FINGERPRINTING EXPLAINED: HOW IT WORKS & HOW TO BLOCK IT



Fingerprinting is a tracking technique that advertisers and companies use. This tracking is such a shocking invasion of privacy that I feel compelled to explain it and how you can block it.

My concern is not the only one. Different companies have developed browser plug-ins to block fingerprinting, and one open-source project has given away their code, which shows how fingerprinting works—and we'll explain in this article.

What is fingerprinting?
Can I find my own fingerprint?
How is fingerprinting so accurate?
Who is most vulnerable to fingerprinting?
Why should I care about fingerprinting?
Can I block fingerprinting?
What is the user agent?
Does this approach work for all browsers and operating systems?
Note on browser behavior
Firefox on Mac
Chrome on Mac
iCab Mobile on iPhone and iPad
What about advertising cookies?

Washington Post example
CNN example
Privacy concerns

What is fingerprinting?

I first heard about fingerprinting in The Washington Post, when Edward Snowden said, in the information he gave to journalists, that the NSA was using the screen resolution of computers to identify terrorists and others. Now, advertisers are using these same techniques. It shocks me that the techniques of spy agencies have gone mainstream.

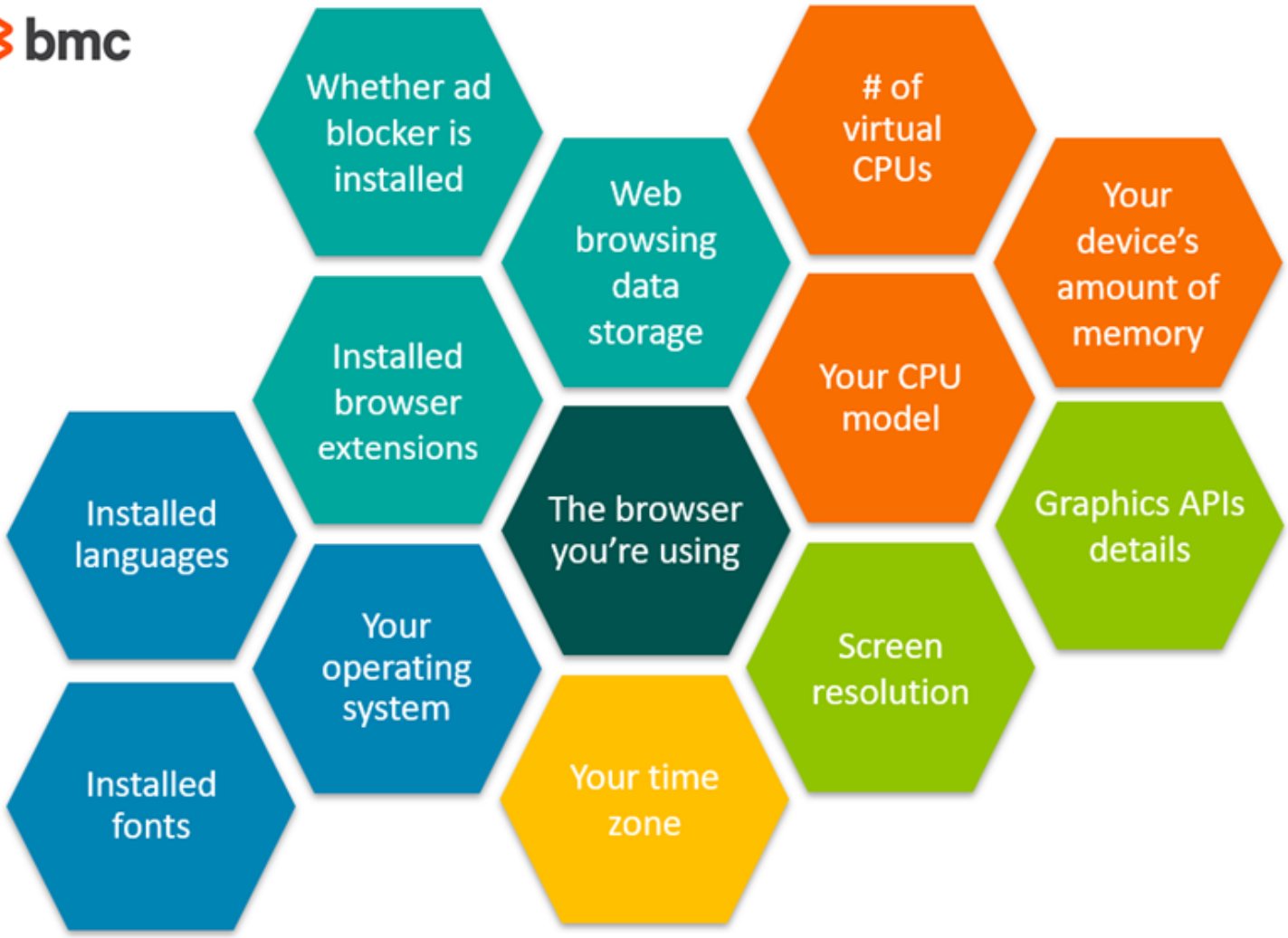
A **fingerprint** is a number that is calculated from information about your computer, some of it the user perhaps thinks might be private. This includes:

- The browser you are using
- Your screen resolution
- Information on your graphics drivers
- CPU type
- Operating system and version
- Time zone
- Etc.

Much of this information is contained in the browser. Other information can be stolen in clever ways that researchers have discovered.

The fingerprint takes all that data, turns it into numbers, sums it, and then runs a calculation over it to yield a single value. Because this algorithm uses the same calculation every time, it will provide the same value (number) every time. As long as you are using the same device and browser, every time you visit a web site that uses fingerprinting, that website knows who you are—with approximately 95% to 99.5% accuracy.

