yegg 8 hours ago | parent | context | favorite | on: DuckDuckGo's Microsoft deal disallows blocking MS ...

This title is very misleading (and really should be changed).

This is not about search. To be clear, when you load our search results, you are completely anonymous, including ads. For ads, we actually worked with Microsoft to make ad clicks privacy protected as well. From our public ads page, "Microsoft Advertising does not associate your ad-click behavior with a user profile." This page is linked to next to every Microsoft ad that is served on our search engine (duckduckgo.com). https://help.duckduckgo.com/company/ads-by-microsoft-on-duck....

In all our browsing apps (iOS/Android/Mac) we also block third-party cookies, including those from Microsoft-owned properties like LinkedIn and Bing. 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.

This is just about non-DuckDuckGo and non-Microsoft sites in our browsers, where our search syndication agreement currently prevents us from stopping Microsoft-owned scripts from loading, though we can still apply our browser's protections post-load (like 3rd party cookie blocking and others mentioned above, and do). We've also been tirelessly working behind the scenes to change this limited restriction. I also understand this is confusing because it is a search syndication contract that is preventing us from doing a non-search thing. That's because our product is a bundle of multiple privacy protections, and this is a distribution requirement imposed on us as part of the search syndication agreement. Our syndication agreement also has broad confidentially provisions and the requirement documents themselves are explicitly marked confidential.

Taking a step back, I know our product is not perfect and will never be. We face many constraints: platform constraints, contractual constraints (like in this case), breakage constraints, and the evolving tracking arms race. Holistically though I believe it is the best thing out there for mainstream users who want simple privacy protection without breaking things, and that is our product vision.

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. And we constantly work to improve its capabilities and will continue to do so, including in this case. For example, we've recently been adding bespoke third-party protections for Google and Facebook, like Google AMP/Topics/FLEDGE protection and Facebook embedded content protection.

reply

zenexer 5 hours ago | 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 4 hours ago | 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 3 hours 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

colechristensen 4 hours ago | root | parent | prev | next [–]

"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.

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.

reply

thrwawy283 4 hours ago | root | parent | next [–]

Still coming to my own conclusion here, but I wouldn't dismiss "easy button" as marketing. We keep hoping for easy buttons and reasonable default settings in things like openssl or pgp. I do like organizations that understand an easy button is the safest default. Is that what we have here?

reply

colechristensen 4 hours ago | root | parent | next [–]

I'm commenting only on the rhetoric, calling it an "easy button" stinks of marketing BS. People desiring simple straightforward tools is a separate subject.

reply

xchip 4 hours ago | root | parent | prev | next [–]

We have a new marketing word: "multi-pronged protection"

reply

FabHK 2 hours ago | root | parent | next [–]

"Defense in depth" strikes me as a legitimate security technique.

https://www.cisa.gov/uscert/bsi/articles/knowledge/principle...

reply

boomboomsubban 5 hours ago | parent | prev | next [–]

>and is required to avoid disclosing that fact,

Isn't this entire story about them disclosing this fact?

reply

zenexer 5 hours ago | root | parent | next [–]

> Isn't this entire story about them disclosing this fact?

It seems to be, but they're claiming the details are confidential. It's rather confusing. I wonder whether Microsoft's intention was to prevent them from disclosing it altogether, or whether they just wanted to avoid the general details of the contract getting out (rather than this particular tidbit of info). I'm inclined to suspect it was the latter--just a general NDA. In any case, I don't like it.

reply

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

No, it is not just a general NDA.

reply

mda 3 hours ago | root | parent | next [–]

One wonders what other juicy nuggets are in this non general NDA.

reply

bozhark 1 hour ago | parent | prev | next [–]

DDG is a search engine to most people, nothing more.

Just because other avenues exist doesn't mean people walk them

reply

stjohnswarts 3 hours ago | parent | prev | next [–]

Do you have any sources you can cite that Microsoft has breached contracts with companies in the past in an effort to get at your ID for advertisers? Otherwise, I would consider this a nothing burger.

reply

Aeolun 3 hours ago | parent | prev | next [–]

> To me, that just sounds like marketing mumbo jumbo.

What's more helpful is to hear in which exact situations their blocking doesn't work.

reply

throwAwayWFH873 4 hours ago | prev | next [–]

I found this passage [0] in the DDG help:

> Ad clicks are managed by Microsoft's ad network.

