s...

May 3, 2019 - Following the Christchurch terror attack in which 51 people died, **conspiracy**



they believe have been faked.

● The Christchurch terrorism conspiracy t...
[thespinoff.co.nz](#) > home > society > t...

March 21, 2019 - No sooner had Police arrested the **Christchurch** shooter than the conspiracy theories were proliferating like pond scum. Those narratives are not just wrong, but dangerous and self-perpetuating.

● Fake Christchurch victims seek NZ\$17k
[dw.com](#) > en > fake-christchurch-attac...

June 29, 2019 - New Zealand police have raised concerns over people faking their presence at two deadly mosque shootings in March. More than NZ\$7 million has been paid out to survivors by local victims' funds so far. ... Christchurch police have issued warnings to **two people who police say falsely claimed they were present during the mosque shooting attacks in March to each claim NZ\$17,000 (€10,000, \$11,400) in compensation.**

● The Eerie Absence Of Viral Fakes After T...
[buzzfeednews.com](#) > article > craigs...

March 16, 2019 - A security official stands guard outside the Al Noor mosque in Christchurch, New Zealand. This is the latest edition of The Fake Newsletter from BuzzFeed News. Go here to subscribe.
Friday's attack at two mosques in New

theories included several claiming the attack was a hoax, or a "false flag" event. · The phrase – which originated in

Zealand was committed by a shooter who deployed a social media strategy to go with his actions.

Five of them attack conspiracy theories, maybe worse than what even Google does. And that's not everything that's bad about Brave. Though its [privacy policy \(archive\)](#) ([MozArchive](#)) seems to say that the **IP addresses are not stored**:

You can search for 'cafes near me' and Brave Search will use the IP address broadcast by your device but without sharing that IP address and without storing it. This means we can't tie your searches to you and your location.

It doesn't say literally anything else. We have to go to [another page \(archive\)](#) ([MozArchive](#)) to see just how much stuff Brave stores:

- *Number of daily/weekly/monthly visits*
- *Number of returning visits*
- *Number of search queries per day*
- *Average query length*
- *What percentage of queries led to a user clicking a search result*
- *How many users have chosen to leave feedback about Brave Search*
- *The operating systems people use when they visit (e.g. macOS, Windows, etc)*
- *The browser you've visited from (e.g. Brave, Chrome, Safari, etc)*

They say this is all “*opt-in*” - but in reality, not only is the tracking opt-out (**enabled by default**) but you **cannot even change it without JS** and not at all in Pale Moon. This means they lied in

their privacy policy by pretending that they will only collect the data *“if you allow them”*, which sounds as if it requires actual user action to happen. As usual, cynicism wins over hope. This should have been expected - **it's still fucking Brave**, and there has been a lot of shady shit going on with them. How do we know they won't include some sponsored results or add referral links, the way they did with their browser? How do we know they won't eventually partner with a violator, like they did with Uphold? And that's the biggest flaw of this search engine. Due to Brave's reputation taking several blows to the chin already, we just can't trust it anymore. Image search does not work without JS. **UPDATE June 2022:** Text queries used to work through TOR without JS, but now they bring up this:

Confirm you're not a robot

This page needs WebAssembly to function.

Once a captcha challenge is solved, you can get access to Brave Search again without being subjected to our anti-bots measures, for a limited number of queries. The mechanism used to privately allow you to access Brave Search after solving a captcha challenge relies on WebAssembly. Unfortunately, we have detected that **WebAssembly is currently not enabled in your browser**.

Here are a few things you can do:

- If you are using the **Tor browser** with its **safer** or **safest** security level, WebAssembly support is disabled and you will unfortunately not be able to access Brave Search after your request has been flagged as suspicious. We are actively working on ways to improve the experience of Tor users on Brave Search.
- If the above does not match your situation, make sure that your browser supports WebAssembly and that no extension is currently disabling it on Brave Search.

BS requires JS and WebAssembly enabled to search through TOR, enforcing the usage of bloated browsers. See? I told you to not be hopeful. Trash it and don't look back. **UPDATE:** there is now an onion, so I guess they do not hate TOR now at least on the onion.



UPDATE: it's worse than I thought - keep reading! If we only took into account the privacy policies ([archive](#)) ([MozArchive](#)), this little known search engine from the Swiss Alps would rank very highly indeed:

We do not collect any of our visitors' personal information. None whatsoever. When using Swisscows neither your IP address is recorded nor is the browser you are using (Internet Explorer, Safari, Firefox, Chrome, etc.) collected. No analyses are made, which operating system our users use (Windows, Mac, Linux, etc.); your search are not recorded either. We record absolutely no data from our visitors. The only information we store is the number of search requests entered daily at Swisscows, to measure the total overall traffic on our website and to evaluate a breakdown of this traffic by language and mere overall statistics.

No IP or browser data is stored! Swisscows even realizes (unlike, say, DuckDuckGo) that saving the search queries is also dangerous, even if allegedly disassociated from so-called personal information:

Furthermore, it is important not to store any search terms, given that these can also contain personal data. (Just think about someone who enters their own name and/or their insurance number into the search box.)

For a while I thought that - while they might not store anything themselves - they might still share some data with Bing (which they use for their results) - but my suspicions were defused:

Swisscows does not transmit any personal information to third party search engines or to the providers of sponsored results.

All of this is **according to their privacy policy only**. However, we know better than to believe a privacy policy blindly - especially when there are some problems with the trustworthiness of Swisscows. First of all, they **require JavaScript** to display the page at all - which is a terrible design; worse yet - the code is heavily obfuscated - almost as if they were hiding something. I got a report of Swisscows including redirect links in its results. At first I thought it's some mistake, but decided to investigate **and confirmed it**. They look like this:

[http://www.smartredirect.de/redir/clickGate.php?u=\[UniqueId?\]&m=12&p=\[YetAnotherID?\]&q=\[YourSearchQuery\]&url=\[TargetURL\]&r=https%3A%2F%2Fswisscows.ch%3Fquery%3D\[YourQuery\]](http://www.smartredirect.de/redir/clickGate.php?u=[UniqueId?]&m=12&p=[YetAnotherID?]&q=[YourSearchQuery]&url=[TargetURL]&r=https%3A%2F%2Fswisscows.ch%3Fquery%3D[YourQuery])

Shady as fuck and **contrary to their privacy policy** of not sending your data anywhere - because that redirect service will **absolutely get** your browsing history with what seems to be an user ID (unconfirmed yet) attached to it; as well as the search engine you used (in this case, Swisscows - but who knows what other partners in crime they have). According to this stat site (archive) (MozArchive), Smart Redirect seems to collect the browsing history of almost **20K different people every day** - a pretty significant violator, then. What this service actually does is **show sponsored results** that are indistinguishable from the regular ones aside from a little image next to them (for which Swisscows makes another third-party request). If you click on those links, your browser will make a request to an affiliate marketing company such as awin or linksynergy - which also seem to contain **unique user IDs**. Sometimes, searches from the Tor network **will be denied** - this might depend on which exit node you get. Regardless, they **lied about not sending your data to third parties** - safe to say, then, that the myth of the little private

Swiss Cow is dead and buried. But let's dig a little deeper:

The only legitimate reason for our beginning to collect personal data would be the existence of a legal warrant or a court order, which would require us to do so in connection with a specific user, who is suspected of such a serious crime that such a violation of his or her privacy would be justified.

So they will **perform targeted surveillance** without notifying you when the government comes knocking (that's the great Swiss Privacy Law in action). The search engine also has this "family-friendly" shtick, which means you might get a message such as:

Dear user, the entered word is not allowed for under 18 year olds, since we have decided on the protection of minors, the word "insert search term" is excluded from the search. Thank you very much for your understanding!

This is activated by many porn-related queries and some violence-related ones but you can still find really graphic stuff like people's limbs being cut off pretty easily. And thankfully, information alone does not seem to be censored.

Swisscows also has a “*semantic map*” feature which displays additional terms relevant to the search you've typed, narrowing the results to what you might be looking for. I haven't found it very useful though, or maybe I just don't get how to use it. The search engine does not run without JavaScript enabled at all (can only see a white background - bad design!). XHR is also required to display the actual results (which come from Bing exclusively). Used to not work in Pale Moon but that seems to have been fixed recently (whether by them or by PM...). Swisscows can search for images, videos, and news; it ~~also includes the only (AFAIK) privacy-~~

~~aware translator which is unfortunately also family-friendly (cannot translate swear words...)~~
does not include the translator anymore, so the one thing it was useful for is gone. Of course, the Swisscows Privacy Wall came crashing down above; it's not a sure thing we can even trust its policy when they've already broken it. So, Bing might be getting your data after all. Having problems with Tor seals the deal even further. **Another one bites the dust**, as they say!

sp StartPage sp

A privacy-based proxy for Google search. Claims to “*believe privacy is a fundamental human right*”; let's see how much do they actually follow that belief:

Why we don't collect any "personal data"

We saw the perils of that in DDG's section - where, for example, measuring “*engagement of specific events on the page*” was considered non-personal, along with the actual search queries. But let's give the benefit of doubt and see what is StartPage's interpretation of the term:

We don't record your IP address

With the most important potential roadblock out of the way, the privacy train is running at full speed!

We don't serve any tracking or identifying cookies

No hiccups so far.

We do measure overall traffic numbers and some other – strictly anonymous – statistics. These stats may include the number of times our service is accessed by a certain operating system, a type of browser, a language, etc.

The privacy train is slowing down. I spoke of the problems with so-called anonymous data in DDG's section. Remember: *“the only anonymous data is no data”*. But it gets worse. StartPage includes advertisements from Google (these cannot be removed by uMatrix, only element hiding) on top of their search results page, and:

In order to enable the prevention of click fraud, some non-identifying system information is shared

Aaand the privacy train has been totally derailed! Now you have to trust StartPage's determination of what is *“non-identifying”* enough to be safe in Google's hands. Now they don't say exactly what that data consists of - but if it's the same set mentioned above that StartPage uses for their statistics, it would definitely leave the possibility of revealing someone thanks to browser fingerprinting. So StartPage sends potentially identifying data to Google. It's not all that bad though - at least they apparently don't store it themselves. And then there's this:

Any request will have to come from Dutch judicial authorities. We'll only comply if we're legally obliged to do so. But we're not likely to receive requests by governments to hand over user data – simply because we don't have any.

And:

We will never comply with any voluntary surveillance program

So it seems that, at least - you're pretty safe from the government's prying eyes. The other issue with StartPage are the **absolutely terrible search results**. That is because Google runs a massive censorship campaign (archive) (MozArchive), deranking any alternative or conspiratorial content. This means you will even get results that **don't relate to your query at all** - and I've confirmed it with tests. Try searching for something like "was the Christchurch shooting faked" and you will see what I mean. Then compare with Qwant or DDG. I did this for many other queries which would result in displaying alternative or conspiratorial websites (if the search engine was honest, that is), but instead showed me irrelevant trash. Also, just like Google, it supports no other ways to search aside from Web and Images. StartPage works perfectly with JavaScript disabled and has the handy *"Anonymous View"* feature, allowing you to visit returned sites without revealing yourself to them (however, much functionality will be disabled).

Interestingly, a long time ago StartPage used to run a search engine called IxQuick that used their own index. I used that extensively when it was around and the results were pretty good AFAIK. Why did they take it down and submitted completely to the Google botnet? We could have had an actual privacy-based search engine with **no dependency** on the tech giants and no censorship (since StartPage doesn't seem to believe in it, unlike Qwant). But with the situation as is, I **cannot recommend StartPage at all** due to the censored results and sharing your system data with Google. Use only for emergencies when you **really** need Google's huge web index. UPDATE: actually, **fuck that**. StartPage just literally got bought by an advertising company (archive) (MozArchive) and also ran a Mozilla-esque PR piece (archive) (MozArchive) defending the acquisition. UPDATE November 2020: now they became totally authoritarian, hating TOR, VPNs and even *"private browsers"*.

