
Exposed record
Data breach
digital
classification
search
DATA
PRIVACY
Protection
law
anonimous
Metadata
Regulations
Patient privacy
Privacy
Risk
Sensitive Information
Authentication
compliance

Privacy On the Internet

Agenda of our Privacy On the Internet Series:

- ✓ **Part One: VPN's (Virtual Private Networks)**
- ✓ **Part Two: Browsers and basic browser privacy settings**
- ✓ **Part Three: Search engines**
- **Part Four: Some of the ways you can be tracked**
- **Part Five: Anti-tracking and add blocker software**
- **Part Six: The privacy policies of the internet giants and what they do with your information**
- **Part Seven: Can you remove all your personal info from the internet?**

Then we'll see where we go from there

Privacy On the Internet

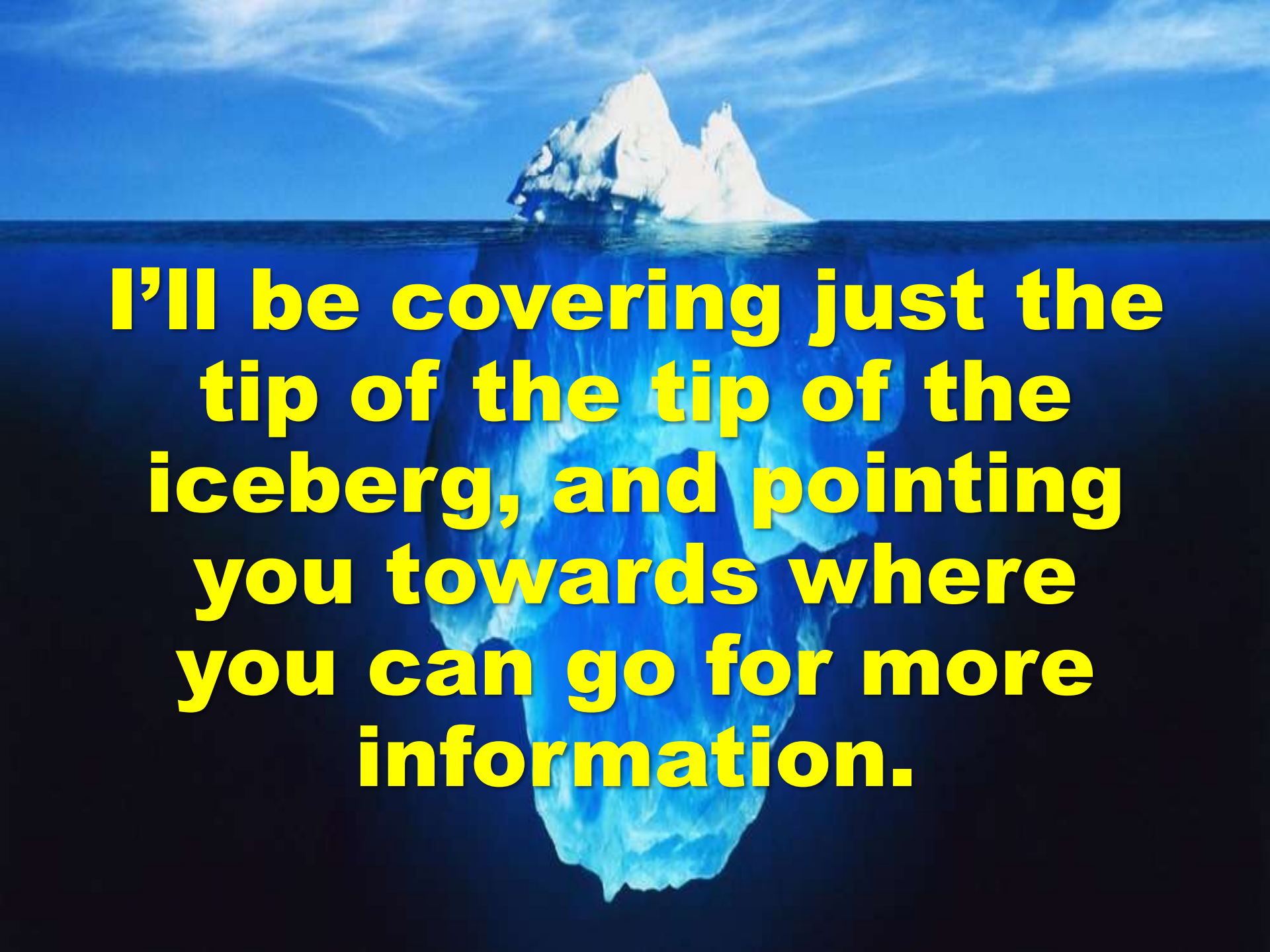
Last session we looked at

PRIVATE SEARCH ENGINES

This week we'll look at

SOME OF THE WAYS YOU CAN BE TRACKED

and how they can affect your privacy.


I'll be covering just the tip of the tip of the iceberg, and pointing you towards where you can go for more information.

Who's Tracking YOU!

Many companies, including internet giants Google and Facebook, make most of their money by using your personal information for targeting advertising or by selling your personal information to advertisers, insurance companies and others.

