“Quite Misleading”: DuckDuckGo CEO Responds To Microsoft Tracker Controversy

Description

Update: DuckDuckGo CEO Gabriel Weinberg took to Twitter on Saturday, calling our headline “**quite misleading**” since “this isn’t about our search engine and we actually restrict Microsoft scripts in our browsers, including blocking their 3rd party cookies.”

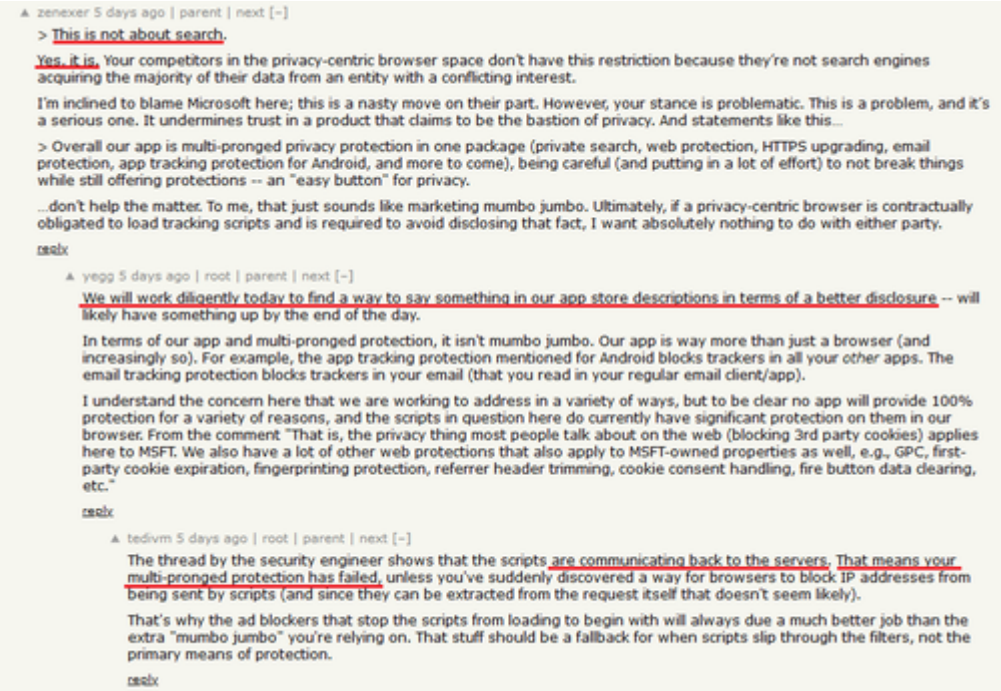
> FYI — this is a quite misleading headline since this isn’t about our search engine and we actually restrict Microsoft scripts in our browsers, including blocking their 3rd party cookies. For full context, I left detailed explanation on reddit:https://t.co/AfDSKceldw
>
> — Gabriel Weinberg (@yegg) May 29, 2022

Weinberg links to a *Reddit* thread he created on Wednesday when the tracking controversy broke. In it, he explains: “**this article is not about our search engine, but about our browsers**,” adding that “When most other browsers on the market talk about tracking protection they are usually referring to 3rd-party cookie protection and fingerprinting protection, and **our browsers impose these same restrictions on all third-party tracking scripts, including those from Microsoft**.”

And while Redditors appeared sympathetic in the replies, users in the more technically oriented YCombinator Hacker News forum **weren’t buying it.**

The top response refutes Weinberg’s claim that “this is not about search,” explaining; “Your competitors in the privacy-centric browser space don’t have this restriction **because they’re not search engines acquiring the majority of their data from an entity with a conflicting interest**.”

Another user replied: “**The thread by the security engineer shows that the scripts are communicating back to the servers. That means your multi-pronged protection has failed** , unless you’ve suddenly discovered a way for browsers to block IP addresses from being sent by scripts (and since they can be extracted from the request itself that doesn’t seem likely).”


zenexer 5 days ago | parent | next [–]

> This is not about search.