> Microsoft and DuckDuckGo have partnered [..] 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

It seems DDG is not that privacy focused when it comes to ads.

[0] https://help.duckduckgo.com/duckduckgo-help-pages/company/ad...

reply

yegg 4 hours ago | parent | next [–]

Actually, that's not the case. First, that page is a linked to directly from every Microsoft ad on duckduckgo.com -- it's a public disclosure for transparency. Second, we specifically worked with Microsoft to make our ads privacy protected. When you load them, they are completely anonymous. When you click on them, we 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."

reply

colechristensen 4 hours ago | root | parent | next [–]

I think a legal department could be convinced that "accounting purposes" could adequately cover most all of the business of tracking, optimizing, and attributing ad clicks.

"Microsoft Advertising does not associate your ad-click behavior with a user profile."

Does somebody else besides Microsoft Advertising do it? I'd guess so.

Is there another kind of association besides a "user profile" which has substantially similar concerns for an end user? I'd guess so.

This is all coming off as an attempt to cover up what's really going on with deception. *That might not be the case*, but if it were, this is exactly how I expect a "privacy focused" organization to communicate when they had been corrupted by a compromise to a third party.

reply

Raed667 3 hours ago | root | parent | prev | next [–]

So now I also have to trust Microsoft before clicking on a DDG ad. Based on a pinky promise not to use my IP address + User-Agent + whatever fingerprint they make?

reply

Aeolun 2 hours ago | root | parent | next [–]

Why'd you even click on an ad in the first place if you are worried about that?

reply

freediver 1 hour ago | root | parent | next [–]

They wouldn't, and DDG has a convenient way to disable ads which I am sure many users take advantage of.

Still, millions of users do click those ads, because if nobody did, DDG would not exist. A less tech savvy user, who is probably DDGs main target, came on the promise of privacy and does click those ads and is also being tracked around the web by Microsoft if they use DDG browser (from what I understand).

This is less than ideal from the standpoint of "privacy simplified" promise, but really no other way around it when selling ads is your business model.

reply

tedivm 3 hours ago | root | parent | prev | next [–]

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.

reply

RONROC 1 hour ago | root | parent | prev | next [–]

For those keeping score at home, this is what a "smart" full of shit guy thinks.

reply

ipaddr 2 hours ago | root | parent | prev | next [–]

Accounting purposes?

That brings us back to: What does Microsoft considers accounting purposes?

Fingerprinting the user/browser can be used for valid accounting purposes like identifying the user to prevent ad fraud.

reply

yucky 1 hour ago | parent | prev | next [–]

Brave search (and the Brave browser) are both great. As a longtime DDG user I think this is the final push I need to move on.

reply

jasonlotito 9 minutes ago | root | parent | next [–]

Brave cannot be trusted. They were misrepresenting themselves and their relationships with content creators. As far as I saw it, they were stealing and lying about it. They've inserted referral codes to cryptocurrency websites. That sounds completely anti-privacy and antithetical to anyone wanting a privacy-focused browser. Sorry, but that all just smells untrustworthy.

reply

dang 2 hours ago | prev | next [–]

The submitted title was "DuckDuckGo Paid by Microsoft to not block their trackers". We've changed it now. If anyone wants to suggest a better (i.e. more accurate and neutral) title, we can change it again.

reply

ignoramous 5 hours ago | prev | next [–]

> *Taking a step back, I know our product is not perfect and will never be.*

You may be making it worse. Really need to dial down on click tracking (or, at least respect the *dnt* header).

Ex A: Searching for *Cristiano Ronaldo* (from Chrome Incognito but not Firefox, amusingly) returns this *horrible* href:

```
duckduckgo.com/l/?uddg=https%3A%2F%2Fen.wikipedia.org%2Fwiki%2FCristiano_Ronaldo&rut=4a9ada2347e29c8fce96a95bde34e6343c279202dbc22b4fe61524ab39bf8eff
```

reply

yegg 5 hours ago | parent | next [–]

That does't occur in modern browsers and is actually a privacy feature that prevents your searches from leaking to the sites you click on, generally in very old browsers that need to use our non-JavaScript site (http://duckduckgo.com/html). See https://help.duckduckgo.com/duckduckgo-help-pages/results/rd... for details. From that page:

**

When you click on a link in our results page, your search terms are not sent to the site that you click on, which can be the case on other search engines due to something called HTTP "referers".

