Brave, the false sensation of privacy

2021/06/08

Categories: Harmful Software

Brave is a chromium based browser, which comes with a built-in adblocker and with a “rewards” program, that is supposed to make you earn money. But the relevant part today is that Brave is advertised as a “private browser by default”.

Brave has taken the false privacy approach similar to other companies (yes Apple, I’m looking at you), they use “privacy“ for marketing but in reality they provide a hypocritical service that “blocks tracking” but instead tracks you and profits from you.

But Brave is more private than Firefox by default

No, not at all. People who claim this have fallen for Brave’s marketing strategy which consists on telling lies and flawed arguments.

I’ll give you numerous facts and counter-arguments that will prevent yourself from falling for Brave’s lies.

Brave’s built-in adblocker

> Block data-grabbing ads and trackers

One of the biggest Brave’s selling points is their built-in adblocker. But let me tell you a couple of things about Brave’s adblocker:

Their adblocker is just a fork of uBlock Origin, which isn’t necessarily bad. The problem comes when you realise that **it has a hardcoded whitelist**. They’re **whitelisting trackers from Facebook and Twitter**, so they can use scripts in third parties' websites to track you across the web. This was their response:

> Loading a script from an edge-cache does not track a user without third-party cookies or equivalent browser-local storage, which Brave always blocks and always will block. In other words, sending requests and receiving responses without cookies or other means of identifying users does not necessarily create a tracking threat.

This is completely false. They’re blatantly lying to their users. Anyone who knows a bit about how JavaScript works and it’s capacities to track you without the need of using cookies will be laughing after reading that.

Using Facebook’s and Twitter’s scripts is more than enough to track and identify you. Blocking cookies doesn’t help.

I mean, what’s the point on making a “private” browser if Facebook’s scripts (that are everywhere btw) will track you?

Another problem with their built-in adblocker is that it’s better for extensions to be separated from the core of the browser, since they don’t follow each other’s update cycles. **This means that you need to update the entire browser to fix a bug in the adblocker. Stupid, isn’t it?**

Another reason to avoid using Brave is that **uBlock Origin works best on Firefox and there isn’t anything that Brave can do about it**.

The limitations are Chromium's fault and Google isn't going to do anything about it. Brave is dependent on Google and they'll always be limited by this fact. Since they're based on Google's browser and web engine, Google takes development decisions over the 95% of Brave. It's important to bring focus to the fact that **Brave isn't more than Chromium with another skin and a built-in adblocker with reduced functionality**.

Other side effect of using a browser which is made by Google is that **Google will take decisions that benefit their advertisement business**, like **making impossible to use adblockers on any Chromium based browser**. And of course, this will affect Brave.

However, of course that **they won't tell you anything of this on their homepage**. Part of their marketing strategy consists on making their "privacy shield" look like the best and unrivaled adblocker in the world, when it is just a really limited uBlock Origin, with a hardcoded whitelist.

Brave Rewards

Rewards is their shitty program that will replace ads displayed on websites with their own. They claim that you can earn money with it. Well, they aren't lying to you on this. If earning half a penny in a month is okay for you, in exchange of your privacy, because of course, they're tracking you with Rewards, then enjoy your money. But remember, Brave's fee is 30% of your earnings.

If you don’t mind that and you decide to use Rewards, it’s important to say that Rewards uses Uphold, which has an excellent policy /s:

> To verify your identity, we collect your name, address, phone, email, and other similar information. We may also require you to provide additional Personal Data for verification purposes, including your date of birth, taxpayer or government identification number, or a copy of your government-issued identification
>
> Uphold uses Veriff to verify your identity by determining whether a selfie you take matches the photo in your government-issued identification. Veriff’s facial recognition technology collects information from your photos that may include biometric data, and when you provide your selfie, you will be asked to agree that Veriff may process biometric data and other data (including special categories of data) from the photos you submit and share it with Uphold. Automated processes may be used to make a verification decision.

Contrary to popular belief, Rewards isn’t opt in. Don’t believe me? Check it yourself. **Brave will recurrently make requests to the following domains, no matter if you use Rewards or not**:

- rewards.brave.com
- api.rewards.brave.com
- grant.rewards.brave.com

The names can be a bit confusing but these domains aren't just for updates and **they fetch affiliates for Brave Rewards, with pings such as Grammarly, Softonic, Uphold**, etc.

So **despite explicitly opting out, Brave's Rewards will still be used to track you**.

Brave sends requests to numerous domains

They also make requests to various domains that are believed to be related to the crypto aspect of Rewards. I won't elaborate here since it's better explained on **this article**. Here you have a list with the different domains that Brave sends a request to:

- variations.brave.com
- laptop-updates.brave.com
- static1.brave.com
- brave-core-ext.s3.brave.com

There isn’t a way to opt out from sending this requests.

It is also worth mentioning that **Brave has built-in telemetry**. **Brave will make a ton of requests to the domain p3a.brave.com as telemetry**. This telemetry can be opted out, but a lot of people believe in their marketing and think that Brave is private out of the box.

Suspicious behavior which installs 5 extensions

brave-core-ext.s3.brave.com fetches 5 extensions and installs them. It is said that this might be a backdoor. But I don’t want to get conspiracist. I prefer giving you verifiable facts. I’ll limit myself to inform you about suspicious activities.

