

https://panopticklick.eff.org/results?#fingerprintTable

Panopticklick

Search - fingerprinting... New Issue - brave/brow... Panopticklick About Brave

A RESEARCH PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION **DONATE**





PANOPTICCLICK

Is your browser safe against tracking?

How well are you protected against non-consensual Web tracking? After analyzing your browser and add-ons, the answer is ...

Yes! You have **strong protection against Web tracking**, though your software isn't checking for Do Not Track policies.

Help us defend the Web against tracking:

Test	Result
Is your browser blocking tracking ads?	✓ yes
Is your browser blocking invisible trackers?	✓ yes
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✗ no

10:22 PM 12/9/2016

https://panopticklick.eff.org/results?#fingerprintTable

Panopticklick

Search - fingerprinting... New Issue - brave/brow... Panopticklick About Brave

✗ your browser has a unique fingerprint

Does your browser protect from **fingerprinting?**

Note: because tracking techniques are complex, subtle, and constantly evolving, Panopticklick does not measure all forms of tracking and protection.

Your browser fingerprint **appears to be unique** among the 186,600 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 17.51 bits of identifying information**.

The measurements we used to obtain this result are listed below. You can [read more about our methodology, statistical results, and some defenses against fingerprinting here](#).

Browser Characteristic	bits of identifying information	one in x browsers have this value	value
Limited supercookie test	0.43	1.34	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	8.47	353.41	891f3debe00dbd3d1f0457a70d2f5213
Screen Size and Color Depth	3.17	9.03	1366x768x24
Browser Plugin Details	1.75	3.36	undefined
Time Zone	3.3	9.83	300
DNT Header Enabled?	0.77	1.71	True

10:24 PM 12/9/2016

HTTP_ACCEPT Headers	7.69	206.64	text/html; q=0.01 gzip, deflate, br;en-US
Hash of WebGL fingerprint	5.46	44.14	undetermined
Language	0.99	1.99	en-US
System Fonts	5.91	60.14	Arial, Arial Black, Arial Narrow, Calibri, Cambria, Cambria Math, Comic Sans MS, Consolas, Courier, Courier New, Georgia, Helvetica, Impact, Lucida Console, Lucida Sans Unicode, Microsoft Sans Serif, MS Gothic, MS PGothic, MS Sans Serif, MS Serif, Palatino Linotype, Segoe Print, Segoe Script, Segoe UI, Segoe UI Light, Segoe UI Semibold, Segoe UI Symbol, Tahoma, Times, Times New Roman, Trebuchet MS, Verdana, Wingdings, Wingdings 2, Wingdings 3 (via javascript)
Platform	1.26	2.39	Win32
User Agent	10.26	1227.63	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36
Touch Support	0.48	1.39	Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false
Are Cookies Enabled?	0.2	1.15	Yes

RE-TEST YOUR BROWSER

Thanks to [Fingerprint2](#) for various fingerprinting tests, [Aloodo](#) for portions of the tracker test, [browserspy.dk](#) for the font detection code, and to [breadcrumbs](#) for supercookie help. Send questions or comments to panopticlick@eff.org.

SHARE ON FACEBOOK SHARE ON TWITTER SHARE ON GOOGLE+

About Panopticlick

- [About Panopticlick](#)
- [Methodology](#)
- [What is browser fingerprinting?](#)
- [What is Do Not Track?](#)

Panopticlick is a research project designed to better uncover the tools and techniques of online trackers and test the efficacy of privacy add-ons.

When you visit a website, you are allowing that site to access a lot of information about your computer's configuration. Combined, this information can create a kind of fingerprint — a signature that could be used to identify you and your computer. Some companies use this technology to try to identify individual computers.

In 2010, EFF launched Panopticlick, a research project to investigate how unique each browser is. We gathered information about the configuration and version information from your operating system, your browser, and your plug-ins, and compared it to our database of many other Internet users' configurations. Then, we generated a uniqueness score — letting you see how easily identifiable you might be as you surf the web.

In 2015, we upgraded Panopticlick with a new feature: tracker blocker testing. Million of Internet users are using privacy add-ons and other tools to block trackers, including tools like Adblock, Ghostery and Disconnect. But how well do these add-ons actually protect users from invasive tracking?