Yes, it is. Your competitors in the privacy-centric browser space don't have this restriction because they're not search engines acquiring the majority of their data from an entity with a conflicting interest.

I'm inclined to blame Microsoft here; this is a nasty move on their part. However, your stance is problematic. This is a problem, and it's a serious one. It undermines trust in a product that claims to be the bastion of privacy. And statements like this...

> Overall our app is multi-pronged privacy protection in one package (private search, web protection, HTTPS upgrading, email protection, app tracking protection for Android, and more to come), being careful (and putting in a lot of effort) to not break things while still offering protections -- an "easy button" for privacy.

...don't help the matter. To me, that just sounds like marketing mumbo jumbo. Ultimately, if a privacy-centric browser is contractually obligated to load tracking scripts and is required to avoid disclosing that fact, I want absolutely nothing to do with either party.

reply

yegg 5 days ago | root | parent | next [–]

We will work diligently today to find a way to say something in our app store descriptions in terms of a better disclosure -- will likely have something up by the end of the day.

In terms of our app and multi-pronged protection, it isn't mumbo jumbo. Our app is way more than just a browser (and increasingly so). For example, the app tracking protection mentioned for Android blocks trackers in all your other apps. The email tracking protection blocks trackers in your email (that you read in your regular email client/app).

I understand the concern here that we are working to address in a variety of ways, but to be clear no app will provide 100% protection for a variety of reasons, and the scripts in question here do currently have significant protection on them in our browser. From the comment "That is, the privacy thing most people talk about on the web (blocking 3rd party cookies) applies here to MSFT. We also have a lot of other web protections that also apply to MSFT-owned properties as well, e.g., GPC, first-party cookie expiration, fingerprinting protection, referrer header trimming, cookie consent handling, fire button data clearing, etc."

reply

tedivm 5 days ago | root | parent | next [–]

The thread by the security engineer shows that the scripts are communicating back to the servers. That means your multi-pronged protection has failed, unless you've suddenly discovered a way for browsers to block IP addresses from being sent by scripts (and since they can be extracted from the request itself that doesn't seem likely).

That's why the ad blockers that stop the scripts from loading to begin with will always due a much better job than the extra "mumbo jumbo" you're relying on. That stuff should be a fallback for when scripts slip through the filters, not the primary means of protection.

reply

The criticism continued further into the thread.

"**"multi-pronged privacy", "easy button", "capabilities", and repeated use of the word "protection" are all signals that what is being said is an attempt to sell me something and that the salesman should be doubted,**" wrote user *Colechristensen*. "What's actually happening is you're forced to allow Microsoft scripts which do indeed do telemetry on users despite some restrictions you put on them, and they're still effective because fingerprinting works. That fact is embarrassing for a product you're trying to sell as promoting privacy so there's this mildly deceptive attempt to hide what's going on with lots of words and claims of protection instead of straightforward disclosure."

Another user slammed DuckDuckGo's relationship with Microsoft Advertising, in which DDG admits: "If you click on a Microsoft-provided ad, you will be redirected to the advertiser's landing page through Microsoft Advertising's platform. At that point, Microsoft Advertising will use your full IP address and user-agent string so that it can properly process the ad click and charge the advertiser."

Weinberg (username: Yegg) responded, arguing that they "got Microsoft to contractually agree and publicly commit (on this page) that "Microsoft Advertising does not associate your ad-click behavior with a user profile. **It also does not store or share that information other than for accounting purposes.**"