Just checking ...

We apologize for the inconvenience: to prevent possible abuse of the Startpage.com service, your Internet connection has been prevented from accessing it at this time.

This happens when a large number of search requests are received from one's Internet connection in a short amount of time -- for example, if you are using "screen-scraping" software, or if you are sharing a connection with many people, perhaps through a proxy service.

Otherwise, if you have received this message in error, please help us in investigation by providing following information:

- Are you using TOR or other anonymous proxies?
- Do you have special browser configuration or extensions?
- Are you using VPN?
- Are you using a company network?

We will seek to refine and correct this whenever possible. Thank you for your patience.

This reminds me of malicious Cloudflare browser checks, where they compare your setup to

what they consider "safe" to decide whether to let you through. I found this out in November, but it's probably been around since earlier. To be honest, I've always felt something was off about these guys; their image was "too clean" if you know what I mean. Now we have proof that for them, "*privacy*" has only served as a useful slogan; they never actually gave a shit about it. Therefore, I can honestly advise to **avoid these frauds completely** now!

UPDATE March 2022: Perhaps I wasn't clear enough, so let me make a stronger statement. StartPage's (Google's) censorship is absolutely disgusting. You will find nothing but what your malicious so-called "elites" want you to find. No COVID skepticism, no analyses of staged events like the so-called US capitol riot. StartPage will ignore your search query if it would result in unapproved opinions, it is nothing but a drip of propaganda. If you like being a slave, sure, keep using StartPage. But I'm a free man, and I throw mind controllers like StartPage into the trash!

W Wiby.me W

An interesting new search engine dedicated to lean, personal, old-school websites. Really recommend keeping an eye on that one - and you can literally support the creation of a better Internet by submitting websites to it (if you know a good one, you should really do that). **No big corpos allowed here!** Does not require JavaScript (actually, there is not a single script on its page). Keeps logs for 48 hours (archive) (MozArchive), though.

 DuckDuckGo 

"The search engine that doesn't track you!" Or at least, that is what it claims. The marketing is

slick and I must admit I fell for it initially and was a fan for a long time - but to be honest, there were **always red flags**. DuckDuckGo hosts a privacy site (archive) with some great guides. They've refuted (archive) (MozArchive) myths (archive) (MozArchive) and went after giants like Google (archive) (MozArchive) - always a plus in my mind and a huge reason to consider a provider trustworthy. Their Twitter account posts privacy stuff all the time, etc. At a glance, DDG appears as just a group of people like you and me, looking to protect their privacy and creating a service to do so (unlike Mozilla's in-your-face manipulation). Unfortunately, like the great magicians they are, they've made a **really convincing illusion** - but still an illusion; and I will show just how.

As I said, the red flags were always there. Gabriel Weinberg - the DuckDuckGo founder - used to run the Names Database (MozArchive), a social network allowing you to reconnect with your old friends from school. However, the most important feature - sending messages - was **locked behind a paywall** which could be bypassed if you **invited 24 people to the network**. They claimed that you could remove yourself from the database if you wanted to:

We enable people to remove themselves from The Names Database at any time, which instantly and automatically deletes any personal information associated with the profile removed from The Names Database.

However, the service did not really respect the user (MozArchive):

(e) The Terms may be modified only by Company posting changes to the Terms on Website. Each time User accesses Website, User will be deemed to have accepted any such changes in effect at the time of access.

Just by visiting the website you've accepted all its terms (what if they've included a line "we can kill you in your sleep") while you weren't looking? Haha.

(a) Company owns all information submitted to it, regardless of who or what submits it, what is submitted, or how or why it is submitted. Such information includes but is not limited to any and all information submitted by User or about User and any User Information submitted during membership or through the normal use of Website and the services available through it.

(b) Any successors or assignees of Company will by default acquire for their own use, in accordance with the Terms, all information collected by Company, including but not limited to all information associated with Website as specified in section 2(a) above.

So everything you submitted there **ceased to become yours** (or even if someone else posted your personal info), and could have been transferred to any other company. Later versions of the agreement ([MozArchive](#)) contained even more egregious stuff such as:

Opobox reserves the right (but not the obligation) to remove or edit Your Information

you may NOT [...] (e) "meta-search" any Opobox Web Site; (f) forge headers or otherwise manipulate identifiers when communicating in any way with the Opobox Web sites [...] (j) use data mining or any data gathering or extraction tools; (k) copy, reproduce, modify, create derivative works from, distribute or publicly display any content (except for Your Information) from the Opobox Web Sites;

So I can't change my user agent; use wget, httrack or curl; or even take a screenshot of the site.

Funny shit. And this is all stuff that the later DDG founder agreed to. Then he sold the database to another company, Classmates.com (archive) (MozArchive), which added this to the agreement:

By registering on the Opobox Web Sites, as an added benefit you will also be automatically registered on Classmates.com, which is owned and operated by Classmates Online, Inc. ("Classmates"), Opobox's parent corporation. To complete this registration on Classmates.com, you consent to have Your Information provided to Classmates by Opobox. Classmates services are provided pursuant to its own Terms of Service and Privacy Policy.

So the privacy guru that later founded DuckDuckGo **sold all your data** to an even more unethical company (archive) (MozArchive). Did he have a sudden change of heart and created the uber-privacy-respecting DDG? Let's check it out:

DuckDuckGo used to claim in its privacy policy that no cookies are used by default, but some years ago it turned out they were setting a cookie from a third party (MozArchive), contrary to their policy. It was only on their help page and they fixed it quite fast. So is that all I've got? A cookie from ages ago?

In their Privacy Policy (archive) (MozArchive) they proudly proclaim - in big letters - that they *“don't collect or share personal information”*. The big question here, of course, is what is meant by *“personal information”*. It turns out that, for DuckDuckGo at least, **search queries alone are not personal** - even if you search for something only you could know. I'm pretty sure most people would disagree with that. DuckDuckGo claims that it is fine if you don't store the user agent or IP address along with the search, though:

We also save searches, but again, not in a personally identifiable way, as we do not store IP addresses or unique User agent strings. We use aggregate, non-personal search data to improve things like misspellings.

What this “*non-personal search data*” consists of, is of course not stated. Is it really only the search queries DDG saves? We do know that, for example, **DuckDuckGo tracks Pale Moon usage** through a parameter in the search query (“*?t=palemoon*”), which is there by default. This also likely happens for their other partners (archive) (MozArchive). Is that not already personal? Could it not be used to link your searches? The funny thing is, DuckDuckGo has spent much of their privacy policy criticizing Amazon for leaking their search queries (archive) (MozArchive), which were able to be linked to single users because they fucked up their anonymization. Can you ensure this also couldn't be done for DuckDuckGo's saved searches? After all they do track other information as I've shown earlier. As DDG itself says (archive) (MozArchive), “*The only truly anonymized data is no data*” - so why not just **not store the search queries**? From the techcrunch article:

The most serious problem is the fact that many people often search on their own name, or those of their friends and family, to see what information is available about them on the net. Combine these ego searches with porn queries and you have a serious embarrassment. Combine them with “buy ecstasy” and you have evidence of a crime. Combine it with an address, social security number, etc., and you have an identity theft waiting to happen. The possibilities are endless.

How long does DDG store the search queries? That is not explained! They do admit they will “*comply with court ordered legal requests*”. What could law enforcement do if they came across queries that **only I could have searched for**? Could those be used against me? No idea but

I'd much rather not have that happen! Then, DuckDuckGo admits to running experiments on their users ([archive](#)) ([MozArchive](#)):

First, you might notice that when you search DuckDuckGo, there may be an "&atb=" URL parameter in the web address at the top of your browser. This parameter allows us to anonymously A/B (split) test product changes we make to DuckDuckGo.

Second, we measure engagement of specific events on the page (e.g. when a misspelling message is displayed, and when it is clicked). This allows us to run experiments where we can test different misspelling messages and use CTR (click through rate) to determine the message's efficacy.

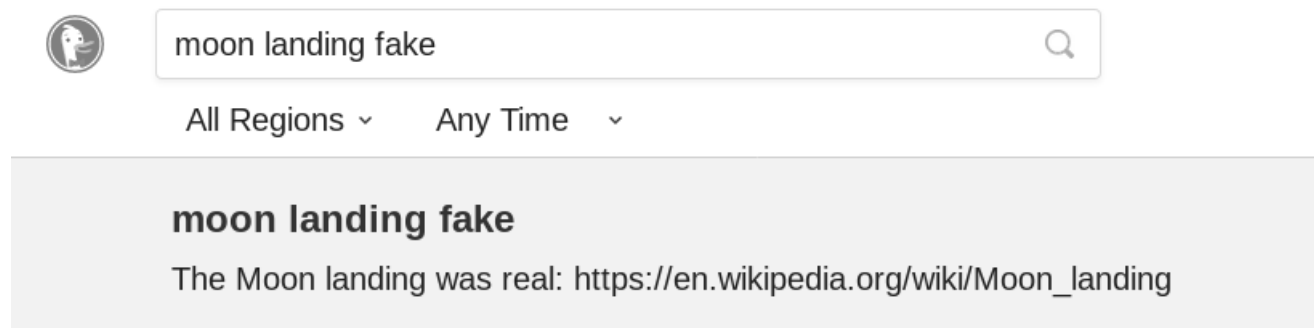
For example, our browser extensions and mobile apps will send an atb.js request with each search made. These requests allow us to count approximately how many devices accessed DuckDuckGo

That's quite a lot of information, and right after **criticizing so-called anonymous data collection!** This is exactly what I've criticized Mozilla for doing and in fact what prompted me to rewrite this whole section (and article). **Gabriel Weinberg** has shown himself to be **hypocritical and broke trust** on many occasions. For a recent one, he has put his shirt selling service behind Cloudflare (a MITM) without notifying the buyer in any way. So what's the final verdict on DDG?

There's no IP storage nor most of the other data search providers usually collect. Third party requests are not made. There is a JS-free version (**results don't go beyond first page**) and they do host a Tor hidden service (which **blocks non-TBB browsers** - tested with Iridium). For the

non-privacy relevant stuff: the search results are really fucking good; Bing and Yahoo are used for them, as well as their own crawler. More than that - DDG displays "instant answers" from over than 400 different sources in the top right corner of the window. Has ads that can be disabled in the settings. In addition to regular sites, DDG can search for images, videos (YouTube results only) as well as news. However, digging deeper shows several serious issues with the founder's lack of reliability and trustworthiness. He clearly **does not truly care about you or your privacy** - as the recent Cloudflare inclusion shows. Being the great businessman that he is, he has pretended very effectively that he does and took great advantage of the recent privacy scares. So, if you care only about pure privacy / functionality, DDG is pretty good still - but due to the shaky ethical foundation and enough cracks if you look hard enough, I **cannot recommend it** as enthusiastically as I did before. You could say it's the Tutanota of search engines - good enough as an entry point, but you can do better. There is nothing out there even approaching the level of RiseUp's email service, though; so DuckDuckGo remains a viable option for regular usage still. **UPDATE September 28, 2021** Now blocks Indian IPs due to some *IT Act 2000* (presumably a law). **UPDATE March 2022:** they now censor (MozArchive) *"Russian disinformation"*. Fuck them.

UPDATE June 2022: DuckDuckGo now includes a misinformation detector:



Are they going to remind me to take my booster next? Earlier I have said DDG belongs in high tier despite the privacy and historical issues. But with the recent violations, CuckCuckGo belongs in the trash instead.