Brave Today

There is a ton of criticism about Firefox’s Pocket. But Brave has something similar, which is called Brave Today.

It is displayed in every blank tab. This feature sends lots of requests to Brave’s servers. **It can’t be disabled**.

So your only option would be setting the tabs to blank, but you’ll still have this shady crap enabled. At least on Firefox you can easily disable Pocket.

Brave’s “SafeBrowsing”

This features is intended to “protect” the user from “unsafe” websites and extensions. However, it seems to have a contrary effect, since **it sends requests to fetch the information required** And it wouldn’t be too far-fetched of Brave **to use Google’s SafeBrowsing**. I’ll elaborate on the next section.

Brave makes requests to Google’s Gstatic

Brave makes requests to static1.brave.com. If you put this on a browser you’ll find that it was directed to Google’s error 404 page.

Isn’t it weird that one of Brave’s domains redirects to a Google’s page? Well, curl –head static1.brave.com shows that **Brave uses Google’s gstatic, which is btw using Cloudflare**.

It’s a concerning issue for a “privacy” oriented browser to connect to Cloudflare’s and Google’s domains, since both of them are telemetry.

But Chromium is more secure than Firefox

Well, you have to understand that security and privacy are different things. Anyway, It is true that Chromium has process isolation. However, Firefox is almost there too. It’s known as the Project Fission. You can already enable it on the about:config with fission.autostart (on nightly). Take into account that it’s still under development.

Process isolation is the only advantage in security that chromium has over Firefox right now and it will not help you with privacy. You may even want to enable Fission if you feel like process isolation is a must have.

Auto-updates

Brave will check for updates every time you run it. **You can’t turn it off, which implies that Brave’ll make this request every time you launch the browser**. Brave’s dedication to privacy is truly amazing /s.

Brave shady practices

Okay, we’ve seen how Brave is everything but private. But I’d still like to list you some of the shady practices they’ve been caught doing in the past, just in case there is someone who still thinks that using Brave is a good idea.

Brave has been caught inserting affiliate codes

In June 2020, a twitter user (@cryptonator1337) discovered that **Brave was automatically injecting referral codes into URLs** for cryptocurrency exchange sites.

So if you typed “binance.us” into the URL bar and pressed enter, Brave would take you to “binance.us/?ref=35089877”.

There was a huge scandal when this was noted. Later, Brave disabled this in the code, in a “sorry we got caught” style.

Uphold

I’ve already shown you how Uphold is everything but privacy respecting. **It wouldn’t make any sense for a “privacy friendly” browser to use such a service, unless they didn’t give a fuck about privacy** and everything was just a marketing strategy…

Incompetence when implementing “privacy features”

Who the fuck implements Tor but doesn’t change the DNS? I mean, this is either total incompetence or, even worse, malevolence on the part of Brave’s team.

Anyway, you can read more about this **here**

Possible scam and theft?

Brave have been accused of **scamming people**. They’ve been promoting this on their home screen, since they get up to $200 per user that uses their affiliate link. I consider this a scam since they’re making a ton of profit from people who will lose their money. **They removed the Reddit post exposing this and the issue on Github**.

They were also accused of theft with BAT but this isn’t verifiable so I’ll only link the **source** for you.

Hostility towards forks

You may have seen in the past a fork of Brave which removed telemetry and other shady practices from Brave. It was called Braver.

Well, that project was given countless lawsuits by Brave, they were forced to rename the project and finally they had to give up out of fear.

So, after all, it seems that **being free software**, or as they prefer to call it, “open source”, **is just another marketing strategy**.

They don’t care at all about software freedom and when someone forks their browser and make one that doesn’t spy on their users, they will harass them until the fork dies, since people using forks aren’t profitable. They want you to use Brave so they can sell your data, force you to use affiliate links and take a 30% cut of your “rewards”.

Chromium and Google’s monopoly

I think that at this point it’s clear that Brave doesn’t care about users' privacy, they only care about making money. But there is something that I haven’t talked about. It’s the fact that Brave is supporting Google's web monopoly.

Why? How? Well, the answer is pretty simple: Brave is just another Chromium skin. So at the end, when using Brave or any other Chromium based browser, you're giving marketshare to Google and supporting their evil web empire.

The only browser that does not use Google's web engine (blink) **is Firefox**. So if you really want some kind of privacy I'd recommend you switching to Firefox or something Firefox based, like GNU Icecat, since a Google's monopoly on the browsers market can't be good for anyone, even if you love Chromium, it is known that monopolies are extremely negative.

And as I mentioned before, **this is already happening with Google trying to destroy adblockers. What will be next?** Forcing every Chromium browser to use FLOC? Making it impossible to disable JavaScript? We don't know it yet, but depending on the biggest data miner and advertisement company (Google) development decisions doesn't seem a great idea if you want to have some kind of privacy.

Conclusion

You shouldn't trust Brave at all. The smart move would be switching to **hardened Firefox**, GNU Icecat, Palemoon or the Tor browser.

If you have any counter-argument, any other info that I could add to the blog post or anything to say about it, you can reach me on the fediverse.

>> Home