On modern browsers we accomplish this by adding a small piece of code to our page called Meta referrer. Some browsers (especially older ones) do not support this standard, however. For those browsers, and also in situations where meta referrer doesn't work, we send the request back to our servers to remove search terms. This redirect goes through r.duckduckgo.com.

You can disable this privacy feature. To do that, go to the settings page, select Privacy, and change the option Redirect to Off.

**

reply

mananaysiempre 1 hour ago | root | parent | next [–]

The "very old" browsers seem to include the very latest version of WebKitGTK-based GNOME Web aka Epiphany. (It does have legitimate conformance problems, admittedly, so I don't know if this is one of them.)

reply

sigzero 1 hour ago | root | parent | next [–]

Then Epiphany needs to fix it.

reply

ignoramous 1 hour ago | root | parent | prev | next [–]

Gotcha.

> *...generally in very old browsers that need to use our non-JavaScript site (http://duckduckgo.com/html).*

I use *duckduckgo.com/html* & *duckduckgo.com/lite* on all my (up-to-date) browsers (Firefox Mobile for Android / Chrome for Debian as two examples); they are "not very old" at all, and I still get ddg-proxied hrefs.

A feature request (if I may): Old browser or not, if the *dnt* header is set, I'd ideally want ddg to *not* proxy/redirect anything at all on my behalf.

reply

digisign 3 hours ago | root | parent | prev | next [–]

Is urlencoding sufficient to hide this? Doesn't appear to be.

reply

Hello71 4 hours ago | root | parent | prev | next [–]

and what is the rut=4a9ada2347e29c8fce96a95bde34e6343c279202dbc22b4fe61524ab39bf8eff for?

reply

yegg 4 hours ago | root | parent | next [–]

It is a random hash (not any kind of user identifier) for security to make sure we don't have an open proxy.

reply

ev1 4 hours ago | root | parent | next [–]

I think the term you want is open redirect

reply

mikub 4 hours ago | root | parent | prev | next [–]

I'm sorry but why do you post an example of an href, saying it's "horrible", when you don't know what it is doing?

reply

ev1 4 hours ago | root | parent | next [–]

Because I can no longer just right click copy or hold/tap to link it to a friend

reply

sitkack 3 hours ago | prev | next [–]

When the answer is so long, it belies the motivation and privacy guarantees.

A shorter answer would have more credence.

https://youtu.be/nzNL0b4d_WY?t=148

reply

Beltiras 3 hours ago | prev | next [–]

I just changed from DDG to Kagi and will probably pay them once out of Beta. So far I am very happy with the search results and I believe that the next innovation in search is it not being beholden to ads. DDG is not in the place where ads will corrupt your business but should you grow and be successful, you one day will be.

reply

dontbenebby 6 hours ago | prev | next [–]

> This title is very misleading (and really should be changed).

What do you think the title should be yegg?

reply

yegg 6 hours ago | parent | next [–]

It is hard to title because people assume this is about search (when it's not, so that should be in there), and also people assume trackers get a free pass (when they do not, e.g., 3rd party cookies blocked, etc.)

Maybe something like:

Microsoft contractually prevents DuckDuckGo's browser from stopping Microsoft scripts from loading on 3rd party sites (FYI: not search related)

reply

altairprime 4 hours ago | root | parent | next [–]

"Bing search contract prohibits DDG browser from blocking Microsoft tracking scripts by default"?

reply

dontbenebby 4 hours ago | root | parent | next [–]

> "Bing search contract prohibits DDG browser from blocking Microsoft tracking scripts by default"?