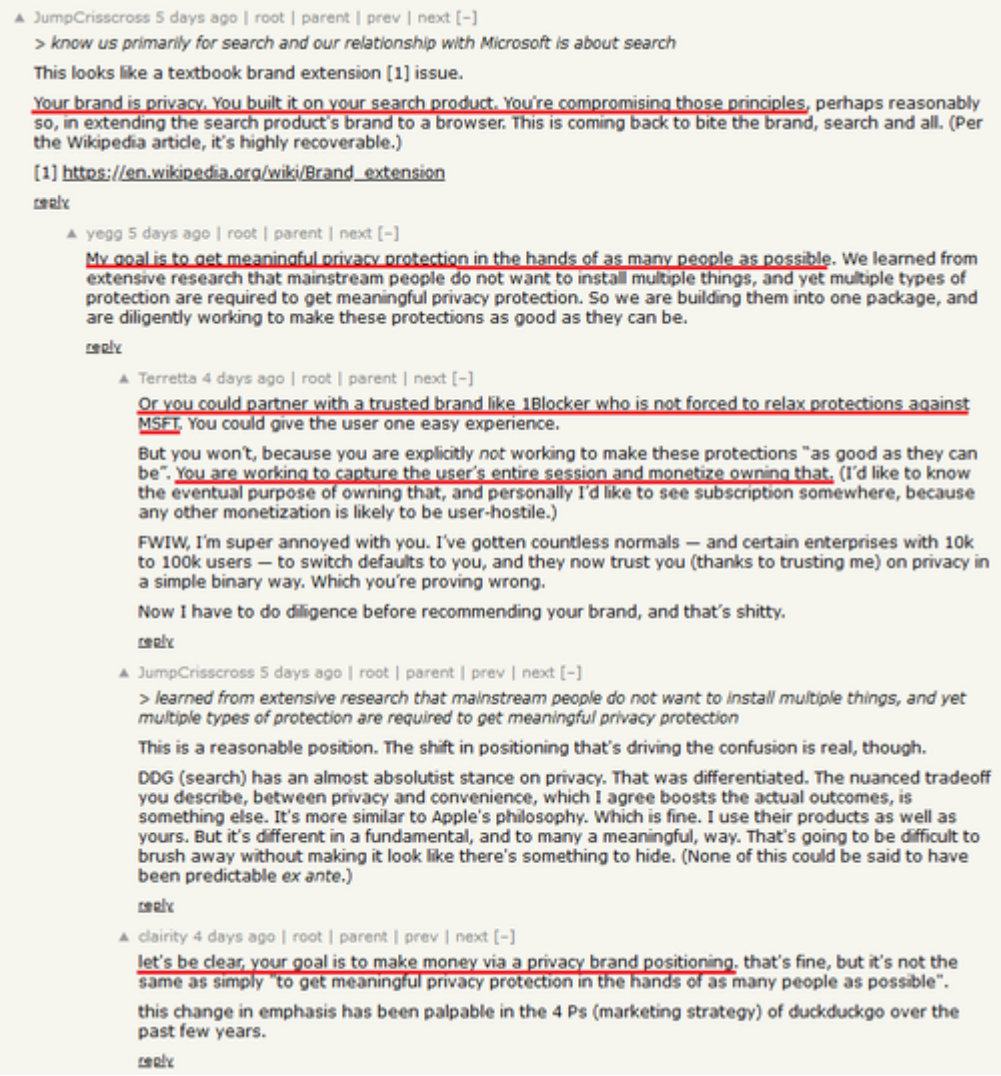
To which user *Tedivm*replied:

> ***So instead of an actual set of real protections, like offered by things such as UBlock, you want us to rely on Microsoft being ethical.***

> *It also ignores that governments like the NSA have tapped these very networks for data (this is what prompted Google's internal SSL drive). Even if we trust the legal entity, the fact is that the information itself is a target and so are those entities. It is always safer not to send the data, but in this case you're explicitly sacrificing that safety to benefit your ad partners.*

When asked what an appropriate headline should be for the controversy, "Yegg" replied: "**Microsoft contractually prevents DuckDuckGo's browser from stopping Microsoft scripts from loading on 3rd party sites (FYI: not search related)**"

It seems like DuckDuckGo may have some more convincing to do.



▲ JumpCrisscross 5 days ago | root | parent | prev | next [–]

> know us primarily for search and our relationship with Microsoft is about search

This looks like a textbook brand extension [1] issue.

