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

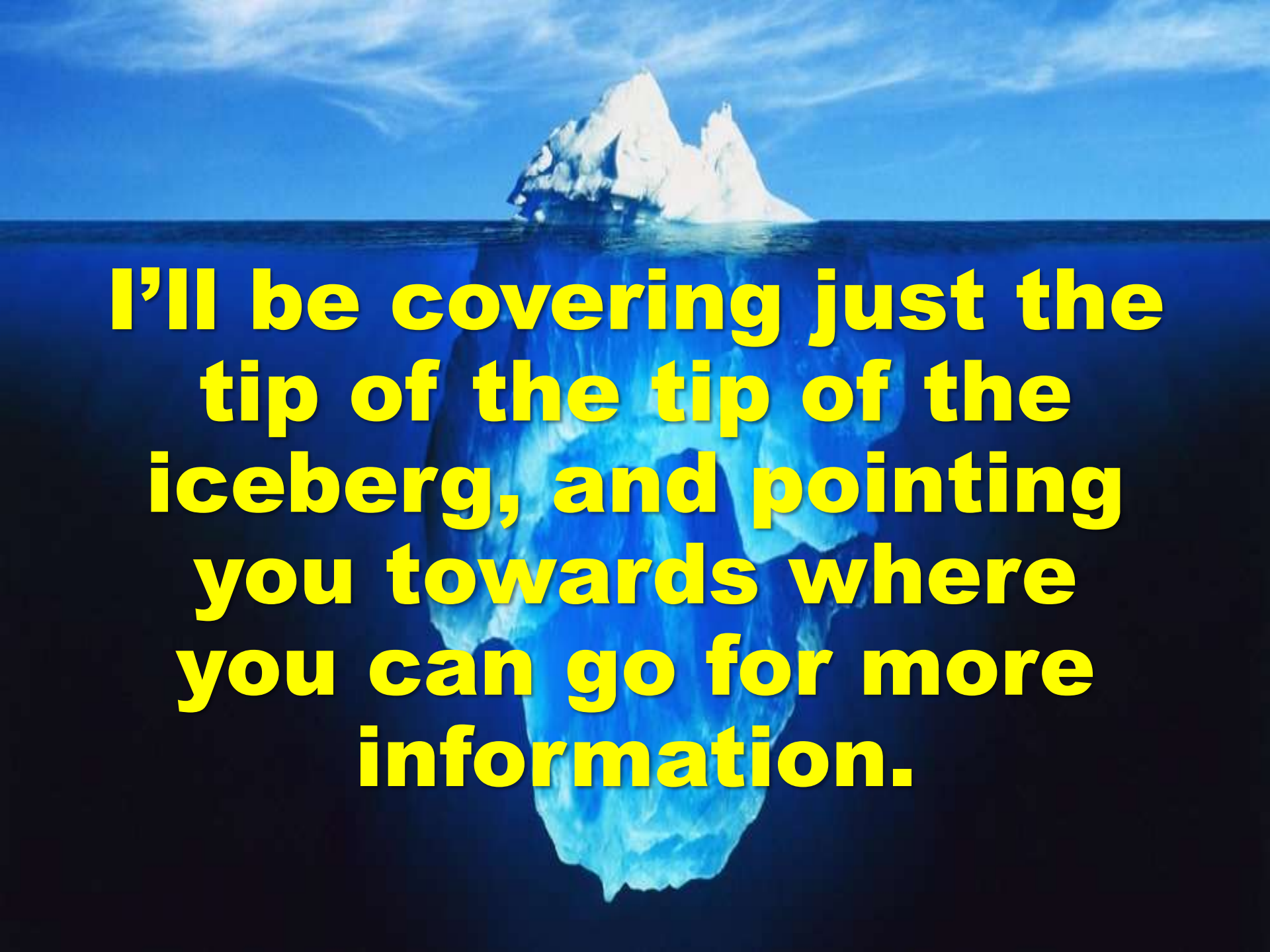
Privacy On the Internet: Browsers

Last week we looked at WHY you might want or need to guard your privacy online.

This week we'll start with the HOW by looking at BROWSERS and basic browser privacy settings.

Privacy On the Internet: Browsers

Keep in mind that your desire or need for privacy on the internet is up to you and your tolerance for having others know more about you than you would like.


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

Privacy On the Internet: Browsers

Online privacy is a major concern in the tech world, and by far the biggest privacy issues arise when you browse the internet.

Why?

Because online marketers of all stripes are keen to monetize you by following you around the web by tracking your browser activity and browser cookies, your IP address, and other device-specific identifiers ('fingerprinting').

Privacy On the Internet: Browsers

We'll cover some of the ways you can be tracked in a future Q&A, but the right browser properly set up can protect you against *some* privacy and tracking infringements.