Thanks for making a definitive suggestion. I hate when someone knows something is wrong, but can't articulate what would be "right" (correct).

reply

gruez 5 hours ago | root | parent | prev | next [–]

> (FYI: not search related)

I agree with the first part of the title, but this part seems like you're going out of your way to defend yourself. The mention of "DuckDuckGo's browser" should already imply it's not search related.

reply

Jcowell 5 hours ago | root | parent | next [–]

The title off rip makes me think of the search. I didn't even remember they had a browser.

reply

dontbenebby 5 hours ago | root | parent | prev | next [–]

That sounds a bit literal IMHO but I see where you're coming from at least :-)

reply

KoftaBob 6 hours ago | root | parent | prev | next [–]

What's an example of a Microsoft script loading on a 3rd party site, to help wrap my head around this?

reply

yegg 6 hours ago | root | parent | next [–]

The original example was Workplace.com embedding a LinkedIn script.

reply

KoftaBob 6 hours ago | root | parent | next [–]

Ah, I see!

I think for transparency sake, it could be helpful to list the Microsoft trackers that were essentially white listed and therefore allowed to load on a particular site, right under the list of trackers that were blocked.

reply

boomboomsubban 6 hours ago | root | parent | prev | next [–]

When you visit a site, a variety of scripts are downloaded and run. Some from the website you visit, some from their CDN, and some from a variety of third parties that may track what you're doing and/or provide some other functionality. Google and Facebook are the major parties involved in this from my experience, but there are quite a few different ones including Microsoft.

This is what I've gathered from running uMatrix for years.

reply

rhim 6 hours ago | prev | next [–]

Why? The title does not claim to be related to the search, does it?

reply

yegg 6 hours ago | parent | next [–]

People know us primarily for search and our relationship with Microsoft is about search, so it will be assumed by most people this is about search (when it is not, it's about browsers).

Additionally the way it is phrased implies Microsoft trackers get a free pass, when they are in fact heavily restricted, e.g., blocking 3rd party cookies, fingerprint protection, etc.

And the current title can further easily be misinterpreted to be about more than Microsoft scripts on 3rd party sites (e.g., other companies, which it is not).

reply

r3trohack3r 5 hours ago | root | parent | next [–]

FWIW this is exactly what happened to me and I support the title change.

As a long time DDG user, my stomach turned when I saw this. Following the link to Twitter, it required a lot of digging to find what was really happening.

For those of us using DDG search - this is a big nothing burger. For folks using DDG browser, this is misleading at best. The difference between the title and reality, from my understanding, isn't nuance.

My reading of this title (and Twitter) made me believe DDG was sharing user data with MSFT across all of their properties (including search) by serving users MSFT trackers with DDGs content.

reply

chrisweekly 4 hours ago | root | parent | next [–]

Same. 100% agreed w/ proposed title change.

reply

JumpCrisscross 5 hours 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 4 hours 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

JumpCrisscross 3 hours ago | root | parent | 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 2 hours 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

blinding-streak 6 hours ago | prev | next [–]

What is the real, tangible improvement to someone's life with all this claimed privacy protection? IE, when my mom asks why she should switch from Google, what would I tell her that would actually make a difference in her life?

reply

yegg 5 hours ago | parent | next [–]

We have a page specifically about helping people switch: https://duckduckgo.com/spread

To answer your question though, comprehensive privacy protection prevents data profiles from getting created about you, which in turn prevents ad and other content targeting. This targeting, regardless of how it's done, enables general manipulation (e.g., exploiting personal characteristics for commercial or political gain), filter bubbles (e.g., creating echo chambers that can divide people), and discrimination (e.g., people not seeing job opportunities based on personal profiles).

More generally though, I view privacy as protecting you from coercion. Yes, it protects personal information, but that's not the real point. The real point is autonomy -- the freedom to make decisions without coercion. From this perspective in addition to helping reduce identity theft, commercial exploitation, ideological manipulation, discrimination, polarization, etc., it also helps reduce self-surveillance (i.e., chilling effects), and just general loss of freedom (e.g., mass surveillance).

reply

digisign 2 hours ago | root | parent | next [–]

It's a shame that page doesn't address the benefits you mention here eloquently. It basically just says we don't track you, and implies that is good. I do think it is good but it's losing the value prop for most people.

Please put your second paragraph up at the top of that page, maybe with some bullet points and icons and I'll send out the URL.

reply

jeffbee 5 hours ago | root | parent | prev | next [–]

> prevents ad and other content targeting

You want me to pitch my mom on un-targeted advertising? How do you phrase it in practice? "On Google, you get evil ads relevant to you, such as restaurants near you. On Duck Duck Go your privacy is protected, so you get ads for restaurants in Omaha, Nebraska. Therefore you should switch to Duck Duck Go". Something like that?