Your brand is privacy. You built it on your search product. You're compromising those principles, perhaps reasonably so, in extending the search product's brand to a browser. This is coming back to bite the brand, search and all. (Per the Wikipedia article, it's highly recoverable.)

[1] https://en.wikipedia.org/wiki/Brand_extension

reply

▲ yegg 5 days ago | root | parent | next [–]

My goal is to get meaningful privacy protection in the hands of as many people as possible. We learned from extensive research that mainstream people do not want to install multiple things, and yet multiple types of protection are required to get meaningful privacy protection. So we are building them into one package, and are diligently working to make these protections as good as they can be.

reply

▲ Terretta 4 days ago | root | parent | next [–]

Or you could partner with a trusted brand like 1Blocker who is not forced to relax protections against MSFT. You could give the user one easy experience.

But you won't, because you are explicitly *not* working to make these protections "as good as they can be". You are working to capture the user's entire session and monetize owning that. (I'd like to know the eventual purpose of owning that, and personally I'd like to see subscription somewhere, because any other monetization is likely to be user-hostile.)

FWIW, I'm super annoyed with you. I've gotten countless normals — and certain enterprises with 10k to 100k users — to switch defaults to you, and they now trust you (thanks to trusting me) on privacy in a simple binary way. Which you're proving wrong.

Now I have to do diligence before recommending your brand, and that's shitty.

reply

▲ JumpCrisscross 5 days ago | root | parent | prev | next [–]

> learned from extensive research that mainstream people do not want to install multiple things, and yet multiple types of protection are required to get meaningful privacy protection

This is a reasonable position. The shift in positioning that's driving the confusion is real, though.

DDG (search) has an almost absolutist stance on privacy. That was differentiated. The nuanced tradeoff you describe, between privacy and convenience, which I agree boosts the actual outcomes, is something else. It's more similar to Apple's philosophy. Which is fine. I use their products as well as yours. But it's different in a fundamental, and to many a meaningful, way. That's going to be difficult to brush away without making it look like there's something to hide. (None of this could be said to have been predictable *ex ante*.)

reply

▲ clairity 4 days ago | root | parent | prev | next [–]

let's be clear, your goal is to make money via a privacy brand positioning. that's fine, but it's not the same as simply "to get meaningful privacy protection in the hands of as many people as possible".

this change in emphasis has been palpable in the 4 Ps (marketing strategy) of duckduckgo over the past few years.

reply

Or as *ZeroHedge* reader *koan* put it: ***fuckfuckno***

* * *

DuckDuckGo, the search engine which claims to offer 'real privacy' because it doesn't track searches

or store users' history, has come under fire after a security researcher discovered that **the mobile DuckDuckGo browser app contains a third-party tracker from Microsoft**.

Researcher Zach Edwards found that while Google and Facebook's trackers are blocked, ***trackers related to bing.com and linkedin.com were also being allowed through***.

> You can capture data within the DuckDuckGo so-called private browser on a website like Facebook's https://t.co/u8W44qvsqF and you'll see that DDG does NOT stop data flows to Microsoft's Linkedin domains or their Bing advertising domains.
>
> iOS + Android proof:
> ????????????? pic.twitter.com/u3Q30KIs7e
>
> — ???? ??????? (@thezedwards) May 23, 2022

In response to the revelation, **CEO Gabriel Weinberg essentially shrugged** – telling *BleepingComputer* that the company offers "above-and-beyond protection" that other browsers don't, but that he 'never promised' anonymity when browsing.

"We have always been extremely careful to never promise anonymity when browsing, because that frankly isn't possible given how quickly trackers change how they work to evade protections and the tools we currently offer," he said.

DuckDuckGo CEO Gabriel Weinberg

"When most other browsers on the market talk about tracking protection, they are usually referring to 3rd-party cookie protection and fingerprinting protection, and our browsers for iOS, Android, and our new Mac beta, impose these restrictions on third-party tracking scripts, including those from Microsoft. What we're talking about here is an above-and-beyond protection that most browsers don't even attempt to do — that is, blocking third-party tracking scripts before they load on 3rd party websites," he continued.