Other internet companies from giants like Amazon to maandpa.com to everything in between also make some of their money selling your personal information.

Who's Tracking YOU!

- **Google trackers are present on 82% of the web traffic.**
- **25% of the web has a hidden Facebook tracking pixel. Facebook knows a lot more than just what you do on Facebook.**
- **Google's own domains don't contain that many trackers. The same is true for Facebook. But that's because they place most of their trackers on other websites.**
- **A third of the 6000 top websites have more than 10 trackers per page.**
- **Organizations tracking you include advertising and marketing companies, web analytics companies, political parties and news organizations. Companies like Amazon, Yahoo, Google, AppNexus, SpotX, Quantcast and DoubleClick.**

Who's Tracking YOU!

There's a great story in the New York Times titled *'I Visited 47 Sites. Hundreds of Trackers Followed Me.'* * that shows that everything you do online is tracked and logged in exquisite detail, you have no privacy.

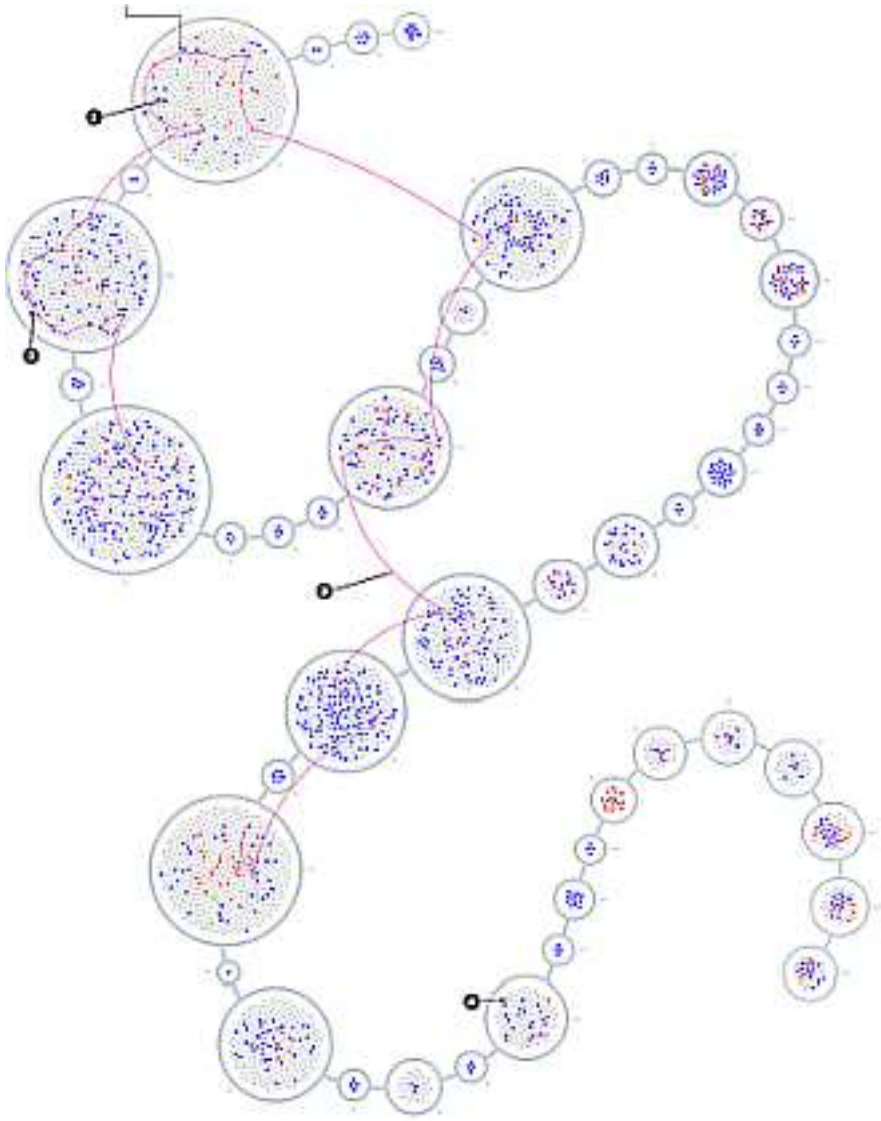
* - https://www.nytimes.com/interactive/2019/08/23/opinion/data-internet-privacy-tracking.html