To be specific, fingerprinting uses these metrics:



Select metrics that advertisers use in fingerprinting

These metrics are available in the fingerprinting JavaScript code, shown below. The authors of that open source code say there are working on gathering other metrics that advertisers use, such as information about your camera.

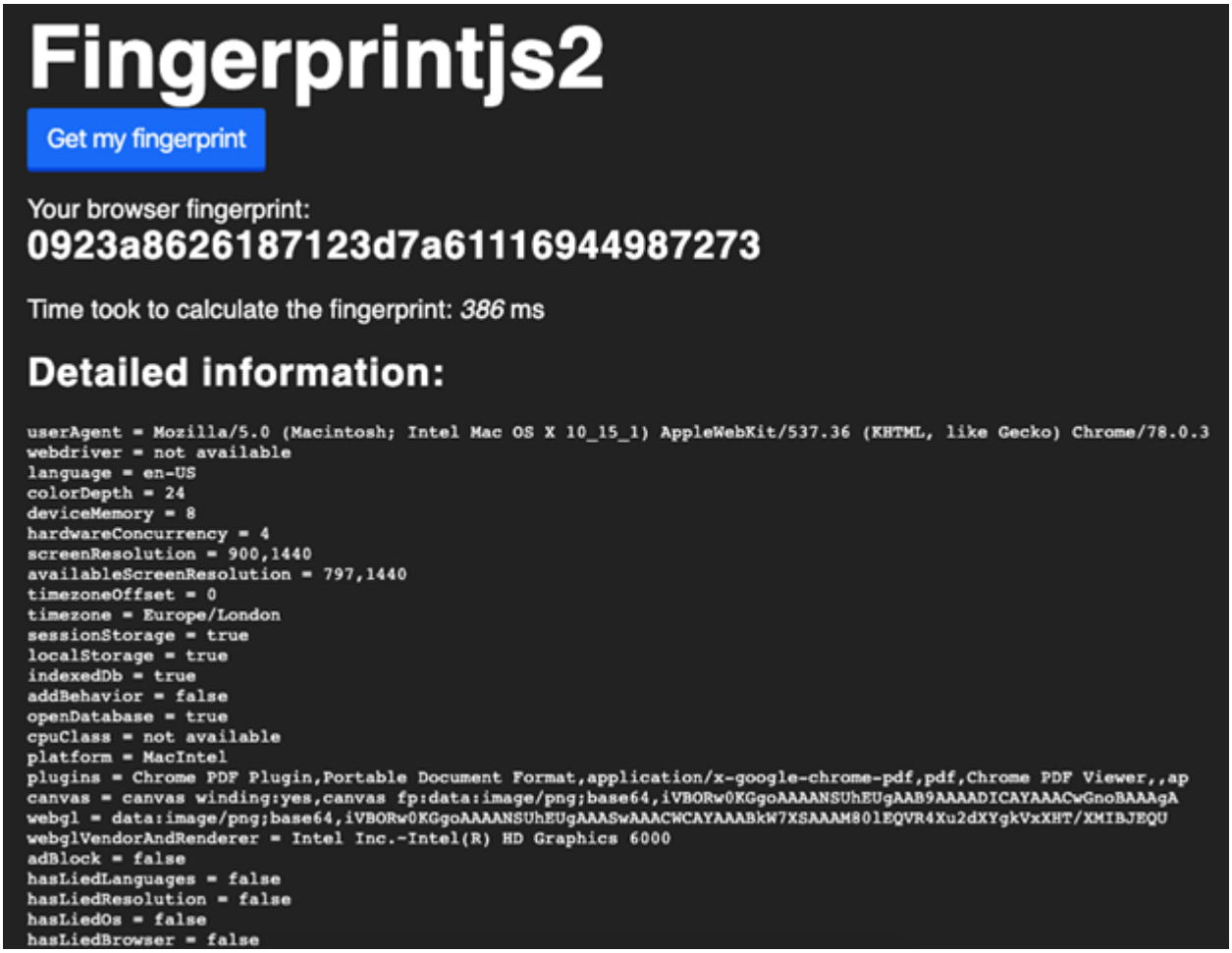
What's remarkable is that fingerprinting is able to extract this information simply by querying what is in the browser. It does not require access to the operating system at all.

At least one item, screen resolution, does require some clever thinking. To figure that out, the web site sends you a graphic of a known size and resolution, then reads the pixel resolution that your browser is able to display. And, it does this **without** displaying the image at all.

Can I find my own fingerprint?

To find your fingerprint, visit this page I set up. I sourced this code and put it on a web server. The programmers of this code wanted to expose this practice by providing JavaScript code and links to other code and research to explain how fingerprinting works.

The screen below shows your fingerprint and the metrics gathered from your machine used to calculate that fingerprint.



How is fingerprinting so accurate?

To understand the claim made by this code that this is 99.5% accurate, consider some simple math.

Suppose you and 1,000 other people all bought the same iPad. The chance of guessing which of those people is you is 1/1000 or 0.001. But what about we look at your time zone? There are 24 of those. So, if we know your time zone, and we assume that people are evenly dispersed across time zones (they're not), then the chance of identifying you is 1/24.

But what if we also look at the type and version of the browser you are using. Suppose there are 700 types and versions (there are actually many more). Given that we know what browser you are using and what time zone you are in the chance of finding you among those 1,000 iPad owners is 1 - (1/24)*(1/700) which is 1 - 0.000059 or virtually 100%.

Of course, browsers and people are not evenly dispersed, so that number will vary widely. But as we add more metrics, the calculation becomes much more accurate. Subtle differences in your machine versus another machine make a big difference in figuring out who you are.

Who is most vulnerable to fingerprinting?