Our new version of Panopticlick researches both. We analyze how well you are protected against online tracking by checking the privacy protections you have in place. The test simulates loading of a visible ad that performs tracking, an invisible script that performs tracking, and a site that looks superficially like a tracker but actually has committed to honor Do Not Track.

Even if your privacy add-ons are working well, you may still be vulnerable if your browser fingerprint is unique. So we also analyze the uniqueness of your browser and let you know how it stacks up to other visitors we've observed recently.

We generate a report about your tracker protections and browser fingerprint for your own use, and we'll include anonymous results from your test in our larger research report.

Running tests on Panopticlick both gives you this information about your own browser, and also helps EFF use statistical methods to evaluate the capabilities of Internet tracking and advertising companies, and the best forms of protection against tracking without consent.

A paper reporting the early statistical results of this 2010 Panopticlick experiment is available: *How Unique Is Your Browser?*, Proceedings of the Privacy Enhancing Technologies Symposium (PETS 2010), Springer Lecture Notes in Computer Science. <https://panopticlick.eff.org/browser-uniqueness.pdf>

Methodology:

The results of Panopticlick use several simulated tracking domains to trigger tracker blockers. Some blockers (such as Adblock Plus or Ghostery) are triggered by URL parameters that match ads or tracking beacons. Other blockers (such as AdAway or Disconnect) match on a per-domain basis, and we strive to have our test domains included in such tools' lists. Still other blockers (such as our own Privacy Badger) use a heuristic approach, blocking the inclusion of trackers by detecting their use across domains.

In order to detect these different approaches, we have simulated tracking which triggers all three types of blocking. The site generates third-party requests like:

https://trackersimulator.org/?action=tracking_tally&ad_url=123456

https://eviltracker.net/?action=tracking_tally&trackingserver=123456

https://do-not-tracker.org/?action=tracking_tally&random=123456

Each of these URLs attempts to set cookies, and is loaded from three first party domains in order to trigger heuristic blocking.

The first URL simulates tracking by a visible ad (if the ad is blocked, the test passes); the second simulates a non-visible tracking beacon (if the beacon is blocked, the test passes); and the third interaction with a domain that has implemented the Do Not Track Policy (if the domain's scripts are unblocked, the test passes).

If the simulated ad or beacon trackers load, but with their cookies blocked, those results are reported as "partial protection", since the site doesn't get an easy unique identifier, but tracking by IP addresses and other means remain possible.

In addition to tracker blocking, Panoptick measures the uniqueness of your browser. We anonymously log the following information, and compare it to a database of many other Internet users' configurations that we've observed recently:

- The user agent string from each browser
- The HTTP ACCEPT headers sent by the browser
- Screen resolution and color depth
- The Timezone your system is set to
- The browser extensions/plugins, like Quicktime, Flash, Java or Acrobat, that are installed in the browser, and the versions of those plugins
- The fonts installed on the computer, as reported by Flash or Java.
- Whether your browser executes JavaScript scripts
- Yes/no information saying whether the browser accepts various kinds of cookies and "super cookies"
- A hash of the image generated by canvas fingerprinting
- A hash of the image generated by WebGL fingerprinting
- Yes/no whether your browser is sending the Do Not Track header
- Your system platform (e.g. Win32, Linux x86)
- Your system language (e.g. en-US)
- Your browser's touchscreen support

Then, we generate a uniqueness score — letting you see how easily identifiable you might be as you surf the web. [Here's more information on how this score is derived.](#)

What is fingerprinting? What does it mean if my browser is unique?

“Browser fingerprinting” is a method of tracking web browsers by the configuration and settings information they make visible to websites, rather than traditional tracking methods such as IP addresses and unique cookies.

Browser fingerprinting is both difficult to detect and and extremely difficult to thwart.

When you load a web page, you will automatically broadcast certain information about your browser to the website you are visiting — as well as to any trackers embedded within the site (such as those that serve advertisements). The site you are visiting may choose to analyze your browser using JavaScript, Flash and other methods (just like Panoptick does). It may look for what types of fonts you have installed, the language you've set, the add-ons you've installed, and other factors. The site may then create a type of profile of you, tied to this pattern of characteristics associated with your browser, rather than tied to a specific tracking cookie.