Who's Tracking YOU!

Using special software from Mozilla, a reporter was able to track the trackers over several days as he carried out his normal internet activities.

The diagram on the left shows the tracker's activity in just one session as he researched a story online over a couple of hours. Each small dot represents one tracking resource (like a script, tracking pixel or image).

They were able to see every site and page he visited, what clicks he made, what searches he made, and they were even able to get some of his user names and passwords.



Who’s Tracking YOU!

He didn't have to visit any shady sites or make any untoward searches - he just had to venture somewhere, anywhere on the internet and he was watched.

This is happening every day, all the time, to any of us.

So How Are You Being Tracked?

- Cookies
- Zombie cookies
- Evercookies
- Supercookies

} Bad Cookies

- Internet Protocol (IP) address
- Beacons (AKA tags or pixels)
- Fingerprinting
- Extended URL’s

Cookies*

- When a user visits a website for the first time, the web server may generate a unique identifier (cookie) and store it on the user's browser or local space. More than one cookie may be placed on a user’s device during a session.
- The website can read and identify the user in their future visits with the stored identifier, and the website can save login information, language selections, user preferences, internal site bookmarks, keep track of the user’s shopping cart, etc.
- Due to privacy concerns, all major browsers include mechanisms for deleting and/or refusing cookies from websites.

* - Also known as HTTP cookies, web cookies, Internet cookies or browser cookies

Cookies

- **PERSISTENT cookies (also known as first-party cookies, authentication cookies, permanent cookies and stored cookies) work by tracking your online preferences.**
- **The security of a persistent cookie generally depends on the security of the issuing website and the user's web browser, and on whether the cookie data is encrypted.**
- **Security vulnerabilities may allow a cookie's data to be read by an attacker, used to gain access to user data, or used to gain access (with the user's credentials) to the website to which the cookie belongs (known as cross-site scripting or cross-site request forgery).**

Cookies

- **SESSION cookies are temporary cookies that memorize your online activities. Since websites have no sense of memory, without these cookies, your site browsing history would always be blank. In fact, with every click you would make, the website would treat you as a completely new visitor.**
- **A good example of how session cookies are helpful is online shopping. When you're shopping online, you can check-out at any time. That's because session cookies track your movement. Without these cookies, whenever you would go to check-out, your cart would be empty.**
- **Usually session cookies expire as soon as you close out of a web page, but some websites may have them stay for the next session (e.g. shopping cart).**

Cookies

- **TRACKING cookies are commonly used as ways to compile long-term records of an individual's browsing histories — a major privacy concern.**
- **A FIRST-PARTY cookie (persistent and session cookies) comes from the site you're on.**
- **A first-party cookie can also be a tracking cookie so that the site can track your other internet activity.**

Cookies

- **A THIRD-PARTY cookie comes from a different website and are almost always tracking cookies designed to track your internet activity across other websites.**
- **Most browsers have a setting to block third-party cookies.**

Cookies

In most browsers, *'Private'* mode (aka *'Incognito'* mode or *'InPrivate'* mode) doesn't share cookies with the regular browsing mode, and it doesn't save cookies once you close it, but check your browser's settings to be sure.