UPDATE September 2021: French search engine using its own index plus Bing. As far as I can see, most of its flaws have been fixed. TOR and VPNs are accepted now. The search results are not being "eaten" anymore. JavaScript-free for all the categories, with a better interface than SearX. The side options have also been improved, with more sources for videos (Dailymotion in addition to YouTube) and news (but the social media and music categories have been deleted). **Qwant Lite has a massive flaw**, though - namely that you can't copy the link addresses since Qwant sends them all through some kind of local redirect. This makes it annoying when you just want to link something in an article instead of going there yourself.

However, the privacy policy has been revised (MozArchive), and it's become worse. I suspect they are simply revealing what was the case all along. Anyway, let me analyze the updated privacy policy:

Qwant stores your search queries for 12 months, and for the first 7 days connects them to an unique identifier:

Qwant retains for 7 days the keyword(s) entered associated with a pseudonym identifier calculated from the User Agent of your browser and the salted hash of your IP address. After this period, the keywords are no longer associated to an identifier and are retained for 12 months for aggregate statistical analysis

Microsoft (“*this partner*”) gets your full IP and stores it for 18 months:

Qwant may also collect and transfer to this partner your full IP address.

This data is transferred to this partner within the European Union, and may be retained in accordance with Bing’s Privacy Policy for a maximum period of 18 months.

Qwant, also, collects pretty much everything in order to “*evaluate its audience*”:

- – *The source of the user’s visit to the site (the HTTP referrer and the search field used to trigger the request);*
- – *Information about the type of link clicked (for example the position of the clicked link in the results with the number of results proposed);*
- – *Some information deduced from your User Agent (type of browser, operating system, major version of the browser,...)*

I can't say I'm very impressed with their privacy policy, regardless of their front page posturing. Especially the Microsoft partnership is worrying. Anyway, let's check out [their ToS \(archive\)](#) ([MozArchive](#)):

In the event that you notice content that may relate to apologies for crimes against humanity, provocation to or apologies for acts of terrorism, incitement to racial hatred, towards people on the basis of their sex, their sexual orientation or identity or handicap, child pornography, incitement to violence, attacks on human dignity, when browsing the Services, you have the option to let us know by contacting us at the address legal@qwant.com (also available at our FAQ).

All I need to know is here. Qwant accepts the removal of entries that violate their favorite victimhood issues. Wouldn't be surprised if they are also covid cucks who will remove alternative information about it.

What is the verdict, then? Privacy policy isn't that great anymore (Microsoft is getting your shit), but otherwise it's fine. The censorship is worrying but I haven't heard a practical case of it. **UPDATE September 28, 2021:** they now block Indian IPs since about a week ago. Gave a non-answer ([MozArchive](#)) when asked about it:

Hello, this is a difficult decision, but we have decided to close access to our services in some countries where we feel we cannot provide the expected quality of service. We apologise for this. Best regards.

UPDATE March 2022: another bunch of cucks that censor so-called ([MozArchive](#)) “war propaganda” (but only if it comes from Russia). Fuck them too.



UPDATE September 2024: now paid-only. Probably going to die altogether soon:

The reason is that Yahoo terminated our contracts unilaterally and without any notice on Monday. Upon request, we were merely informed that Yahoo would no longer be operating the business in Germany. For us as the operator of MetaGer, this means on the one hand that we no longer receive any advertising revenue, which has been used to pay for office space, servers and employees. On the other hand, we will also no longer be able to deliver our search results as part of the ad-financed search. Only with Yahoo did we

have a central deal to receive search results in return for advertising. This no longer applies.

This reveals to us two important issues. First of all, any search engine without its own index is a slave to its parent provider. And when he pulls the plug, it might scream and cry, but it will die. As happened here, the upstream violator won't even bother to tell you you're getting murdered.

Second, all big search engines depend on being able to fill your mind with clutter / trash / bullshit or as they are colloquially called, "advertisements". Which often (like here) also comes along with additional tracking, or inconveniences such as not being able to copy a link. And when the ad-spam money dries up (like here), they just helplessly die. It's time to think about how our everyday usage of the internet is held up by something that brings massive ethical problems and can snap anytime. We should only be using search engines that have ethics built in; one ad-spam and we're out! Anyway, here's the old review that is now completely irrelevant:

This one from Germany also advertises itself as private, but it not only stores your IP (archive) (MozArchive)...

For this purpose alone, we store the full IP address and a timestamp for a maximum of 96 hours

...but also shares a part of it with advertisers:

To receive this advertising, we give the first two blocks of the IP in connection with parts of the so-called user agent to our advertising partners.

Then, their website collects and stores the following data for up to one week:

Your IP-Address, Name and URL of the retrieved file, Date and time of access, The referrer you sent, The user agent you sent

So, as we can see, MetaGer is not so great for privacy (**Edit:** but it's not so bad either. At least we get the duration - which most services don't bother to give - and it's not long). A later section says this:

When using the MetaGer plugin, the following data is generated:

IP-Adress: Will not be stored or shared.

User-Agent: Will not be stored or shared.

It would be easy to assume that searching through the MetaGer plugin (unlike their site) stores no logs, but that would be naive and wrong. In fact, the first sentence of the “*Accumulating data by context*” section disconfirms this interpretation:

When using our web search engine MetaGer via their web form or through their OpenSearch interface, the following data is generated:

And then comes the stuff about IP storage and everything. So, all the above means is that the plugin usage stores no **additional** data over what the site itself already does. So, MetaGer's privacy is not that good, but at least you **do get a maps service that stores no logs:**

When using the MetaGer map service, the following data is generated:

IP-Adress: Will not be stored or shared.

User-Agent: Will not be stored or shared.

Search query: Will not be stored or shared.

Location data: Will not be stored or shared.

UPDATE March 2022: I don't know why I ever said the search results aren't that great, because they are. I recommend using either the onion or the German mirror, as they include Yandex in their searchable index. This will find you some results the English version won't, though the onion will throw you a captcha sometimes. There is a great *“Open Anonymously”* feature, which means you can view the sites through MetaGer, instead of going to them directly (this is the same as StartPage's *“Anonymous View”*). MetaGer, also, has pretty good image results - which work with JS disabled, as everything else other than the maps. The privacy policy isn't great, but at least it's concise and contains no unnecessary posturing, which is commendable, I guess. You can change the language used for the results in the hamburger menu at the top, last option.

UPDATE August 2023: MetaGer, instead of just the Bing ads at the top, now also serves a bunch of "partner" results mixed in with the others (no idea when they've implemented it, but seems pretty recent). When you click them, you are taken to the destination only through an intermediary site *tatrck*, which is Cloudflared - so for TOR users, or users of unconventional browsers etc. those results will be unavailable. You also can't copy a "partner" search result and share it with someone without that intermediary getting in the way. This makes MetaGer now unsuitable for its main purpose, that is actually finding information and being able to read it. We won't even get into the data collection done by tatrck itself; it being Cloudflared indicts it enough. Edit: way, way too many sites are *“partners”*, which also disables the *“Open*

anonymously” functionality for them, that I was hoping to use for some CFed sites. I think MetaGer just killed itself.

Jive Search (DEAD)

Another one with seemingly zero logging - *“we don't store your search terms, ip address nor information about your browser.”* - and even has a Tor domain. Supports searching only for regular sites (results sourced from Yandex - very high quality according to my short testing) and images (on the other hand, these **suck**). Provides Instant Answers similar to DDG and SearX, as well as proxy links (with JS stripped out to prevent tracking and deanonymization). As with Ecosia, MetaGer and StartPage - relying on a single source for the results, regardless of its quality, is subject to eventual bias and censorship. That, as well as absolutely zero customizability (can't change the basic, ugly default theme, or even turn off autocomplete) means it's probably worse than DDG. Edit: bumping it down since the amount of results is being cut off for some reason. Apparently the engine itself contains much more functionality - but the actual instance sucks, and that is what I'm rating.

Mojeek

I'm just going to rewrite this. In an age of widespread (archive) (MozArchive) censorship (MozArchive), Mojeek is significant because it is focused on unbiased search results (archive) (MozArchive):

Mojeek doesn't have an agenda, and neither does it support any particular view, whether that's in regard to politics or if blue is a nicer colour than green. And that's the way we

believe search engines should be. Our task is to provide you with relevant search results, not to force a point of view on you, or hide ones we don't agree with.

As far as I know, **no other search engine makes this commitment**. Mojeek can do so because it is **using their own index, instead of relying on the censoring violators**. Though the results are not as good in terms of e.g scientific or technical queries, they're a lot better than I remember them being a few years ago. And - in an age of mind control - a hard stance against censorship is more important than slightly weaker results. **JavaScript is not required** at all, even for images. What about their privacy (archive) (MozArchive)? They don't store IPs:

IP addresses are not recorded, instead the IP address is replaced with a simple two letter code indicating the visitors country of origin.

There is also no third party sharing:

The remaining log data (country, time/date, page requested, referral data, and in a separate log browser data), which although now contains no identifiable data, would still in no situation whatsoever be sold or distributed to any third party vendors

This is better than what almost everyone else is doing. Please remember that any search engine proxy (such as StartPage or SearX) has to by definition send the requests to the search engine it is proxying. This means a violator gets at least your query, and probably browser data and the other stuff. Mojeek can avoid this due to using their own index, and keep the data only for themselves. **It does store logs though** (the ones given above) and the duration of data storage is not stated. Still, finally we have an independent, non-censoring search engine that at least somewhat cares about your privacy. Unfortunately, Mojeek is pretty useless for non-English

results.



UPDATE June 2021: now Cloudflared, and therefore useless. Their claim to fame has been planting trees for every 45 searches (that's an average) you make using their service - but this, of course, relies on Bing ads being displayed (and I doubt it can counter the rampant deforestation, anyway). It's not very private by default - *“For example, when you do a search on Ecosia we forward the following information to our partner, Bing: IP address, user agent string, search term, and some settings like your country and language setting.”* However, it claims to respect the DNT header: *“If you have “Do Not Track” enabled in your browser settings we do not collect any analytics data. Most other websites ignore this setting - we think users should have a choice.”* Is the IP address apart of analytics data? Depending on how literally the DNT information is interpreted, ~~Ecosia can become a pretty good choice, combining ethics and privacy~~ (okay, this clearly isn't relevant now after *Ecosia* became Cuckflared). You can search for regular sites, Images, Videos, News and Maps. However, the search results are sourced exclusively from Bing. Will work without JavaScript but the images will not be displayed at all.



UPDATE September 2022: can almost never get this to search anymore. An allegedly private one with a not-so-good privacy policy (last updated 2 years ago...). It proudly proclaims several times how it doesn't store information in a way that can identify you (can you be any more vague), however the myth that this is a privacy-respecting practice has been busted (archive) (MozArchive). And they don't actually say what they DO store and for how long - an indirect

admission that they do store quite a bit of data indeed. Then comes this gem: *“Oscobo uses cookies to determine the effectiveness of our own marketing campaigns”*. And the funniest thing is I don't see any cookies being set in my uMatrix (outdated privacy policy, as mentioned before; however, it does show they did that at one point, or at least planned to do so). Then it says: *“Oscobo uses proprietary technology to hide you search history from others who may use your device after you search. This may save you from some embarrassing situations”* But I see the search queries in my browsing history, plain as a day - so this claim was a mistake too (and a negative one this time). Oscobo can search for images (flickr only - almost useless), videos and maps (embedding google directly, yawn); it doesn't require JavaScript but images won't show up then. Anyway, due to the issues mentioned earlier, this search engine does not seem trustworthy at all, and I don't recommend it. It has nothing over the more widely known ones and for something even funnier, it contains a direct link to some shady "Oscobo Browser" executable file. Haha - avoid.

Discrete Search

UPDATE March 2022: This trash doesn't work anymore in Pale Moon or Librewolf. I have no idea why I even checked it out, but there you go.