"Because we're doing this where we can, **users are still getting significantly more privacy protection with DuckDuckGo than they would using other browsers**."

In short, DuckDuckGo doesn't provide the type of privacy they've earned a reputation for – **they simply betray users the *least*.**

As *TechRadar* notes, this didn't go over well.

> ***The news quickly drew in crowds of dissatisfied users**, with DuckDuckGo founder and CEO Gabriel Weinberg, soon chiming in to confirm the authenticity of the findings.*
>
> *Apparently, DuckDuckGo has a search syndication agreement with the software giant from Redmond, with Weinberg adding that the restrictions are only found in the browser, and are not related to the search engine.*
>
> *What remains unknown is why the company who is known for its transparency decided to keep this agreement a secret for as long as it could. -TechRadar*

See Edwards' entire May 23 Twitter thread below:

> DuckDuckGo has browser extensions & their own browsers for iOS / Android @ https://t.co/2Il4VrBVqc
>
> iOS @ https://t.co/srtR22gtfS
>
> Android @ https://t.co/STtTve3vS7
>
> Both versions of the DDG browser claims to use tools which "automatically blocks hidden third-party trackers" ? pic.twitter.com/amhdT0w3Ru
>
> — ???? ??????? (@thezedwards) May 23, 2022

I don’t have the full list of advertising domains that the DuckDuckGo browser is allowing to collect data within their new “private” browser ((anyone have that or parsed itsomewhere??) but any list that doesn’t include “linkedin[.]com” + “bing[.]com” is*purposefully* broken. pic.twitter.com/xjkcWafZqD

— ???? ??????? (@thezedwards) May 23, 2022

But you won’t find any public articles from DuckDuckGo explaining *why* they are not blocking Microsoft-owned 3rd party data flows on websites *not* owned by Microsoft, like on Facebook’s Workplace[.]com domain sending data to Bing & Linkedin in the DDG “private” browser. ???? pic.twitter.com/ATS4J7aBhE

— ???? ??????? (@thezedwards) May 23, 2022

You can capture data within the DuckDuckGo so-called private browser on a website like Facebook’s https://t.co/u8W44qvsqF and you’ll see that DDG does NOT stop data flows to Microsoft’s Linkedin domains or their Bing advertising domains.

iOS + Android proof:
????????????? pic.twitter.com/u3Q30KIs7e

— ???? ??????? (@thezedwards) May 23, 2022

So another question to ask: if you were a DDG privacy researcher who knew that Microsoft has a variety of domains they use for cross-site tracking to optimize their ads systems, and you already knew that DDG was giving IP address & UA string data to MSFT, did you know this too?? pic.twitter.com/08ryUFY6rH

— ???? ??????? (@thezedwards) May 23, 2022

Personally, I think that both Google & Apple have an obligation to users within their app marketplaces to remove apps which claim to do X, Y, Z, but do the opposite, merely because it makes the parent company more money.

If you say you block 3rd party data flows, *do that* …

— ???? ??????? (@thezedwards) May 23, 2022

I don’t think there is a public list of *all* the domains that the DuckDuckGo browser is *not* blocking, but they seem to be doing this w/ hardcoded rules. The DDG browser stops data

> flows from tons of domains…. except DDG's #1 ad tech partner.
>
> Mysterious! ??????? pic.twitter.com/mdC78ihRfr
>
> — ???? ??????? (@thezedwards) May 23, 2022

> I won't hold my breath that DuckDuckGo will update their own so-called private browser to actually stop data flows to their own ad tech partners, but this is one of those things that makes a privacy auditor … annoyed? bitter? confrontational?
>
> Does Google / Apple care? </?> pic.twitter.com/SB0jrizrVi
>
> — ???? ??????? (@thezedwards) May 23, 2022

by Tyler Durden

Category

1. Freedom-Free speech-Resitance & H-rights
2. Main
3. Science-Tech-AI-Medical & Gen. Research

Date Created
05/30/2022