It turns out that the people who are hardest to identify are users without much computing knowledge who are using iPads and iPhones. This is because:

1. Apple does not let third parties install browser plug-ins on iOS.
2. Apple does not license its operating system to other manufacturers.

3. Less experienced users aren't likely to install custom browsers.

Item #1 is important because the variety of plug-ins you have installed helps identify you. Item #2 is important because Apple works with a small number of manufacturers. That means there is a relatively small number of graphics drivers combinations, CPU types and capabilities, etc.

Contrast that with Google Android, Linux, and Microsoft Windows. Thousands of manufacturers around the world build desktops, laptops, tablets, fitness watches, door bell ringers, etc., running Android, difference types of Linux, and Windows. Each of those uses an enormous supply chain of vendors to build graphics chips and CPUs. And each of those has a lot of models and versions of those in use at any one time. Also, consider that Google lets device manufacturers and cell phone providers customize small parts of Android to brand their product.

That's an enormous variety of metrics to feed into the fingerprint algorithm. If you own any one of those devices, it's like walking around with your social security number or national ID number tattooed on your forehead.

But fingerprinting is mainly used by advertisers. Fingerprinting does not reveal your name—they don't need to know that. Advertisers just need to know enough information about you and your browsing history to pitch targeted advertising to you.

Facebook and Google don't need to use fingerprinting, because they record far more information—information that you freely hand over to them when you post updates, click Like, and search topics, people, and events.

So, what can we conclude from this? Are iPhone users safe? What about Mac? It depends.

Even Apple hardware varies from one model to another. But if you are a user who has added Chrome, that sets you apart from less knowledgeable users. And if you are using a Mac, then you are allowed to add plug-ins to your browser.

Therefore, we can conclude that the more you know about computers the more likely it is you can be fingerprinted, as you would have installed more browser extensions than less knowledgeable users.

As for Windows, Android, and Ubuntu users, due to the wide variety of manufacturers and chip makes involved, it is fairly certain that fingerprinting can identify you with 99.5% accuracy or higher.

Why should I care about fingerprinting?

The answer is that you don't **have** to care about fingerprinting. You already know that advertising cookies track you. (We talk more about how that relates to fingerprinting at the end.) If you don't care that advertisers are following you around the internet, then there's nothing to worry about.

But what about web sites beyond the daily newspaper? What about persons who are considering bankruptcy, victims of domestic abuse, drug addicts, or people looking for a divorce attorney? Do you really want people to know that you are visiting those websites?

You might think that cookie ad blockers, VPN, or Tor is making you safe. If you think that, you are wrong. None of those options change your screen resolution, browser version, etc., so they do not change your fingerprint.

You think VPN and Tor protects you because it hides your IP address. Wrong. Those mask your

public IP address. They don't even give away your IP address on your internal network, such as when you are at work in your office, because that uses NAT (It basically translates your IP address from your internal private one to one shared public one) as does your home network.

Your internal address is what someone would need to identify you. So that gives you a bit of anonymity right there.

But advertisers don't even care about your IP address. The only one who might be interesting in that is law enforcement or content owners, like HBO (so they can block international users and sue people who download copyrighted material).

Can I block fingerprinting?

Yes. There is one way and one way only you can do this: you can spoof, i.e., make up the **user agent** on your browser. This effectively destroys the accuracy of the fingerprint calculation by giving it one false value.

For this strategy to work, you'll need to change your user agent frequently. After all, sending an incorrect value as your fingerprint doesn't help if you use that number forever. Fortunately, there are some tools to help you do that. We explore those below.

What is the user agent?

When you visit a web page, the browser sends certain information to the web site. That information is necessary so the browser can know things like whether you are using a mobile device (and thus display a small screen) or a laptop or desktop (use a bigger screen). It also needs to modify the web page code slightly as certain functions work differently or don't work at all on certain browsers.

The user agent looks like this:

```
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_1) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/78.0.3
```

This is three sets of fields:

Field	Description
Mozilla/5.0	This pretty much always says **Mozilla/5.0**. It simply means whether this browser is compatible with Mozilla 5.0. Mozilla invented one of the earliest browsers and thus HTML standards are an extension of that.
(Macintosh; Intel Mac OS X 10_15_1)	Operating System, CPU Type, and OS version. It might also include the device type, but not in all cases.
AppleWebKit/537.36 (KHTML, like Gecko)	This basically tells you for which operating system the browser was built, such as Chrome for Windows.
Chrome/78.0.3	Browser name and version.

Here are some examples:

Browser	User Agent value
Chrome on Windows	Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.106 Safa
Internet Explorer 10 on Windows	Mozilla/5.0 (compatible; WOW64; MSIE 10.0; Windows NT 6.2)
Microsoft Edge on Windows Phone	Mozilla/5.0 (Windows Phone 10.0; Android 4.2.1; NOKIA; Lumia 735) AppleWebKit/537.36 (KHTML, like Ge

Does this approach work for all browsers and operating systems?

I have not looked at Android, Ubuntu, and Windows. I only looked at Apple devices.

The takeaway message is:

- You should not use Safari on Mac or iOS.
- For iOS, avoid Firefox, Chrome, or Safari. Instead use iCab Mobile, which actually is perhaps better than Chrome, Firefox, and Safari as it has many interesting and useful features those don't. Apple does not let the major browsers spoof the user agent. iCab figured out how to do that. This browser is $1.99 on the Apple app store.