To work properly, this one needs all of cookies, JavaScript and XHR enabled. What do you get for that? Let's check out their [privacy policy \(archive\)](#) ([MozArchive](#)):

Discrete Search does not track search history in any user identifiable way.

The big lie of so-called private search engines rears its ugly head again. The reply is the same as to Oscobo - "user identifiable" is vague and often includes a lot of information that can

reveal you if put together (archive) (MozArchive). Why not just mention what the fuck do you store and let us decide whether we're comfortable with it? Graciously, Discrete Search DOES provide that information later (unlike Oscobo):

Additionally, we store aggregated search data to improve product performance, but never store IP addresses or unique user identifiers in connection with such searches in order to ensure that none of the information collected in connection with your search activity is personally identifiable.

So “*aggregated search data*” is logged; the important part comes next though. If you read between the lines, they admit that they **do store your IP address** as well as “*unique user identifiers*”, just allegedly unconnected with search queries. And that is what you call private? No thanks! Why rely on someone's dubious "unconnecting" when they could just **not store the data**? And Discreet Search does seem to store a lot of it, increasing the risk. Then there's this gem from the TOS (archive) (MozArchive):

You certify that you own all intellectual property rights in Your Content. You hereby grant us, our affiliates, and our partners a worldwide, irrevocable, royalty-free, nonexclusive, sub-licensable, license to use, reproduce, create derivative works of, distribute, publicly perform, publicly display, transfer, transmit, distribute, and publish Your Content and subsequent versions of Your Content for the purposes of (i) pursuing our business interests, (ii) distributing Your Content, either electronically or via other media, to third parties seeking to download or otherwise acquire it, and/or (iii) storing Your Content in a remote database accessible by third parties. This license shall apply to the distribution and the storage of Your Content in any form, medium, or technology now known or later developed.

TL;DR everything you submit **or transmit** to the engine becomes theirs (not just queries but stuff like the headers your browser sends), and they are going to store it in unspecified third party databases. Ha ha. Discrete Search puts fucking **image ads** on top of your searches - a practice I've never seen anywhere else. At least they've fulfilled the promise of encrypting your searches locally, unlike Oscobo (yeah I've checked). Still, avoid this trainwreck.

Gibiru

Claims to be “*Protecting Your Privacy Since 2009*” on its main page. If you read their privacy policy, it all checks out - Gibiru stores no logs or cookies. Of course, what they've neglected to mention is that they **literally use Google directly for their results** (without proxying them, like StartPage does or Scroogle used to). Gibiru will not work without enabling Google scripts, and so all the data that it allegedly doesn't collect, Google will happily take instead. Unfortunately - as you can see - search engines have their fair share of frauds too. **Avoid!**

Gigablast

UPDATE May 2023: Dead! Ugh. RIP. Had a nice 23 year long run. Though it's not necessarily over forever.

Independent search engine, ran since the year 2000. Gigablast's index is surprisingly good, and it **does not appear to censor** (same as Mojeek). However, it requires JavaScript to display results. Image search shows only thumbnails alongside text, no "gallery" like everyone else does, so you will need to use something else for images if you want that functionality. No third party requests, good privacy policy, preventing third party sharing of your data and deleting

logs “regularly” - though that is not elaborated on.



UPDATE May 2023: now redirects to Kagi Search that's paid and seems completely different, review maybe coming soon.

When I learned of Peekier after rating some less-than-stellar search engines, I was delighted to finally find another one that respects the user. There is no IP storage, no third party requests, no logging the data your browser sends (aside from temporary search queries - same policy as DuckDuckGo). It also has the handy feature of displaying the resulting website without visiting it - showing you the relevant information in an efficient way. And then I see this:

Cloudflare, our caching provider, may use a single session cookie for anti-DDOS measures.

Okay, so while YOU might not store anything, Cloudflare - hiding in the shadows between you and me - will happily take it all. And this claim - then - becomes a lie:

SSL/TLS is enforced throughout the website. No unencrypted information is transmitted over the internet.

Because Cloudflare **decrypts the request on their servers**, it cannot be said that the information is encrypted for its whole journey. Since Cloudflare might be the biggest current Internet evil (archive) (MozArchive), I cannot just let this seemingly small point slide. Of course, Peekier also claims it “*does not use cookies in any way to track you or store personally identifiable*

data”, but it does require a Cloudflare cookie to work (which is literally a tracking cookie), as well as enabling JavaScript. And that, my friends, ruins a search engine that could have topped the list.

▣ Presearch ▣

Some people have inquired about this, so I guess I have to write about it. I'm so tired of these crypto scams, which is the entire reason to exist for Presearch, it seems. You can earn their special crypto token in there by searching. Though there are some serious requirements (archive) (MozArchive) to satisfy:

For Usage Rewards:

1,000 PRE must be earned in order to claim Usage Rewards

A maximum of 1,000 PRE may be claimed every 90 days

Presearch reserves the right to increase or decrease these thresholds at any time

So, you cannot withdraw your funds until you earn at least 70 USD. The really malicious part is that they can change that amount at any time; no problem to start requiring 10 000 or a trillion PRE to withdraw; you cannot ever feel confident that you will be actually able to do so. Many people on their Twitter (MozArchive) are complaining that they can't withdraw their funds even a year later, so this has all the hallmarks of a crypto scam. Presearch can also just steal the tokens you've earned:

If a Member stakes PRE toward search staking and then is determined by our fraud detection system to have generated invalid search or referral activity, then their staked

tokens may be forfeited and not recoverable.

Any advertiser can buy his way [\(archive\)](#) [\(MozArchive\)](#) into this system:

To enable advertisers to have their ads displayed under certain keywords that the advertisers 'stake' their tokens against

The biggest payer for a given keyword wins and gets their ads through to you:

Advertisers can stake their PRE to a keyword, and whichever advertiser stakes the most tokens will have its ads displayed when a user searches on the term selected.

To participate, they will have to buy at least 70 USD worth of the PRE token, for which Presearch charges 10% markup [\(archive\)](#) and that they can of course steal at any time. This is funny too (as if they couldn't make it anymore obvious what they're doing):

If paying by credit card, a 7 month hold on ability to withdraw tokens to the blockchain may be applied to protect against charge backs

You can also host a node, and if you pay 4000 PRE [\(archive\)](#) [\(MozArchive\)](#) (280 USD; who's going to spend that much on this scam?!), you will also get rewarded for it:

In order to incentivize node operators who commit to providing consistent, stable and responsive computing resources, we are paying Presearch PRE tokens as rewards for node operators who stake a minimum of 4,000 PRE tokens on their node.

FOSS lovers can go home because the node software is closed [\(archive\)](#) [\(MozArchive\)](#):

This software is currently not open source and you are relying on our assurances that nothing malicious is happening underneath the hood. We promise that this is true, but the ability to verify it for yourself would currently be limited to packet sniffers and any other means that you have available to you. It is our intention to open source this software in the future, but we're not there yet.

Either way, you will almost certainly not earn [\(archive\)](#) [\(MozArchive\)](#) what is required to cover your spendings:

Though the amount paid is variable, we are also ensuring that any node operator who successfully served at least one query receives a minimum of 100 PRE, with numbers increase from there up to about 70x that amount for the most active node operators.

Signing up for an account requires solving malicious hCaptcha, which I obviously didn't bother to do so I don't know what information is required to give otherwise. You don't need to care about this if you only want to use the engine though - but then, why bother? It's not too good and the results are heavily censored for queries like *“Moon landing was fake”*; Presearch does not have its own index [\(archive\)](#) [\(MozArchive\)](#):

The next step is to begin layering our own index on top of this platform so that community-driven results can supersede the external results

“Next step”, meaning it hasn't happened yet. It relies on [\(archive\)](#) [\(MozArchive\)](#) *“a number of the world's top search engines and other data sources”*, like everyone else. So the claims of it being *“decentralized”* are fake, too. Using Presearch requires JavaScript and cookies to be enabled. Lots of data is collected [\(archive\)](#) [\(MozArchive\)](#):

- *Any information you provide through your profile (name, nickname, avatar, etc.)*
- *Your email address*
- *Your password (one-way encrypted)*
- *Any information provided when making a purchase*
- *Account referrals*
- *The search engine providers you select*
- *Search events (when a search was conducted, how many tokens were earned, and which provider was used)*
- *Your IP Address*
- *Your blockchain wallet address if you submit or connect it to your account or use it for a deposit or withdrawal.*

It is also all shared with shady “*Business partners*” that are not specified:

Partners. We may share transient information with trusted partners during a particular request, for purposes of providing the Service. This may include trusted advertising providers who contractually agree to delete the information after the request is completed so that it is not stored.

When Presearch finally decides to fuck off, they will give their buyer all the data they've collected:

Business Transfers. We may share personal information when we do a business deal, or negotiate a business deal, involving the sale or transfer of all or a part of our business or

assets. These deals can include any merger, financing, acquisition, or bankruptcy transaction or proceeding.

As was obvious all along, Presearch is a crypto scam pretending to be a search engine. Its existence is based entirely on advertisers buying their way in (with a 10% cut for Presearch) to shove ads down your throat, and then Presearch doing everything to prevent the exchange of their tokens to a cryptocurrency that is actually useful. But of course people got lured in by promises of easy money and revolutionizing searching through “*blockchain technology*”. Trash it and don't look back.

UPDATE August 2024: I got notified that this section was linked in the [Presearch subreddit \(archive\)](#) ([MozArchive](#)) and saw that the admin apparently replied to it. So let's see what he has had to say:

I don't know where you got that article from but that's not from Presearch, For security reasons it is better that you do not open it

Don't you dare look behind the curtain.

What that article says is incorrect, Presearch pays for the pre As long as you have used the search engine correctly

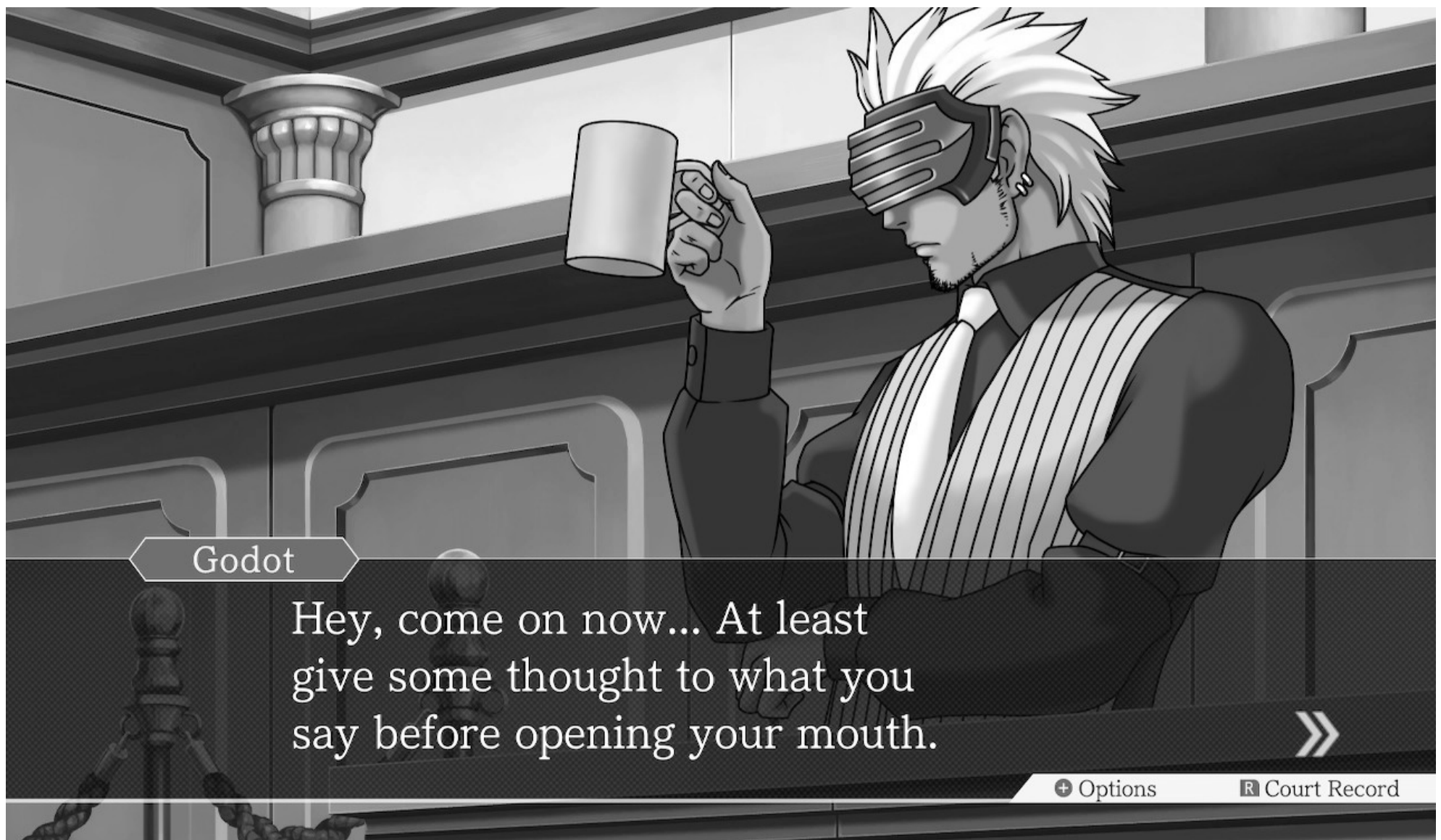
Were the Twitter reports fake then? Or maybe they all have simply not “*used the search engine correctly*”?