Privacy On the Internet: Browsers

Private browsing mode, variously called Incognito mode, InPrivate, or simply Private mode, usually doesn’t really protect you against tracking.

Private browsing mode usually only hides your activities from the local machine's history so that people with access to your device (e.g. your boss or your parents) can't see where you've been on the web.

In most browsers it doesn't share cookies with the regular browsing mode, and it doesn't preserve cookies once you close it.

Privacy On the Internet: Browsers

There's a setting in many browsers called '*Do Not Track*'. This was supposed to be an easy way to opt-out of tracking, similar to how the National Do Not Call Registry was supposed to be an easy way to opt-out of telemarketing calls. Unfortunately, both efforts have failed to deliver.

There's no enforcement for Do Not Track. A website can choose to honor your setting or not, and you don't know if they are. So, we need to take other steps to limit tracking.

Privacy On the Internet: Browsers

Some browsers do a better job than others at guarding your privacy. Let's have a look at some of them.

Most of the following info comes from:

https://www.pcmag.com/picks/stop-trackers-dead-the-best-private-browsers *

and

https://www.zdnet.com/article/best-browser-for-privacy/

and

https://www.bitcatcha.com/blog/most-secure-browser/

and

https://defendingdigital.com/best-anti-tracking-software/

*** - Some of PC Magazine's testing was done using the Electronic Frontier Foundation's 'Cover Your Tracks' tool.**

Privacy On the Internet: Browsers

Other than Firefox, Tor, and Safari, most browsers including Microsoft Edge are based on a customized version of Chromium, the code that powers Google Chrome.

Brave Privacy Browser

- **Brave is a browser with an emphasis on privacy and ad-blocking, but at the same time, it lets you earn cryptocurrency while you browse.**
- **The EFF's 'Cover Your Tracks' tool reports "*strong protection against Web tracking*", and a feature called Shields blocks third-party tracking cookies and ads by default.**
- **Brave forces HTTPS (something now common among other browsers) and lets you choose between Standard and Aggressive tracker and ad blocking.**
- **Brave also has advanced fingerprinting protections that "*randomize the output of semi-identifying browser features*" and turn off features commonly used to sniff device info. Brave was the only browser for which the EFF tool reported a randomized fingerprint.**
- **Brave is coming out with its own Brave Search private search engine for use in the browser.**
- **The company has yet another new initiative called SugarCoat, designed to thwart scripts that gather your browsing data while maintaining site functionality.**
- **Platforms: Android, iOS, macOS, Windows**
- **Learn more about Shields settings and using Shields while browsing.**

Mozilla Firefox

- **Mozilla has long been at the forefront of trying to improve privacy on the web.**
- **Firefox was the first browser with a private browsing mode that could hide browsing not only from people with access to your device, but also from other sites. Firefox is an exception to the norm, in that it includes tracking protection in its Private Browsing.**
- **Firefox's Enhanced Tracking Protection's Standard setting blocks social media trackers, cross-site tracking cookies, cross-site cookies in Private Windows, tracking content in Private Windows, cryptominers, and fingerprinting. The EFF's 'Cover Your Tracks' tool reports "*strong protection against Web tracking*" at this setting. Strict mode blocks trackers hidden in ads, videos, and other site content.**
- **The fingerprinting protection currently uses a list of known fingerprint trackers, but Mozilla is working on a future update that will make the browser look more undistinguishable to thwart fingerprinting.**
- **Like some other browsers, Firefox collects what they say is "*anonymized metadata*" "*to help them make a better product*". You can manually opt-out of this data collection but they don't make this clear during install**
- **Firefox Focus is a privacy-focused browser for iOS and Android that blocks ad trackers and has a built-in ad blocker.**
- **Platforms: Android, iOS, macOS, Windows, Linux**
- **Learn more about Enhanced Tracking Protection for Firefox.**

Privacy On the Internet: Browsers

Depending on which ‘expert source’ you look at, it’s a toss up between Firefox and Brave for being the “*most private browser*”.

DuckDuckGo

- **The famed private search provider DuckDuckGo has a standalone mobile web browser.**
- **The group is also working on a DuckDuckGo desktop browser. The company hasn't yet made many details public about how it may handle issues such as fingerprinting.**
- **Until the desktop browser becomes available, you can install the DuckDuckGo Privacy Essentials extension to turn your EXISTING desktop browser into a privacy-focused piece of software. It blocks third-party trackers, switches your search engine to its own privacy-focused one, forces sites to use an encrypted (HTTPS) connection where available, and lets you see a privacy score for sites you visit. The extension raised Google Chrome's score on the EFF's 'Cover Your Tracks' tool to "*strong protection*".**
- **Platforms: Android, iOS, extension for desktop browsers**