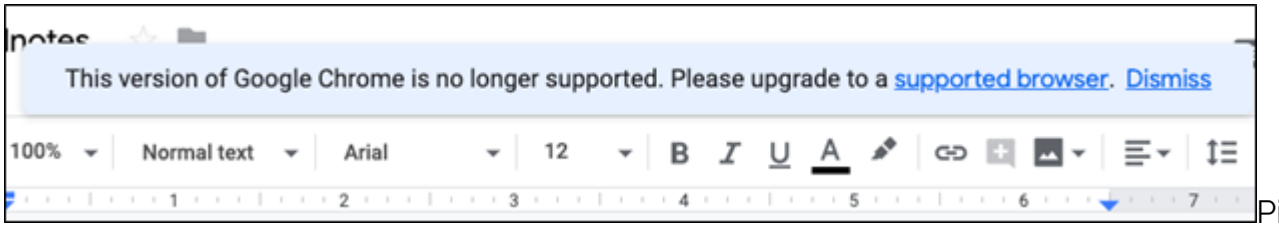
Here is the list of what browsers on Apple Macs, iPads, and iPhones for which I have verified that you can spoof your User Agent.

Browser	OS	Can you spoof the user agent?
Firefox	Mac	Yes, by making a change
Chrome	Mac	Yes, with a plugin
iCab Mobile	iOS	Yes, with built-in functionality

Note on browser behavior

Here, we'll show you how to protect your identity by spoofing the user agent. When you do this, know that certain web pages will behave differently depending on your selected browser. You usually don't need to worry about this and can ignore any warning messages.

For example, the web page might say you are using an old browser. But if you are using a laptop and your user agent tells the web page you are using a mobile device, the screen could look entirely different.

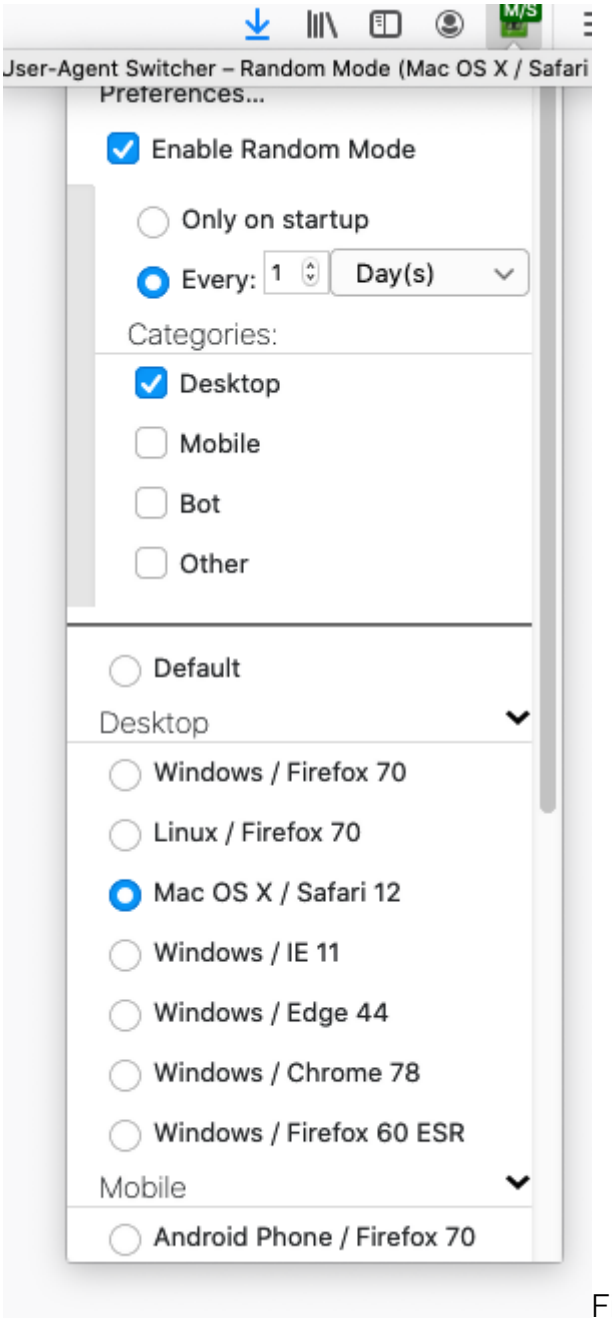


Pick something that is reasonable and not too obscure—for example, Nokia on MeeGo might not be a good option.