Cookies

In most browsers, you can set the browser to delete all cookies at the end of a session, but you can usually have specific cookies for the sites you visit often (e.g. Amazon) remain.

Cookies

You can search on how to clear and manage cookies for the particular browser(s) you use.

A good place to start:

'How to clear cookies in Chrome, Firefox, Safari, and other browsers'

https://us.norton.com/internetsecurity-privacy-how-to-clear-cookies.html

Cookies

Several companies also offer tools for clearing browser cookies and caches, often as part of a more general maintenance or security package, but use these with caution and pay attention to the settings (don't let them mess with your registry or drivers!).

Examples are *'Avast Cleanup'* or *'System Mechanic'*.

Bad Cookies

The terms *'zombie cookie'*, *'evercookie'* and *'supercookie'* are often used interchangeably but they are slightly different.

Keep in mind the exact definitions are NOT universally agreed to*.

One thing that is agreed to is that they are all bad cookies.

The names are rather misleading because these are not actually cookies.

*** - Definitions given in this presentation are from https://en.wikipedia.org**

https://en.wikipedia.org/wiki/HTTP_cookie

https://en.wikipedia.org/wiki/Zombie_cookie

https://en.wikipedia.org/wiki/Evercookie

Zombie Cookies

A zombie cookie is code that has been placed by a web server when a user visits the website, on the user's computer or other device *in a hidden location outside the visitor's web browser's dedicated cookie storage location*, and that automatically recreates a regular cookie after the original cookie had been deleted.

The zombie cookie's data and code may be stored online or directly on the visitor's device, in a breach of browser security. This mechanism makes zombie cookies very difficult to remove.

Since they do not rely on normal cookie protocols, the visitor's web browser may continue to recreate deleted cookies even though the user has opted not to receive any new cookies.

Zombie Cookies

Zombie cookies are also used to remember unique IDs used for logging into websites. This means that for a user who deletes all their cookies regularly, a site using this would still be able to personalize to that specific user.

Supercookies (Evercookies)

- **Supercookies don't use local storage as regular cookies do. Instead, they are injected at the network level as Unique Identifier Headers (UIDH).**
- **Supercookies are inserted by your Internet Service Provider (ISP) rather than the website itself.**
- **You may not be aware of their existence as the ISP might use them in secret.**
- **UIDH personal data can be revealed to any website and potentially sold to third parties.**

Supercookies (Evercookies)

- **Supercookies allow third parties to track you too. They can independently identify tracking headers themselves and use the data to serve you targeted ads across the web.**
- **Like zombie cookies, supercookies can restore the data of your deleted cookies and link the data with new ones. They can access your login credentials, image and file caches, and plug-in data.**
- **Ad blockers can’t block them, and you can't clear them by deleting your browser history and cache data.**
- **You can’t simply delete supercookies.**

Supercookies (Evercookies)

So what can you do about supercookies?

- **Supercookies depend on HTTP connections, so making an encrypted connection with a website stops tracking headers from functioning. Visiting only HTTPS websites (those that use SSL or TLS certificates) should help you avoid supercookies tracking you or catching them in the first place.**
- **You can use a VPN (virtual private network), preferably one with multi-hop and/or split tunneling. The encrypted link between your computer and the VPN server short-circuits the ability of the UIDH (Supercookie) to see and track what you are doing.**

Internet Protocol (IP) Address

The Internet Protocol (IP) address is the Internet address given to your device by your network or Internet Service Provider (ISP).

It can reveal your general location and other information.