There is nothing arbitrary and the terms and conditions are clear,

Is this not arbitrary? *“1,000 PRE must be earned in order to claim Usage Rewards” [...]* *“Presearch reserves the right to increase or decrease these thresholds at any time”*. Yes, the "get out of jail free" clause is still there 2 years later and it alone exposes Presearch as a total scam. Because **you can never be sure of the ability to withdraw your tokens**. And the ToS is indeed *“clear”* about it.

And how about this for arbitrary? *“If your account is left dormant for more than one year, meaning that you do not login and record a search for 365 days, Presearch will consider your account abandoned and will rescind any unclaimed Rewards tokens in your account”*. Your tokens will get stolen after a year of inactivity regardless.

It's probably a person who cheated OR just used Presearch to get reward, Then he got upset because the anti-fraud system detected that he was doing token farming



I shouldn't even have to say it but I have not and would never sign up for this trash, nor try to earn its fake tokens. And just for fun, let's check out how the search results page looks these days:

bury this scam

Sign up to Earn

All Images Videos News **SCOUT** Share

Results from decentralized nodes in the eu-de-1 region.

Advertisers

To activate Presearch AI in your account, you must stake or hold at least 1000 in your PRE Wallet.

Presearch AI



academy.samcart.com/referral/hbafunnelbuilder/0i0AlzTqs02i8... 

2024: Make money online today!

Affiliate Marketers made \$177,586 in 2023 - ZipRecruiter.com *** Learn how today

www.bury.gov.uk/my-neighbourhood/fraud

Fraud

What counts as fraud · giving false information to pay less Council Tax · not registering for Council Tax when moving into a property · claiming to be on the only ...

www.reddit.com/r/MEDICoreTARDS/comments/1da8ffr/ntas_attempt...

NTA's attempts to bury NEET 2024 scam

The biggest NEET exam scam in history has just happened, affecting 25 lakh students! Thousands of futures are at stake. Watch my latest video to uncover the ...

www.scam-detector.com/validator/bury-com-review

bury.com Reviews: Is this site a scam or legit? – Scam Detector

bit★Starz



Top Slots & Live Games [Ad]

Spin and win with our top-rated slot games.

Try Now

Heh. Half the page taken up by a casino ad. Five ads on the left sidebar and two top search results are ads. And you want to tell me this crap is something other than an attempt squeeze money from people who have been bullshitted by its slick advertising? A quick look at their subreddit makes it even more obvious. This isn't even a search engine, my friends - that is just a cover for the scam similar to the microtransaction-filled games. Anyway, nothing really changed here (at least for the better) so run as fast as you can.

Right Dao

Another search engine with its own index; if you're hopeful, don't be - **it is bad**. I can't find anything related to conspiracies with my usual queries, though I don't necessarily think they are censoring things - their index is just that weak. Even obscure video game stuff doesn't appear - but does in eg Mojeek. After doing a few more tests with other queries, it appears I can find pretty much nothing I want to, so my verdict is that this search engine is useless. Oh, and no image search - just *Web* and *News*. Despite Right Dao being useless, let's check out its privacy (archive) (MozArchive) while we're here:

IF YOU ARE NOT AT LEAST 16 YEARS OLD, DO NOT USE THE SERVICES.



No.

Hey, I just happen to be 14. What you gonna do, report me to Joe Biden? Moving on...

We do not track our users, and do not collect user identifiable information.

I'm tired of these generic slogans, just tell us what exactly you collect - then we will decide whether we consider that tracking or “*user identifiable*”.

We collect very limited data to improve our service.

Improving search quality: we analyze user submitted queries and result clicks.

Sounds like tracking to me. And not very “*limited*”.

And we do not sell and share such data to any third-parties.

Thanks. At least there is that. But...

We retain the information we collect for as long as necessary to fulfill the purpose and for the purpose of satisfying any legal, accounting, or reporting requirements.

Worthless. Fucking worthless. Tell us the maximum duration, or you're no better than the biggest violators. Might as well have said nothing since this sentence doesn't provide any actionable information to the user (except to **stay away from you**). Since they admitted to collecting search queries and clicks, and the duration is unlimited, those might be used against you someday. [Their ToS \(archive\)](#) ([MozArchive](#)) contains something funny:

Access the Services by any means other than through the interface that is provided by Right Dao [...is not allowed];

You may not send automated queries of any sort to the Services

Curling chads can go home. Anyway, I'm getting tired already. Can I say something positive about this engine? Well, it doesn't discriminate against TOR or Pale Moon. And results appear

pretty fast, though they suck. Nevermind, this is pointless. Just skip it.



UPDATE February 2024: 4get now has a custom-made captcha required to solve before you can search; and you get 100 searches per solution. If you block cookies, then you get a new captcha for every search, which makes the engine unusable. There are 4get instances that don't have the captcha, though.

New search engine someone recently mentioned to me. It [promises to be simple \(archive\)](#) ([MozArchive](#)):

Provide users with a privacy oriented, extremely lightweight, ad free, free as in freedom (and free beer!) way to search for documents around the internet, with minimal, optional javascript code.

And private:

I don't log IP addresses, user agents, or anything else. The npt tokens are the only thing that are stored (in RAM, mind you), temporarily, encrypted.

Just the way I like it :D. Anyway, let's get down to the details. Right off the bat we have an advantage over SearX in that you don't have to fiddle with engines in the settings before you search - you **choose one during searching**. This means that results get displayed from only one of the source engines, but that is the way I prefer it. In SearX - if I wanted to see only the Mojeek results - I'd have to go to the settings and turn all the other stuff off, which is annoying.

What 4get does is much cleaner.

Another advantage is the availability of Yandex and Marginalia as source search engines, which SearX lacks. More importantly, 4get **actually lifts results reliably**; you avoid the famous failing search engines from SearX, which is what made me give it up completely. Though, this might only be temporary, before the source search engines start banning 4get. Enjoy it while it lasts (**UPDATE July 2024**: yeah, that's gone now). Overall, SearX has more search engines to choose from, but many of them are duplicates eg DDG and Qwant, or Startpage and Google - which use the same indexes. Still, 4get lacks a Google-based search engine option currently, which would be nice to have. **UPDATE July 2024**: exists now, as well as some other additions.

SearX has lots and lots more features...but to be honest, I've never needed any of them aside from the Wayback Machine integration - which is just a convenience feature that can be easily replicated by hand (edit: actually, it **does exist here** if you click the favicon of a search result, to the left of the text). What I don't like, though, is that - if using DDG or Brave source engine - images, videos, or Wikipedia results display on the right side of the page. I get that it's because the source engines themselves do that - but in a simple engine, I'd rather just remove that and only display the actual results. After all, *“Videos”* and *“Images”* are already categories that you can choose. So they shouldn't be mixed in with the textual results that you wanted. Wikipedia is also a propaganda site, so I hate giving it privileged space. I understand that this might be a bitch to code, though.

So, for me this is the **best search engine** for now. Aside from that small issue I mentioned above, it ticks all the boxes. 4get also has an onion domain. There is no JS dependency, either. Oh, maybe another issue is that the donation service is behind Cloudflare - but not really relevant to the engine itself. IMO, it should just give crypto addresses, and that's that.



Requested review. I hate doing these now, but this "patient" seems unique enough, so might as well begin the diagnosis and hopefully finish it quickly.

First of all, JavaScript is required to load the website at all. The website is horribly designed in general; to even reach the policies, you have to scroll to the bottom of it, but since “*trending stories*” keep being loaded, you will have to be really quick in clicking the links, since they'll be buried in a second or two - forcing you to scroll again. And if you allow the entire column for *freespoke.com* in uMatrix, an analytics subdomain will also get loaded, which you will have to separately block later. According to their [privacy policy](#) (MozArchive) ([archive](#)), Matomo collects this data:

the website from which you visited us from, the parts of our site you visit, the date and duration of your visit, your anonymized IP address, information from the device (device type, operating system, screen resolution, language, city in which you are located in, and web browser type) you used during your visit.

Freespoke doesn't specify directly whether it uses its own index or not, but I'm certain it doesn't. You can see in uMatrix that their image search simply loads the images from Bing. Their privacy policy appears to confirm the reliance on Microsoft's engine:

But we've learned, the hard way, that to reach a like-minded audience we must participate in the very system that we're trying to overthrow. Ironic? Yes. Hypocritical. No. Because we're working inside the beast to overthrow it. We're a trojan horse trying

to restore the Internet to a time when no one company could censor the information flowing to billions of people because that information dared to challenge said beast's political ideology.

Nice way to justify being cucks. Here are some other gems lifted from there:

This Website is hosted on Netlify. By default, Netlify collects your connection request, including timestamp, referring URL, IP address, and user agent, and all of that data is provided to and used by us only in the aggregate for basic analytics purposes (“Default Information”). According to Netlify’s policies, access logs, including IP address, are deleted after 30 days.

Netlify uses cookies to collect this information. The Website will not function without collecting some Default Information about when and where users are visiting our Website. This cannot be turned off, but it is stored and analyzed in the aggregate.