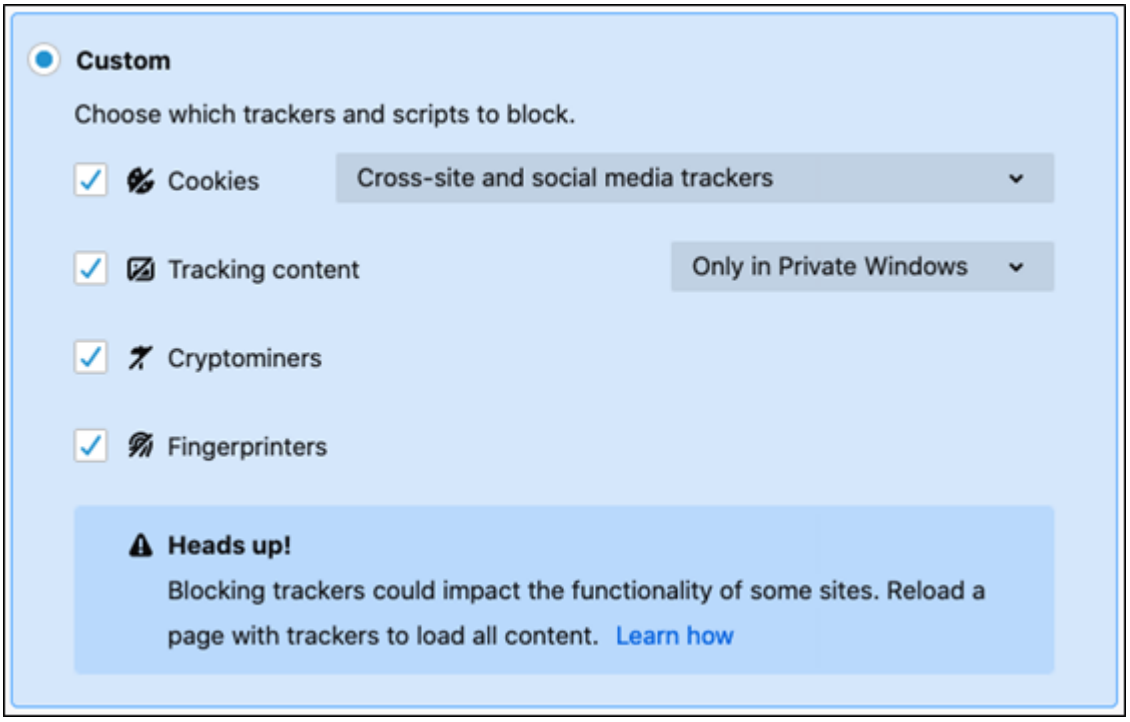
Firefox on Mac

Use the browser plugin Firefox User Agent Switcher. This plugin will not work on the iPhone or iPad, as Apple does not allow browser plugins on those devices.

Remember we said it is important to change the user agent frequently? This one is handy because you can set it up to automatically rotate through those.

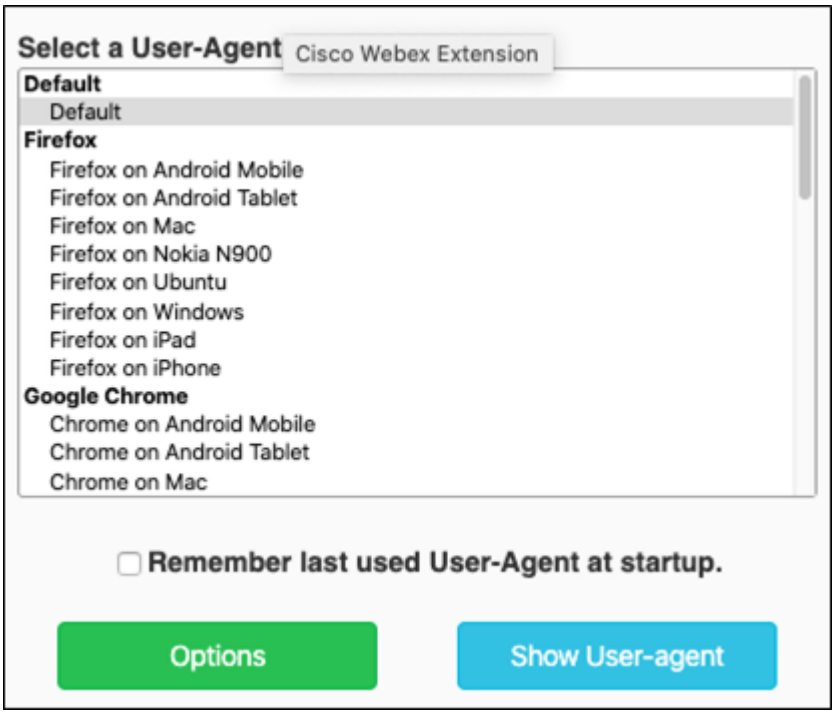


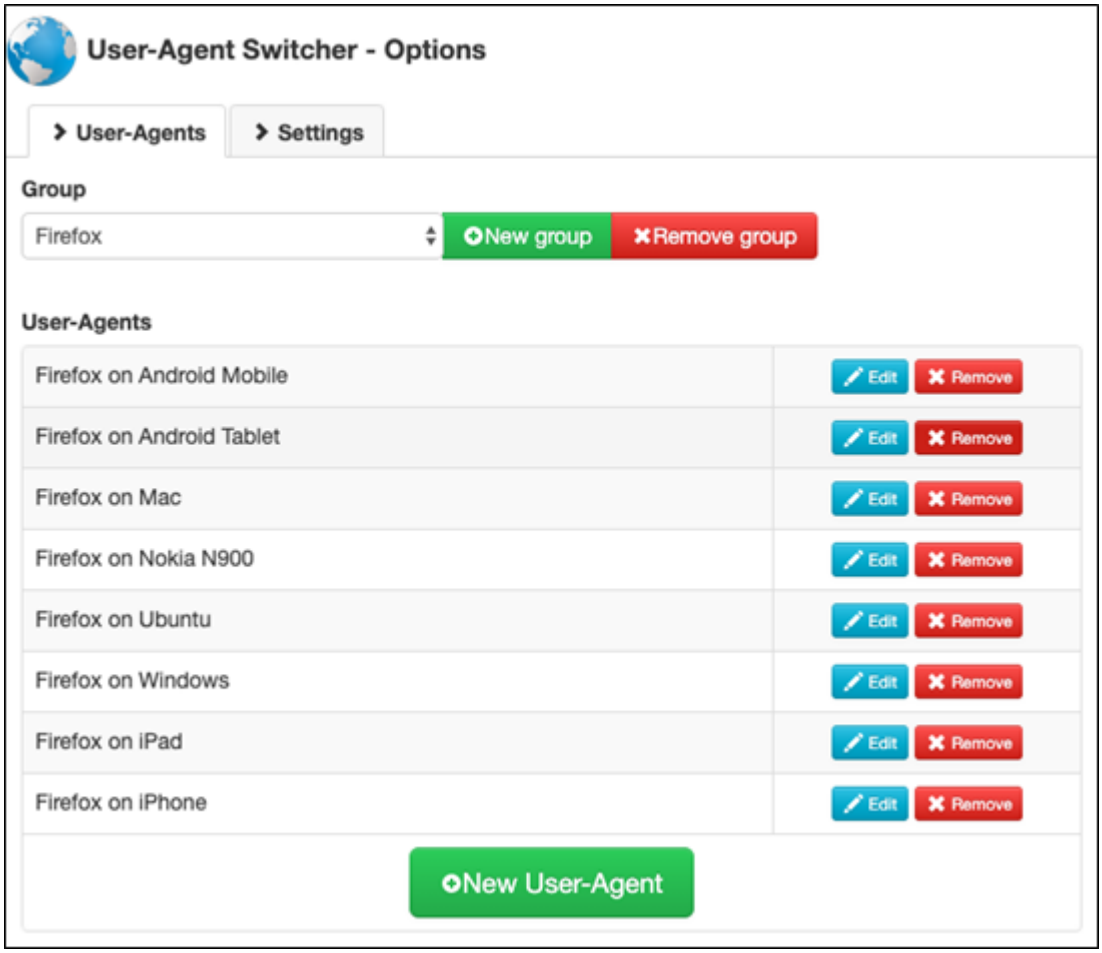
Firefox also has built in the ability to defeat fingerprinting. In my testing, however, this function does not work.