Internet Protocol (IP) Address

- **Some Privacy Browsers can ‘spoof’ or disguise your IP address.**
- **VPN’s give you a new IP address, usually on a session by session basis. The new IP address gives the general location of the VPN server, not you.**

Web Beacons

(AKA Tags or Tracking Pixels)

- **A web beacon is a technique used on web pages and email to unobtrusively (usually invisibly) allow checking that a user has accessed some content.**
- **Web beacons are typically used by third parties to monitor the activity of users at a website for the purpose of web analytics or page tagging.**
- **They can also be used for email tracking (‘Mailtrack’).**
- **Using beacons, companies and organizations can track the online behaviour of web users.**
- **At first, the companies doing such tracking were mainly advertisers or web analytics companies. Later social media sites, especially Facebook, also started to use this tracking technique.**

Web Beacons
(AKA Tags or Tracking Pixels)

- **Some email specific web beacons can be blocked by browser extensions like PixelBlock.**
- **Email specific web beacons can be defeated by deactivating auto-loading for embedded images in your emails.**
- **We'll be looking at anti-tracking tools in a future session.**

Fingerprinting

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 make and model of your device
- Operating system and version installed
- Browser and version you are using
- Your screen resolution
- Information on your graphics drivers
- Software and hardware versions
- CPU type
- Time zone
- Language preferences
- Internet protocol (IP) address
- Deduced physical location
- Internal searches performed
- Number of times the interaction occurred
- What time they happened

Fingerprinting

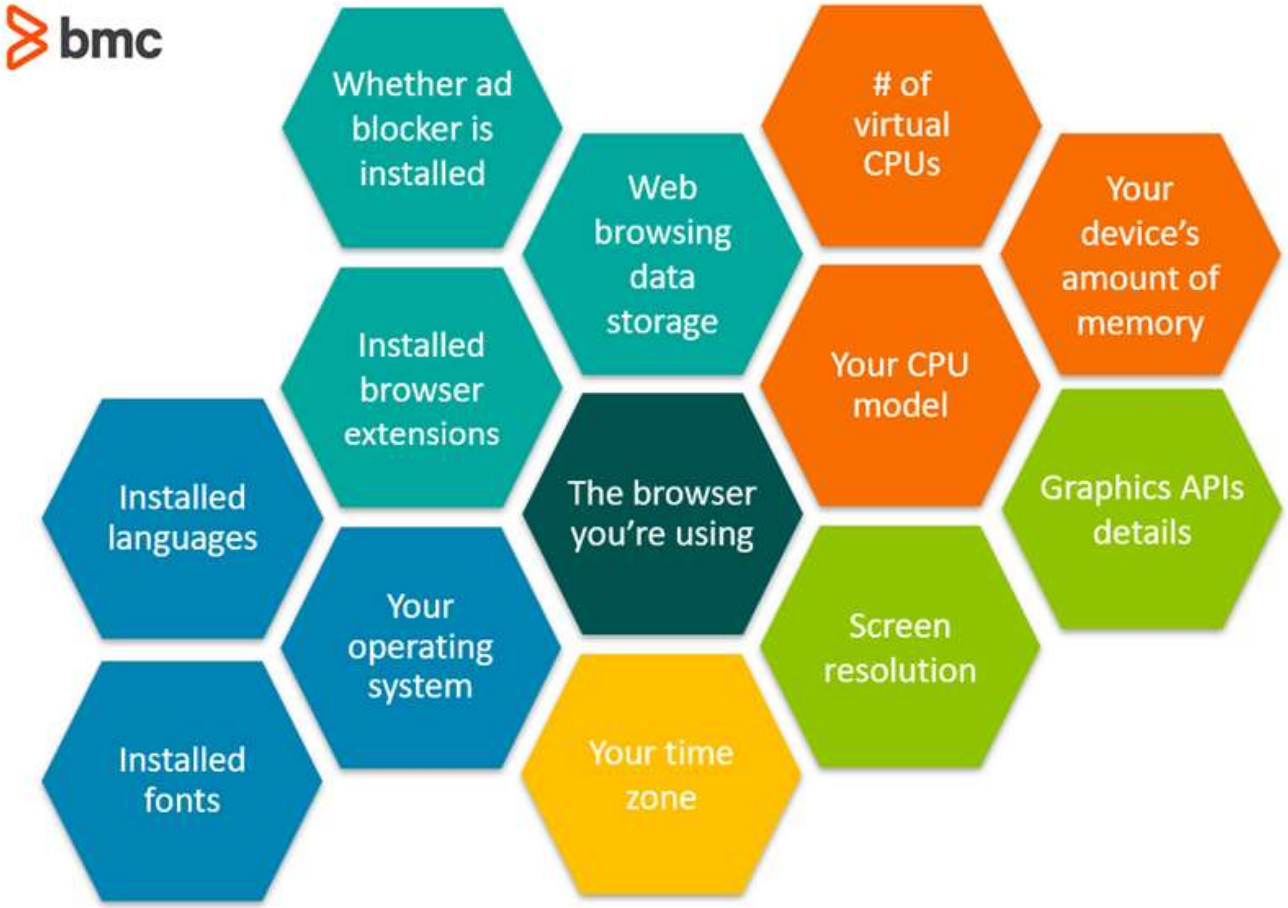
Fingerprinting is able to extract this information simply by querying what is in the browser. It does not require access to the operating system at all.