If your browser is unique, then it's possible that an online tracker can identify you even without setting tracking cookies. While the tracker won't know your name, they could collect a deeply personal dossier of websites you visit.

Deleting your cookies won't help, because it's the characteristics of your browser configuration that are being analyzed. Read our [suggestions to help defend against browser fingerprinting.](#)

What is Do Not Track? Why would I want to unblock ads that respect Do Not Track?

Every time your computer sends or receives information over the Web, the request begins with some short pieces of information called **headers**. These headers include information like what browser you're using, what language your computer is set to, and other technical details.

Do Not Track is a simple, machine-readable header indicating that you don't want to be tracked. Because this signal is a header, and not a cookie, users can clear their cookies at will without disrupting the functionality of the Do Not Track flag.

In all the major browsers, there is an easy way to tell websites that you do not want to be tracked by setting the Do Not Track header. (**Do it yourself** or **install EFF's Privacy Badger** and we'll turn it on for you in Chrome and Firefox.)

When websites respect the Do Not Track signal, it's easy for users to protect themselves from online tracking. The average Internet user won't need to remember to delete cookies, install additional privacy software, or even worry about browser fingerprinting. (link to browser fingerprinting section).

Unfortunately, most websites and online trackers — with some laudable exceptions — currently ignore the Do Not Track signal entirely.

Setting your browser to unblock ads from websites that commit to respecting Do Not Track rewards companies that are respecting user privacy, incentivizing more companies to respect Do Not Track in order to have their ads shown at all. By preserving privacy-friendly ads, sites that rely on advertising funding can continue to thrive without adjusting their core business model, even as they respect users' privacy choices.

Over time, we believe we can shift the norms on the Web to ensure privacy and respect for users comes first. But that can only happen if online advertisers are incentivized to respect user choices.

You can help us by **installing EFF's Privacy Badger**.

Is it possible to defend against browser fingerprinting?

Browser fingerprinting is quite a powerful method of tracking users around the Internet. There are some defensive measures that can be taken with existing browsers, but none of them are ideal. In practice, the most realistic protection is using the Tor Browser, which has put a lot of effort into reducing browser fingerprintability. For day-to-day use, the best options are to run tools like Privacy Badger or Disconnect that will block some (but unfortunately not all) of the domains that try to perform fingerprinting, and/or to use a tool like NoScript for Firefox, which greatly reduces the amount of data available to fingerprinters.

Use the Tor Browser

The Tor Project has spent considerable effort trying to "standardize" various browser characteristics like the User Agent string, in order to prevent them from being used to track Tor users. In response to Panopticlick and other fingerprinting experiments, the **Tor Browser** now includes patches to

prevent font fingerprinting (by restricting which fonts websites can use) and Canvas fingerprinting (by detecting reads to HTML5 Canvas objects and asking users to approve them). The Tor Browser can also be configured to be aggressively block JavaScript. Taken together, these measures make the Tor Browser a strong defense against fingerprinting. Unfortunately, browsing through Tor is currently a lot slower than browsing without it.

Disable JavaScript

Disabling JavaScript is a powerful defense against browser fingerprinting, because it cuts off the methods that websites can use to detect plugins and fonts, as well as preventing the use of most kinds of supercookie. Unfortunately, JavaScript is necessary to make a lot of sites work well.

At least two ways to block some sites from using JavaScript while allowing others to use it are available. One, **NoScript**, is more of a power-user tool than a solution for everyone: it will block JavaScript everywhere and allow you to manually reenable it for some sites. This is a lot of work, and requires good intuitions about when a site isn't working because JavaScript is disabled. Common adblocking tools tend to be quite good at blocking ads, because users can instantly see when they're present. Tracking or fingerprinting scripts are generally invisible, so even if users enable features that **focus on privacy**, some trackers may still **slip past the net**.

Try to use a "non-rare" browser

The most obvious way to try to prevent browser fingerprinting is to pick a "standard", "common" browser. It turns out that this is surprisingly hard to do. It appears that the most likely candidate would be the latest version of Chrome running on a modern Windows version. But even so, many of those Chrome on Windows browsers can be distinguished from one another by the enormous range of plugin versions and fonts that can be installed with them. The first generations of smartphone browsers **were comparatively hard to fingerprint**, but as these devices have become more diverse and supported wider ranges of features, they have also become very fingerprintable.