Chrome on Mac

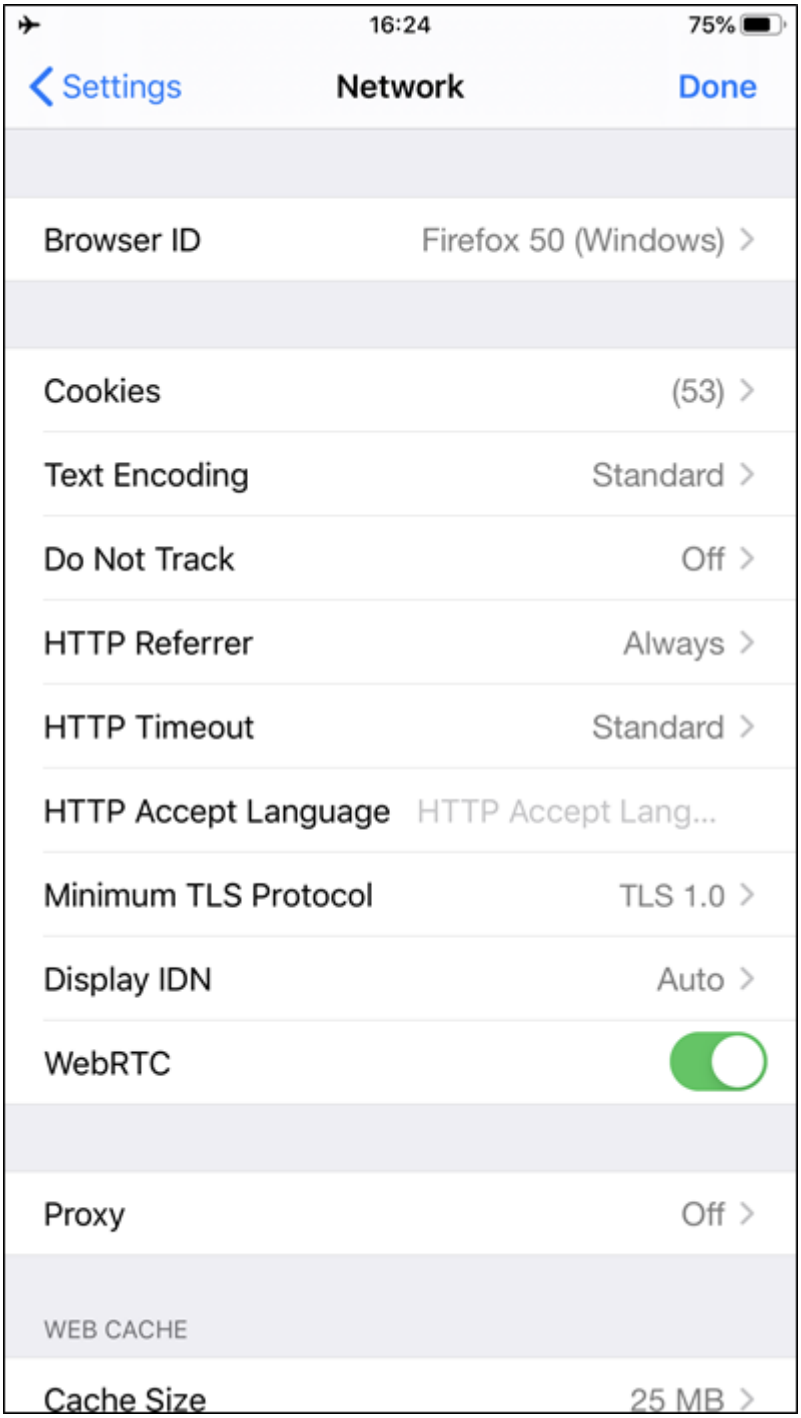
Normally you shouldn't trust Google with anything related to privacy. But you can safely use the Chrome User Agent Switcher browser extension. The image below shows how you simply select the browser you want to emulate.