The fingerprint takes all that data, turns it into numbers, sums it, and then runs a calculation over it to yield a single value.

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, no cookies required.

Fingerprinting

To be specific, fingerprinting uses these metrics:



Select metrics that advertisers use in fingerprinting

Fingerprinting

Ad blockers, VPN's, or using TOR does NOT make you safe from fingerprinting.

None of those options change your screen resolution, browser version, etc., so they do NOT change your fingerprint.

Fingerprinting

The Brave browser has advanced fingerprinting protections that *'randomize the output of semi-identifying browser features'* and turns off features commonly used to sniff device info.

Firefox and the TOR browser also offer some protection against fingerprinting.

See *'Privacy On the Internet Part Two: Browsers and basic browser privacy settings'* for more info on the browsers.

Extended URL's

Some URL's have extra info appended that identifies you when you use the URL. An example:

https://ottawacitizen.com/life/food/cook-this-renee-kohlmans-family-favourite-cabbage-rolls/wcm/dc993f2e-7955-4aef-68c7-8518b71b9fd7

NOTE: I changed some of the gobbledegook in the above URL so it won't work

Extended URL's

This is a crude technique some websites use to track returning users and to link you to others you may have passed the URL on to.

Sometimes **you can delete the extra gobbledegook at the end of the URL and still get to the intended website without being tracked.**

Privacy On the Internet

Some of the above tracking techniques were originally developed or adopted by the intelligence community.

I've covered the well known tracking techniques, there are doubtless others we don't know about.

Privacy On the Internet

Some Reading:

Browser Fingerprints, Zombie Cookies, & the Death of Privacy
https://www.privacypolicies.com/blog/browser-fingerprints/

What Are Tracking Pixels, and How to Stop Them from Spying on You?
https://www.vpnadept.com/tracking-pixels-web-beacons/

How to Clear the Cache and Cookies in Your Web Browser
https://its.uiowa.edu/support/article/719

How to Remove Mailtrack from gmail
https://www.youtube.com/watch?v=0vGkv19T_jA

Privacy On the Internet

Some More Reading:

Fingerprinting Explained: How It Works & How To Block It

https://www.bmc.com/blogs/how-to-block-fingerprinting/

How Types of Computer Cookies Affect Your Online Privacy

https://crusolutions.com/blog/how-types-of-computer-cookies-affect-your-online-privacy

Super cookies: definition and removal (sponsored by NordVPN)

https://nordvpn.com/blog/super-cookies-going-global/

What Are Tracking Pixels, and How to Stop Them from Spying on You?

https://www.vpnadept.com/tracking-pixels-web-beacons/

You Tossed Your Cookies But They're Still Tracking You; Here's How to Hide Your Browser Fingerprint

https://www.pcmag.com/how-to/you-tossed-your-cookies-but-theyre-still-tracking-you-heres-how-to-hide

Privacy On the Internet

So this session we've looked at *some* of the ways you can be tracked.

Next session:

Part Five: Anti-tracking and ad-blocker software