This comment is based on the actual results I was served by DDG for "best burger".

reply

guelo 4 hours ago | root | parent | next [–]

Your mom will have a better experience and more control if she learns to search for "best burger in <city name>" instead of trying to give the wheel to Google's mind reading AIs.

reply

Invictus0 4 hours ago | root | parent | next [–]

That doesn't sound like a better experience to me.

reply

jeffbee 4 hours ago | root | parent | prev | next [–]

My mom is completely satisfied with Google, so we're discussing some theoretical mom.

I honestly do not understand the pitch, that's why I want to hear it from the horse's mouth. Scare words like "tracking" and "profile" and "targeting" are used by the privacy fear industry to disparage the practice of having implicit terms in your search query. These implicit terms greatly improve search quality, which is why the results on Google are so much better. Advertisements are their own separate search corpus where good ranking is desired and the implicit elements of the search vector are also helpful there. To me there can be no rational case made that omitting the implicit terms improves the quality of the result.

reply

oefrha 3 hours ago | root | parent | next [–]

Same. Tried to sell my mom on some privacy stuff, zero care. Tried to sell her on unique passwords and a password manager, zero care. And so on.

Lots of people (most people?) want to do the bare minimum with computers. Sacrificing convenience for privacy or whatnot isn't something they would accept.

reply

guelo 3 hours ago | root | parent | prev | next [–]

Google's search engine is awful. In case you hadn't noticed rants about it are increasingly popular. Part of the reason is that Google keeps taking away user's control of the tool, partly in the name of convenience but also to manipulate you, get you to click on favored links, show you ads or extend their search monopoly to other products.

I'm not arguing that duckduckgo/bing are any better, just that these tracking convenience features have a dark side and many times work against your best interest.

reply

oefrha 3 hours ago | root | parent | next [–]

> rants about it are increasingly popular.

1. Never heard any rant about it outside tech circles.

2. I've given DDG many chances when Google failed to return satisfactory results. In those many cases DDG results were just about the same or even less relevant. Google changing the query? Well DDG either also changes it or returns irrelevant results not containing the query anyway.

The single advantage of DDG I've noticed is that it doesn't CAPTCHA me on a VPN connection.

reply

dazc 6 hours ago | parent | prev | next [–]

She is far less likely to see an ad for a financial service which turns out to be a scam.

reply

gruez 5 hours ago | root | parent | next [–]

I don't see the connection here. Does duckduckgo/bing have more ethical advertisers? Are ads for "financial service which turns out to be a scam" dependent on tracking?

reply

colinmhayes 4 hours ago | root | parent | next [–]

I think the "financial service which turns out to be a scam" ads target older people, especially women. I certainly don't get those ads.

reply

dazc 5 hours ago | root | parent | prev | next [–]

You can see no ads. In default mode you see far less.

reply

utopcell 2 hours ago | prev | next [–]

At the end of the day, you chose to enter the browser space knowing full well that you cannot back your privacy claims.

reply

bryan_w 6 hours ago | prev | next [–]

You've written a lot of confusing statements so help me understand:

Party #1: Me

Party #2: DDG

>currently prevents us from stopping Microsoft-owned scripts from loading

How is this not allowing 3rd party (Microsoft) tracking? Are they loading the scripts from DDG's servers?

reply

yegg 6 hours ago | parent | next [–]

Sorry, I was trying to be clear not confusing :). But no, this has nothing to do with DuckDuckGo servers or sites, whatsoever. This is about completely 3rd party sites that might embed a Microsoft script. The original example was Workplace.com embedded a LinkedIn.com script.

reply

1vuio0pswjnm7 5 hours ago | prev | next [–]

"... an "easy button" for privacy."

Fool's gold. Privacy is never easy.

reply

pcmaffey 5 hours ago | parent | next [–]

Privacy should be the default, not a button. The only way to achieve that is through regulation.

reply

FridayoLeary 4 hours ago | prev | next [–]

OT but thanks for making DDG. I went out and discovered it on my own because i wasn't satisfied with Google Search (too much SEO results, not enough links to forums). But many thanks and i wish you the best of success.

reply

chrisweekly 5 hours ago | prev [–]

GPC?

reply