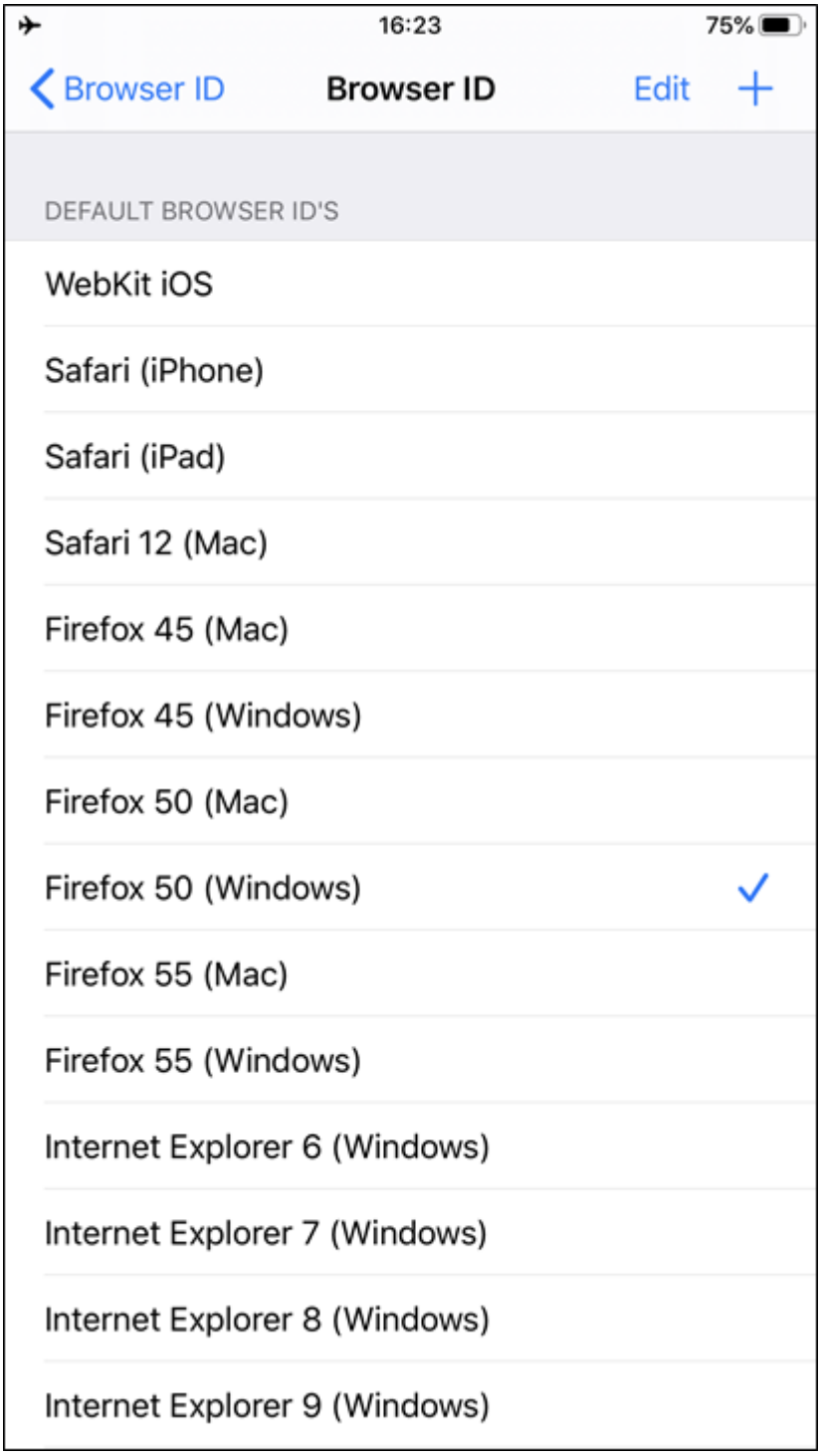




iCab Mobile on iPhone and iPad

If you use iCabMobile, you can click on the **Network** setting and change the browser version, as shown below.


16:24
75%
Settings
Network
Done
Browser ID
Firefox 50 (Windows)
Cookies
(53)
Text Encoding
Standard
Do Not Track
Off
HTTP Referrer
Always
HTTP Timeout
Standard
HTTP Accept Language
HTTP Accept Lang...
Minimum TLS Protocol
TLS 1.0
Display IDN
Auto
WebRTC
Proxy
Off
WEB CACHE
Cache Size
25 MB



What about advertising cookies?

We can make this claim: because of fingerprinting, advertisers don't need cookies at all. They just need the fingerprint.

Consider what a cookie does. An advertiser plants a file (the cookie) on your computer that assigns you an identity. Then, the advertiser can track what websites you visit by reading and updating that cookie as you visit different web sites that also use the same advertising software. It builds an accurate, if partial, view of your online activity.

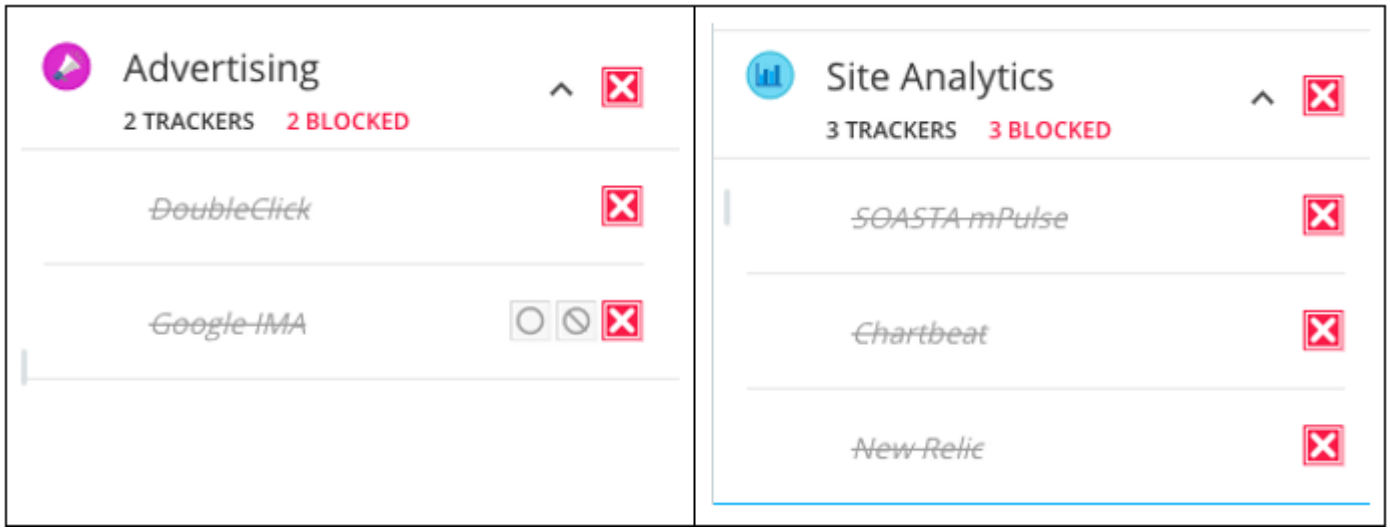
But fingerprinting uniquely identifies you. With fingerprinting, advertisers don't need cookies at all. They simply calculate the fingerprint and save it in their database. It's another means to achieve the same result.