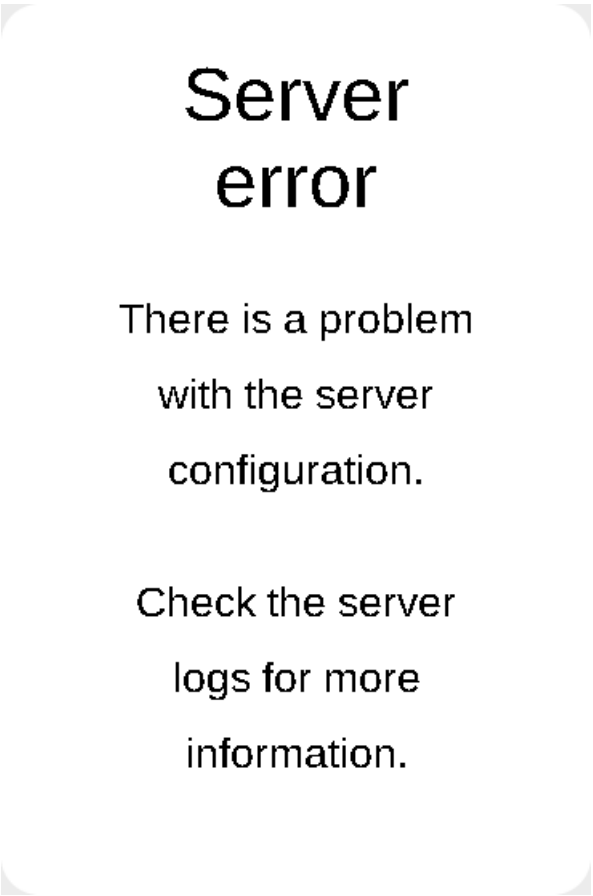
This disproves what they say in their [About page \(archive\)](#) ([MozArchive](#)):

Our searches are 100% private. Freespoke ensures every search is anonymous, with no intrusive profiling or targeted ads—your online journey is yours, and yours alone.

Is it truly mine alone? Or also Netlify's? And obviously Microsoft's. There is also no maximum duration for which the data will be kept:

We retain your personally identifiable information only as long as necessary for the purpose for which it was collected or as required for necessary business purposes.

And this is supposed to be private. What a disgusting fraud. You can also make an account, though I have no idea why you'd do so. In that case, Microsoft will store your personal information (*“Microsoft: We use Microsoft Azure, to store user preferences, “likes” and other individual choices you make for your account. We also use Microsoft 365 to host our email, and therefore Microsoft stores personally identifiable information regarding people with whom we email”*) - all while Freespoke claims you'll be able to *“Break free from big tech”* if you sign up. I wasn't able to create one, either way:



Server error

There is a problem
with the server
configuration.

Check the server
logs for more
information.

Assuming you did manage it and tried to log in, you'd see this:



Welcome Back to Freespoke

Log in to continue:

 Sign in with Apple

OR

Ha! I guess this is how Freespoke lets you “*Break free from big tech*” - by linking directly to <https://account.apple.com>.

Freespoke's ToS (archive) (MozArchive) contains even more gems than its privacy policy. Wow, it's a treasure hunt today!

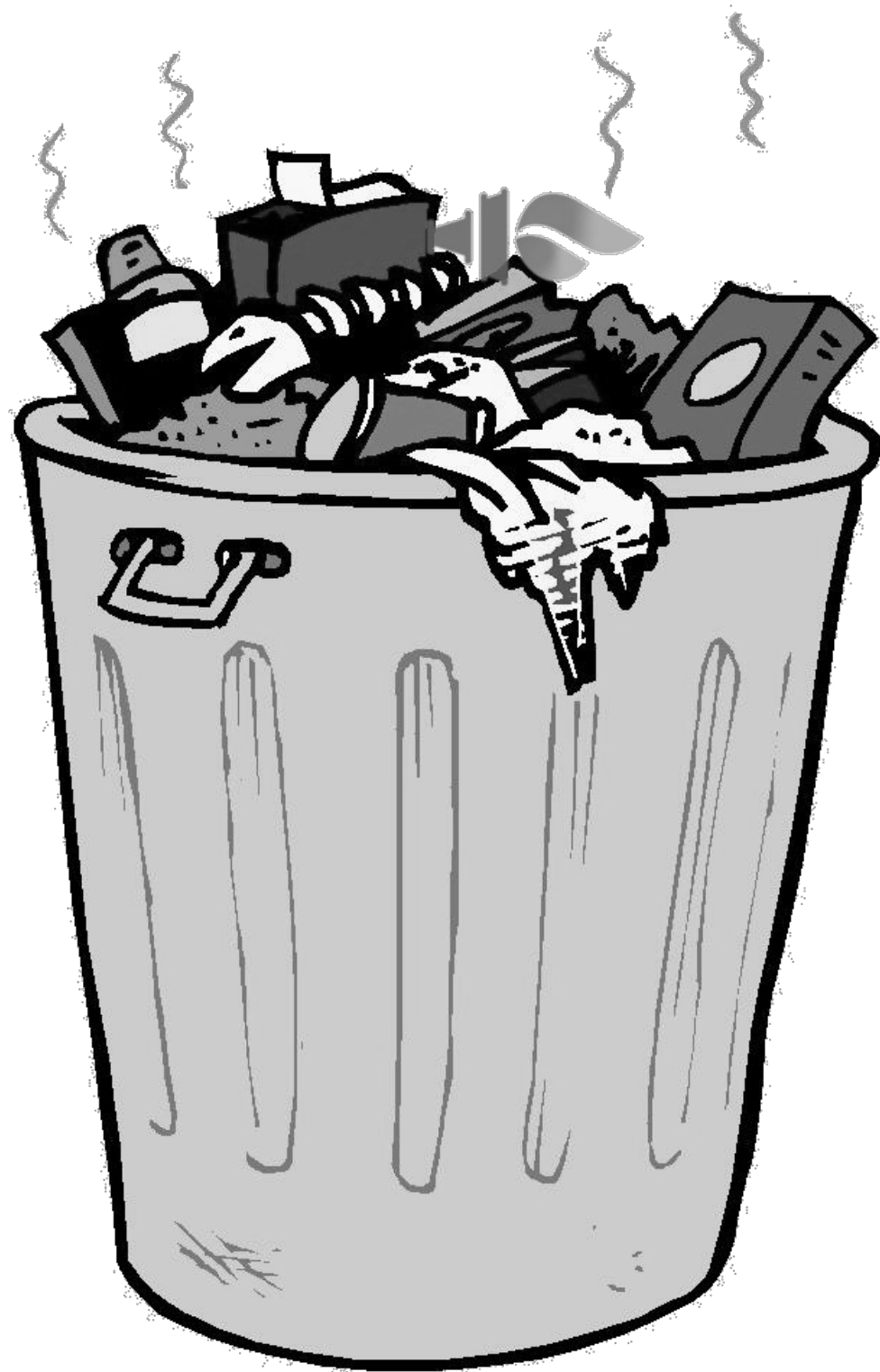
No part of the Websites may be reproduced or transmitted in any form, by any means, electronic or mechanical, including photocopying and recording, except that Freespoke authorizes you to view, copy, download, and print Freespoke documents (such as press releases and FAQs) that are available on this web site, subject to the following conditions:

- *The documents may be used solely for noncommercial, informational purposes*

only.

- *The documents may not be modified.*
- *Copyright, trademark, and other proprietary notices may not be removed.*

Fuck you and your "authorization". Now watch me reproduce and modify your copyrighted, trademarked logo:



Sorry for low effort but this trash doesn't deserve more. Anyway, waiting for the lawsuit; with Phoenix Wright on my defense team, I should be fine. Also, how does the entire “*Acceptable Use*” section make any sense? It's a search engine, I can't use it to “*post*” anything at all. Yet they list all these things you are not supposed to “*post*”, such as “*blatant expressions of bigotry, prejudice, racism, hatred or excessive profanity*” and “*obscene, lewd, lascivious, excessively violent, harassing or otherwise objectionable content*”. And if you dare to violate any of these points, which seemingly could encompass pretty much anything - you will be thrown straight into the legal mill to be ripped apart:

You agree that violations by you, or any person or entity acting on your behalf, of the terms of this Agreement will entitle Freespoke, in addition to any other remedies including referral for criminal prosecution [...]

What's even funnier is they require you to **defend them in court** - and even pay their attorneys' fees (!), which is double the mockery:

By using the Websites and/or Services, you agree to indemnify, hold harmless and defend Freespoke and its officers, directors, agents and affiliates from any claims, damages, losses, liabilities, and all costs and expenses of defense, including but not limited to, attorneys' fees, resulting directly or indirectly from a claim by a third party that is based on your use of the Websites and/or Services in violation of these terms.

So, that's what's supposed to happen if some “*third party*” simply **claims** you have broken Freespoke's ToS. Absolutely insane. But let's think deeper about it. How would they even be able to do so if search queries were not stored by Freespoke? Since that's the only content that's possible to submit through a search engine. And therefore, I think they are - and probably

forever, too. In that case, I really hope you didn't register an account and reveal any personal data for them to hang you with.

Anyway, if all of this isn't enough to bury this patient, let's cover his unique issues, which will definitely be fatal. Namely that **the search field will randomly eat your characters**, especially if you type fast. This makes it basically impossible to actually search, and alone buries this engine. I think this is related to the search suggestions that automatically get loaded (and **cannot be disabled**) for every typed letter. If you try to modify something that's already in the search field, the cursor will also get moved to the end after every key press, which seems like a programming mistake that a child would make. And it pretty much requires starting every request anew, but will still eat your letters. I even switched keyboards because I suspected it might be related to a new one I've recently started using, but it's not. Another possibility is that this issue is unique to Pale Moon, but I don't care even if it turns out to be so. Shouldn't ever happen either way, and no other engine suffers from it. Freespoke is also **extremely slow**, and simply doesn't do anything more than half of the time. Searching through TOR appears to work better for some reason.

I have trashed Freespoke enough, so let's try to provide some balance, though there is not that much available to even start tipping the scale the other way. However, one feature that I really like exists here, and AFAIK, not anywhere else. Look:

NEWS

[See All News](#)

NON-MAINSTREAM COVERAGE (6)

 Just The News
justthenews.com government courts-law
Judge reschedules hearing on whether The Onion can purchase Alex Jones' Infowars
MIDDLE 3d ago

 OAN
oann.com newsroom
X Platform Claims Ownership Of Alex Jones' Infowars Account Amid Bankruptcy Legal Battle
RIGHT Yesterday

[Load More Results](#)

 Benzinga
Elon Musk's X Objects To Sale Of Infowars Accounts To The Onion, Claims Ownership Over Alex Jones's Social Media

MIDDLE 19h ago



 Gizmodo
The Onion Wins Auction to Take Over InfoWars

LEFT 14d ago



 Fortune
The Onion buys InfoWars. Really.

RIGHT 14d ago

Definitely increases efficiency - especially the alternative sidebar. I can't say if the *“LEFT”*, *“MIDDLE”* or *“RIGHT”* labels actually check out, and I obviously question if they are even descriptive. After all, many types of left- and right- wingism exist. But I'm sure it has some value and I like the concept of labeling results simply in principle. It could in theory be adapted for other ways of categorization, too. This doesn't actually end up mattering though, because of - well - all the other stuff I've mentioned. They also brag about linking to some USA-made products - and while Americans might care about this, I don't. Oh, and they block porn completely, but are supposedly 18+ regardless.

▣ FindX ▣

I wasn't supposed to review any more search engines, but this one is doing such a great Mozilla impersonation (pretending to be private with the reality being otherwise) that I just had to do this writeup. To be honest, I have never heard of FindX and likely would not have if a reader didn't mention it to me - but **the level of its privacy fakery** is so great that it deserves a proud spot as the last entry in this report. Let's check out their [About page \(archive\) \(MozArchive\)](#) first:

Findx is a search engine for users who value privacy. We do not collect information about you when you perform searches, unlike most other search engines. Please read the details in our Privacy Policy. If you worry about companies creating invisible profiles of you based on your searches and internet browsing habits - Findx is for you.

The other stuff in there is not very relevant. Remember the above quotes while we inspect their [Privacy policy \(archive\) \(MozArchive\)](#). It starts with the usual GDPR stuff, but interestingly, it seems to try to squirm out of, or not explain properly, many of those rights you allegedly have. For example:

You can request that we restrict usage of your personal data. We are only required to comply in certain circumstances.