As to how many websites use cookies, it would be better to ask **how many advertisers use cookies**—as most websites use advertisers.

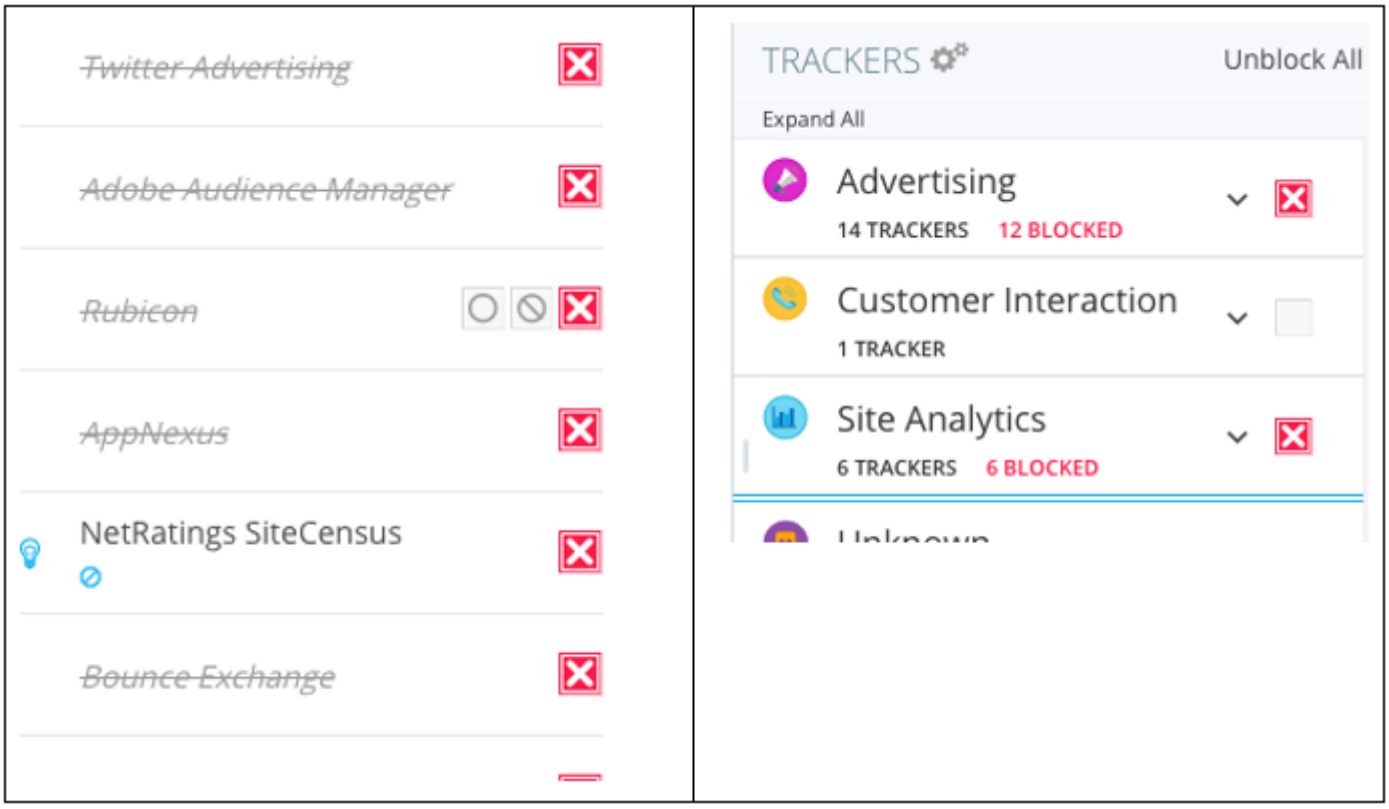
Look at two examples.

Look at the four screens below. These are shown by the Ghostery browser plugin. The first two screens show advertising and site analytics tracking hosted on The Washington Post. The second two are on CNN.

Washington Post



CNN



The site analytics code tracks additional information, like where you click on the web page and how quickly you scroll your mouse.

Privacy concerns

Fingerprinting has flown under the privacy radar because most people don't understand it even if they were to be told about it. Most people know that Facebook and Google have been accused of privacy violations, but fingerprinting should be exposed as well.

On one hand, you might not care about advertisers tracking your online activity. But, on the other hand, you might care when that practice extends to web sites that are private in nature.

Related reading

- BMC Business of IT Blog
- Structured vs Unstructured Data: A Shift in Privacy
- Data Ethics for Companies
- Introduction To Data Security
- Cybercrime Rising: 6 Steps To Prepare Your Business