And from Section 9:

We may ask you for additional information to confirm your identity and for security purposes, before disclosing the PII requested to you. We reserve the right to charge a fee

where permitted by law, for instance if your request is manifestly unfounded or excessive.

Now compare the above with how Qwant treats GDPR ([archive](#)) ([MozArchive](#)). But since I don't put much value into these laws at all, let's move on to the more important sections - namely *"3.2 Findx Search"*, which will tell us what their engine actually collects.

[...] data is transferred to our search partners who only use it to provide better search results on Findx

So one "partner" wasn't enough, there had to be two - CodeFuel and Microsoft. FindX also shamelessly claims that *"Microsoft values your privacy"* - can you believe it? Anyway, what is the data being sent?

IP address, user agent string, search term, country and language settings, filter settings for adult content, active search filter settings (e.g. page number information), an optional Bing ID (read more below) and the ID of the organization that should benefit from your search.

So the privacy-respecting FindX shares pretty much everything possible with not one, but **two third parties!** Do they have an explanation for that? Sure they do - but I'm warning you - this will be **one of the most idiotic things you've ever read on the Internet**. Better wear a helmet, because the stupidity beam is coming!

"But you still pass on my IP-address to CodeFuel and Bing". Yes, we have to. We protect your privacy to the maximum extent allowed under the agreement we have with them.

Other privacy-centric search engines mask part of your IP-address before passing it on to their partners - we are not allowed to do that. It is a matter of trust. You have to trust that the privacy search engines do not pass on your full IP-address to their partners. On Findx, you have to trust that our partners only use it for what they say they will, which is to provide better results on our site (only) - nothing else. We trust them.

Wow, I've been hit with a hurricane of nonsense and I'm so confused I don't even know where to start with this. They literally admit to being worse than all other search engines - since those (such as Swisscows or StartPage) actually limit the data sent to the providers they rely on. FindX just says **fuck that** and dumps all your info onto Bing, then tells you to **just trust their partners** to honor an agreement that is never really specified aside from vague claims of "better search results". Sounds dangerously close to Mozilla's *"improve your experience"* while they abuse all your data. And why would Microsoft submit to some small fry like FindX? It's more likely they just do whatever the fuck they want with your stuff. What about the other partner, CodeFuel?

When search results are displayed, tracking pixels reveal to our search partner which of the results and ads we received were actually seen by you. Our partner, CodeFuel, solely uses this information for building metrics for us and statistics about the service usage. The information is not sold or shared with advertising companies. It simply provides us with information about earnings and various statistics like how many searches resulted in display of ads, how many unique users performed searches, how many results were clicked on etc.

So, FindX assures us that the data collection of CodeFuel is pretty mild. But their privacy policy (archive) (MozArchive) tells a different story:

Certain usage related information regarding your use and interaction with your device, including the Software & Services and Other Software, such as when and how you Use the Software & Services and Other Software, how you use your internet browser and internet search related applications, your language settings, the web pages you visit, applications you use and the content you see, access and utilize on such web pages and applications; for example, offerings and advertisements that you view, use and access, how you use them and your response to them (ie. clickstream data), how frequently you use them, your search queries and the non-precise location, time and date of your searches

Even though FindX explicitly claims in their FAQ (archive) (MozArchive) that this data is not shared with third parties...

CodeFuel acts as a 'middle-man' between small to medium-sized partners and Microsoft, and passes the data on to them in order to serve search results and ads. CodeFuel uses this information themselves to build metrics and statistics about the service usage. The information is not sold to or shared with anybody

CodeFuel does directly state several times that they do so:

In performing fraud detection and prevention, we use the services of third parties who will receive and access your PII.

*We also use your PII to comply with legal and regulatory requirements [...] For this purpose, we may share your information with law enforcement or other competent authorities and **any third party** [...] We will also share this information with our*

professional advisors in the scope of this purpose.

We may also share your information with our subsidiaries, affiliated and parent companies pursuant to the legitimate interest for the provision of the Software & Services to you but their use of such information must comply with this Privacy Policy.

So two "partners" turned into who the fuck knows how many. There is way more dirt on FindX - their website also collects a bunch of data, TOS pretty much makes you a slave, etc. But I don't want to spend more time on this shitty search engine than absolutely necessary. Needless to say, it's not at all private and in fact, it's probably better to use Bing directly since FindX sends everything there anyway while also running their own spy operation (not to mention CodeFuel and their partners also laying their dirty hands on your data). This is probably **the most dishonest search engine** out there, rivaling VFEmail and Hushmail in their shamelessness.

UPDATE September 2022: wow, FindX even manages to only give a **few** results (does not go beyond page 1), and it seems they are all censored (no conspiracy results). Truly the worst search engine in the world.

Ⓢ Stract Ⓢ

Was really excited for this one as it promised customizability (archive) (MozArchive) (*"Immensely customizable -- We aim to give you the ability to customize everything about the search. You can block sites, boost sites, prioritize links from specific sites and much, much more"*), and I was getting tired of common "indexes" chaining me. Well I finally got "inspired" to test it out and I'm not impressed. In theory, you should be able to (archive) (MozArchive) basically make your own "index". The criteria seem quite limited though; for example, date of

creation / update is not one of them. There is also little documentation on how to write optics. But the worst issue is that the optics **don't even fucking work!** I made a few and uploaded them both to my server and 0x0; a friend also confirmed with kallist. Stract says that the preferred host for optics is *raw.githubusercontent.com*, but that “*you are free to host them elsewhere*” - yet that doesn't seem to work in practice. The optics are lifted, but when searched through, do not display anything. Therefore the biggest reason for using Stract has evaporated.

It's still possible that adding a custom optic to GitHub would make it work, but we were trying to avoid big tech, isn't that right? I actually registered for GitHub just to test it, having had to enable a bunch of domains in eMatrix and solve its captcha of nightmares (OctoCaptcha - significantly worse than recaptcha). Some domains also appear only when you have already solved the captcha, failing the solution and necessitating another try. All for what? So that I could graciously add a text file and have an "optic" actually work? Amazing. But even that had a hiccup because the pasting process (on GitHub) actually crashed my browser the first time.

Even after I was finished, it took me a while to figure out that the optic actually works because apparently, it doesn't when you use it the first time and it also requires enabling a third party domain in eMatrix. Oh, and even if you have already added an optic, you can't search through it without that third party request, meaning GitHub AKA Microsoft spies on you every time you search. Why even the need to **add** an optic when it's getting lifted from its source site every time? Or to state this issue in another way, why put it in the URL if it's already downloaded? Why even need an external service for the optic instead of a local file? You even need to enable JS for it (archive) (MozArchive), as well as for other things - “*Javascript is however needed to provide functionality like changing your settings, liking/disliking sites, managing optics, easily remove a single site in 'explore' etc*”. Even changing your settings? Have they not heard about forms and cookies?

In terms of privacy, collecting *“Usage Statistics”* is enabled by default, but can be turned off. Those include:

- *The text used to perform the search.*
- *The list of urls returned for the search.*
- *Whether or not any of the results were clicked and if so, which one.*
- *An id that is autogenerated and unique for each new search.*
- *A timestamp rounded down to the nearest hour.*

Strat also has search suggestions enabled which give "interesting" results such as:

alex jones 

search

alex jones

alex jones'

alex jones' big black cock

alex jones' huge black cock

alex jones' massive black cock

alex jones' significant black cock

These can't be turned off, either - even by enabling "Safe Search" in the settings, which doesn't seem to affect the suggestions. TOR appears to be supported, but I only did one search through it. No image search or anything other than a regular website one. Languages available include *“Denmark”*, *“France”*, *“Germany”*, *“Spain”* and *“US”*. The speed of displaying results is unbearable if you're used to any other search engine. Disgustingly, Stract eventually intends to shove you ads:

In the future we will have, clearly labelled, contextual ads based on your current search query and a subscription option without ads. Just to re-iterate; we will only use your current search to match ads and will never track you across searches.

And at the end they mock you with this:

Oh, and if we ever become evil (maybe by changing our motto) please take our code and start a competitor. The fact that you have this ability will make sure that our values will always be aligned with our users.

You are already evil by depending on Microsoft and even planning to add to our already overflowing ad-spam load. Oh, and you've received money from the EU (archive) (MozArchive) for this project (*“We've been very fortunate to receive an incredible grant from NLnet with financial support from the European Commission's Next Generation Internet program which currently funds our development”*) - money that will surely come with strings attached. Having source code available doesn't necessarily mean anything - see Firefox, Audacity, and countless other examples where the values are decidedly not aligned with those of their users. And the original project almost always stays as the only one known and used, while the forks just die or don't change enough. It's also possible to hide bullshit in the code and has happened many times as well. This is basically gaslighting.

Stract is a good idea, really...finally attempting to put the way searching works into the users' hands, and make it relatively easy. There's simply too much bullshit involved in the execution here. Mostly that it absolutely requires cucking to Microsoft. You can still search without but then it's just a regular engine that has nothing over any of the others, really. Then, the cock suggestions show lack of care - it's pretty much beta software. Add the overdependence on JS,

EU funding and future ads and... Like with the Dissenter situation, I'm hoping someone takes the good aspects of it but throws away the baggage.

Marginalia

This search engine is absolutely awesome. It has found me so many interesting sites that are completely missing from the mainstream search engines. Of course, it's completely useless for technical questions and stuff like that; I tried to use it this way for a while but it just doesn't work. Yet, we have Google and Bing for those things already, right? As the creator says: *“It’s perhaps not the greatest at finding what you already knew was there. Instead it is designed to help you find some things you didn’t even know you were looking for”*. And at this task it performs admirably. The index appears to be a lot bigger than Wiby's, while still keeping most mainstream trash away because of *“heuristics to prefer text-heavy websites”* and *“an upper limit on heavy modern web design inventions”*. It is a breath of fresh air for someone that's mostly been chained to the big engines (and their proxies) for all these years. Unfortunately, Marginalia's *“heuristics”* don't get rid of Wikipedia, StackOverflow, and other stuff I'm tired of seeing. Fortunately, there **are** options to kick those out - such as using either of the filters *“Small Web”* or *“Blogosphere”* (the *“Forums”* filter might be interesting too in an age where all the commotion is on Discord or Facebook groups). When I go back to a "regular" search engine, it just hurts my eyes to see all the nytimes and snopes crap; I wonder how I was able to endure it all those years. Another thing I'm surprised to have endured are the **absolutely terrible visual designs of all modern search engines** - and Marginalia resists this disease, too. Look:

Search The Internet

metallurgy

Search

<https://knifesteelnerds.com/2020/03/30/m390-vs-20cv-vs-204p-3rd-generation-powder-metallurgy-technology/>

M390 vs 20CV vs 204P - 3rd Generation Powder Metallurgy Technology? - Knife Steel Nerds

Edge retention testing is continuing, we have now tested 18 different steels, and four of those steels with multiple heat treatments. Come to Patreon if you want updates on testing as it is completed.

Also from knifesteelnerds.com

[New Micrographs of 42 Knife Steels - Knife Steel Nerds](#)

[AR-RPM9 Knife Steel is False Advertising - Knife Steel Nerds](#)

[USA vs Europe - Powder Metallurgy Knife Steels - Knife Steel Nerds](#)

[S30V Steel - History and Properties - Knife Steel Nerds](#)

[Info](#) [81+](#)

Js Co Tr Ad



Filters

[Remove Javascript](#)

[Reduce Adtech](#)

[Recent Results](#)

[Search In Title](#)

Domains

[No Filter](#)

[Small Web](#)

[Blogosphere](#)

[Academia](#)

[Vintage](#)

<http://www.thehistoryblog.com/archives/date/2017/10/07>

October 7, 2017 – The History Blog

Unlike Ötzi's blade, which was complete with its yew haft and the leather strips binding the two parts together, the Riedmatt axe is the blade alone. Also unlike Ötzi's, the Riedmatt blade is almost pristine, excepting a single notch and

It actually uses colors and margins to separate entries, while all the other search engines just throw the entire mess right onto the background. In Marginalia, half the horizontal space of the screen also isn't taken up by a Wikipedia entry (ugh) or just empty space (like in searx, 4get, mojeek, DDG...). It just looks and functions great; it is obvious someone with a good eye for design created it. You are even told which websites contain ads, cookies, or scripts, and can also deny those that do have JS or ads. Though this is not that useful for uMatrix chads, it's still nice to see someone even caring to divide websites by these criteria. I'd like to see Cloudflare as another criteria in there, while we're at it.

About privacy, it's almost as private as it can be ([archive](#)) ([MozArchive](#)). Access logs are only kept for 24h, and *“After this window is passed, all logs that may contain user queries are shredded”*. Also *“No information about which links are clicked is gathered, and it is not possible to historically correlate IP address to search terms”*. So are there any flaws? Again, it doesn't find "normal" things well at all - which is also its advantage and of course we have all the others that do this. Sometimes the results don't have a lot to do with the exact query, so treat this engine as an exploratory device, and not necessarily an informational one. I don't know the creator's exact stance on censorship; he does say on his about page that *“if you do find something genuinely in bad taste”*, you should report it. But what's the criteria, I don't know. I seem to be finding all kinds of "inappropriate" stuff that would surely be banned on mainstream search engines; I suspect it's mostly about porn and violence. There are also no image results or anything other than just sites - but again, we can use other things for those. For once, it's nice to have something that does one thing and one thing well. In the end, Marginalia is one of the best software projects I've seen recently, after it dropped Cloudflare. **Edit:** has a worse default design now, but the old one can still be [found here](#).

You

No idea what this is, except that it is Cloudflared, and therefore useless.

WebCrawler

Same as above.

Search my Site

Same as above.

MillionShort

Same as above.

Spyda

Same as above.

Excite

Same as above.

4Conservative

Same as above.

GoodGopher

A search engine that rejects mainstream sites. Could be cool, but is unfortunately Cloudflared.

Summary

So, the first edition of this summary was overly positive. I was eager to finally share some good news after the stuff on Mozilla, Proton, and others dirtied the privacy climate. However, I **severely overestimated the situation** and way overrated several search engines such as StartPage, MetaGer and DuckDuckGo. The main issue is that **all of them lack their own index**, meaning they are **fully dependent on the violators**. The ones who do use their own index have weak results. This already proves that the situation is worse than with browsers (which has the independent Pale Moon as well as various other smaller, less viable projects) or E-mail. Not only is there **no provider approaching the quality of RiseUp mail** - but even the second-tier of E-mail providers (such as Posteo or Dismail) outclass the best search engines. The field is also rife with frauds, similar to E-mail. What's a poor user to do, then? It would be best to pull the plug and deal with the inconvenience of terrible results, though of course it's hard to actually do that. However, the situation won't improve until we support the independent search engines. So, **use Mojeek and Wiby** to accomplish that. If you're not prepared to ditch the violators, a **good SearX instance is your best bet**. I recommend weaning yourself off Google since they're so

heavily censored, therefore StartPage is out. The wounded privacy warrior marches on, scraping by until a decent provider finally comes along...

Engine / Feature	Requires JavaScript	Own index	Supports TOR	Has onion domain	IP storage	Search results	Censorship	Shares data with third parties
Swisscows	Yes	No	No	No	No	Good	Mild	Yes
Brave Search	For images	Doubtful	Sometimes	Yes	No	Average	Extreme	No
SearX	No	No	Yes	Conditional	Conditional	Good	None	No
StartPage	No	No	No	No	No	Good	Extreme	No
Wiby	No	Yes	Yes	No	Yes	Bad	None	No
DuckDuckGo	No	Partial	Yes	Yes	Yes	Good	Mild	No
Qwant	No	Partial	Yes	No	Yes	Good	Mild	Yes
Metager	No	No	Yes	Yes	Yes	Good	None	No
Mojeek	No	Yes	Yes	No	No	Average	None	No
Ecosia	For images	No	No (CF)	No	Yes	Good	None	Yes
Oscobo	For images	No	Yes	No	Unknown	Good	Mild	Yes
Discrete								

Search	Yes	No	Yes	No	Yes	Good	None	Yes
Gibiru	Yes	No	No	No	No	Good	Extreme	Yes
Gigablast	Yes	Yes	Yes	No	Yes	Average	None	No
Peekier	Yes	Partial	No (CF)	No	Yes	Good	None	Yes
Presearch	Yes	No	Yes	No	Yes	Good	Extreme	Yes
Right Dao	No	Yes	Yes	No	Possible	Bad	Who knows	No
4get	No	No	Yes	Yes	No	Good	None	No
FindX	No	No	Yes	No	Possible	Bad	Extreme	Yes
Marginalia	No	Yes	Yes	No	Yes	Average	Little / who knows	No
You	Cloudflare so who cares lol							
WebCrawler								
Search my Site								
MillionShort								
Spyda								
Excite								
4Conservative								
GoodGopher								

Explanation of issues:

- *Requires JS* - whether the search functionality works without JS or not.
- *Own index* - Green for only using its own web crawler to display the results, Yellow for own crawler in addition to a violator's index (Bing, Google, Yahoo...); Red for only violator's index
- *Supports TOR* - Didn't spend too much effort testing this. If it throws stupid errors while on TOR, it gets the bad rating. If it doesn't - good rating. Obviously, having an onion domain makes you automatically green in this category.
- *Has onion domain* - self-explanatory. SearX is “*Conditional*” because only a few instances have that.
- *IP storage* - this concerns only whether the service themselves stores your IP address (according to their privacy policy) - not whether some third party gets it. Concerning SearX, the instance's privacy policy decides whether they store IPs or not - that is why it's “*Conditional*”. Also remember to contrast this category with “*Supports TOR*” - if a service is red in both, it's really bad.
- *Search results* - this concerns only the amount of returned results. As in, how easily you can find technical answers, etc.
- *Censorship* - **NEW CATEGORY**. Whether the search engine censors its results. I usually check this with queries like "moon landing was fake" and "COVID vaccines kill". In theory, there should be a mix of sites with relevant keywords on the first page. If I find that conspiracy theory sites (or any non-mainstream ones) are being unfairly buried, I give the engine a Mild censorship grade. If they are not there at all - and I'm being swarmed by fact-checking sites even though they are not the best fits for my query - I will give the engine an Extreme(ly shitty) grade. I don't have exact data for all,

some are partially assumed. SearX gets “*None*” because it doesn't censor by itself and you can choose the non-censorious engines in it. But if you rely on the censorious ones, of course SearX then inherits the grade of those.

- *Shares data with third party* - Embedding stuff from other domains qualifies (if it's required to use the search functionality). Also, if the service admits to sharing the data with the search engine they are proxying (for example, Ecosia giving IP to Bing) - that goes here as well.

You might be wondering as to why I didn't review the Cloudflared engines properly. That is because using Cloudflare is such a big flaw that the other qualities of the search engine don't even matter. Cloudflare is a third party that MitMs your connection and steals your search query and all other sent data, blocks TOR, and is also able to rewrite the served page without you knowing. I can't see anything possibly worse than that.

UPDATE July 2024: I've been questioning the way these criteria are set up recently, I don't find them too descriptive. IP storage is treated as one thing, when it might be for one day or forever. Query storage is missed completely. Censorship has many meanings and might refer to censorship of alternative theories, porn, violence, or just JS-heavy sites. So, the table remains to be improved but for now, I hope it can still provide some useful information

Lyrics search engines

Was looking for the lyrics to a certain song and thought I might as well rate all the engines I find. These won't be in-depth reviews; if my (now low) annoyance threshold is passed I trash the engine and move on to the next one. Most engines were found on the first two / three pages

of a mojeek / DDG search from the query "lyrics search engine", and a few from some websites listing "best lyrics search engines". Anyway let's go:

- <https://www.seekalyric.com/> - results with error *“MySQL Error: 3024 (Query execution was interrupted, maximum statement execution time exceeded) Session halted”*.
- <https://search.azlyrics.com/> - doesn't appear to search without JS, though it pretends to be loading something. Works with JS enabled, but adding *“a keyword for this search”* in Pale Moon doesn't do anything since the searching appears to need a token generated by the website. Using TOR throws a captcha that after solving wants you to wait for like 2 minutes. Database seems small.
- <https://www.allthelyrics.com/> - no search functionality that I can find.
- <https://xiryl.com/> - CF.
- <https://www.aimsapi.com/lyrics-search> - uses AI; appears to need to *“book a demo”* to do anything; the form for it doesn't seem to load in Pale Moon at least.
- <https://www.chosic.com/find-song-by-lyrics/> - CF.
- <https://songfinderbylyrics.com/> - white page without JS; seems to be just a proxy for google, as it needs their JS enabled to actually search.
- <https://www.mldb.org/> - somewhat broken CSS (in Pale Moon at least), though you can partially skip it with the option to *“Add a keyword for this search”*. Many criteria to search by and **all are usable through the search bar**. I like it overall but it did not find my song.
- <https://lyricradar.com/> - CF.
- <https://findmusicbylyrics.com/> - loads so no CF, but extremely slow to search and I can't be bothered to wait and see if it graciously works after 10 minutes. Edit: figured

out it just doesn't like my VPN for some reason. Tried through TOR and it loaded quickly but then slammed me with the message of death: *“Find Music By Lyrics uses Google's search technology to bring you more relevant results from top quality sites using lyrics from songs”*. Hahaha.

- <https://www.musicgateway.com/song-lyrics> - loads without JS, but doesn't search even **with** it (allowed first party only; can't be bothered to play the umatrix game).
- <http://www.lyricsbadger.co.uk/> - cert invalid for domain so http is the only option; it doesn't even matter though because searching 404s with *“Sorry, this is the void”*.
- <https://www.tune-flix.com/lyrics-search-find-song-by-lyrics/> - CF.
- <http://www.lyricsbook.net/> - cert invalid for domain, and expired to boot. Very nice, simple website design. But so what if searching results in error *“Errore nella selezione del database”* (yes even with JS)?
- <https://www.lyricsforall.com/> - cert expired.
- <https://www.letssingit.com/> - no search functionality.
- <https://genius.com/> - CF.
- <https://searchthatsong.com/> - CF.
- <https://www.elyrics.net/> - CF.
- <https://www.shazam.com/> - doesn't seem to be a traditional search engine.
- <https://www.musixmatch.com/search> - needs three JS / XHR domains allowed in umatrix to do anything, but actually finds stuff at least. Does not block TOR either. Feels resource demanding.
- <https://lyricstranslate.com/en/songs> - just as I was about to give up I found this gem. Works without JS; has functional and good looking CSS. Can be added to the search bar like mldb; but unlike mldb it actually found my song. Enabling (first-party)

JavaScript allows to sort by things other than relevance (date, etc). Some of the songs also have translations; often in several languages. TOR is allowed. The only "flaw" is pro-Zelensky propaganda on the main page. But let's end this review on a high note and pretend that that does not exist. **UPDATE February 2026:** now captured by the CF monster.

- <https://lyricsmode.com> - CF.
- <https://www.lyricsplanet.com/search.php> - decent design, works through TOR without JS, but seemingly very small database compared to lyricstranlate (or even mldb). Can be added to the search bar.
- <https://www.lyricsfind.com/> - not a search engine.
- <https://lyricsondemand.com/> - CF.
- <https://www.lyricsfreak.com/> - looks like a lyrics search engine but actually isn't and searches only for song titles.

TL;DR lyricstranlate is ~~great~~ if you don't care about CF, mldb is okay, the rest suck.

[Back to the front page](#)