Microsoft Edge

- **For privacy, Edge includes tracking protection at a choice of three levels: Basic, Balanced, and Strict. According to an Edge blog post, all levels block "*trackers we detect as cryptomining or fingerprinting*". But there's no attempt to make the browser appear more generic and less identifiable as some other browsers included here do. Edge also supports Secure DNS.**
- **Not in its favor, Edge does offer to personalize your advertising in Bing and Microsoft News. You can turn it off by visiting your privacy dashboard to check your settings.**
- **On the EFF's 'Cover Your Tracks' test, Edge gets a rating of "*strong protection against Web tracking*" but indicates you still have a unique, and therefore trackable, fingerprint.**
- **Platforms: Android, iOS, Linux, macOS, Windows**
- **Learn more about tracking prevention in Edge.**

Avast Secure Browser

- **Avast is one of the few browsers included here with built-in VPN functionality, but it is paid for software, so unless you get it as part of the Avast Ultimate or Avast One security packages there are free alternatives.**
- **The browser also features built-in ad blocking, anti-phishing features, and a password manager. The default search provider is tracker-in-chief Google, but you can easily switch to a more private search provider like DuckDuckGo.**
- **The EFF's 'Cover Your Tracks' tool reports "*strong tracking protection*" though with a unique (traceable) fingerprinting profile.**
- **Platforms: Android, iOS, macOS, Windows**

Google Chrome

- **Google Chrome is probably the most secure browser in terms of blocking malware, viruses, etc.**
- **Since much of Google's business is based on tracking users, Google Chrome is probably the worst at protecting your privacy, at least at its default settings.**
- **Using the DuckDuckGo Privacy Essentials extension raised Google Chrome's score on the EFF's 'Cover Your Tracks' tool to "*strong protection*".**
- **If you still want to use Chrome or another browser that doesn't offer much tracking protection, you have recourse to plug-ins that may help protect your privacy, such as the previously mentioned DuckDuckGo, Decentraleyes, PrivacyBadger, or uBlock Origin.**
- **Platforms: Android, Chrome OS, iOS, Linux, Windows**
- **Learn more about increasing Chrome security and privacy.**

The Tor Browser

- **The Tor (it stands for "the onion router") browser's slogan is "*Protect yourself against tracking, surveillance, and censorship*". It's the ultimate in privacy protection in a browser, and the EFF's privacy test reports "*strong protection against Web tracking*".**
- **It provides a multistep encrypted route for your browsing that makes identifying you very difficult. The reason it provides more privacy than a VPN is that your encrypted traffic goes through at least three nodes. The first node knows the source but not the destination of the traffic, the middle ones know neither, and the last only knows only the destination-making it nearly impossible to trace the traffic back to you. In a VPN, the VPN provider has access to both the origin (your browser) and the destination site, so you need to trust the VPN company you choose. Just as VPN exit nodes are known-which enables Netflix and the like to block people from using VPNs-the destinations know you're using Tor, but not your originating identity.**
- **The downside? It slows down your browsing, even more than a VPN would, since it goes through multiple hops between your device and the internet.**
- **If you crank up Tor to its safest level of protection and disable JavaScript, a lot of common sites won't run-basically anything that features interactive content, such as YouTube. Tor lets you access sites that use its own onion protocol that's separate from the standard web, often called the dark web, in addition to providing privacy and access to the standard web.**
- **The EFF's Cover Your Tracks tool reports "strong protection against Web tracking" but that "Your browser has a unique fingerprint." Changing the browser's privacy setting to Safest results in top protection for fingerprinting. That said, there's not much you can do on the web at that setting, since it disables JavaScript.**
- **An even more private way to run Tor is through Tails, a lightweight operating system based on Ubuntu that you run off a USB drive. Tails doesn't save any unencrypted data from your browsing session and leaves no traces on your computer's drive.**
- **Platforms: Android,Linux, macOS, Windows**

Opera

- **Opera has a long history of innovation among web browsers. The Norwegian software company was the first to include tabs and integrated search in a web browser, and an Opera developer invented CSS, just for starters. Now, it has free built-in VPN, and the company offers a gaming browser called Opera GX.**
- **PCMag's VPN experts say the built-in VPN should be called a Proxy, not a VPN. The distinction is that a standard VPN cloaks your IP address from all the traffic from your computer, while Opera's feature only applies to the browser. Opera states that it's a no-logging VPN, which is something you should look for when choosing any VPN.**
- **Opera also blocks ads and trackers by default, and the EFF's 'Cover Your Tracks' test reports "*strong protection against Web tracking*". It doesn't have specific anti-fingerprinting features, so that same test says it presents a unique fingerprint, though with the VPN/proxy feature enabled that changes to "*a nearly unique fingerprint*".**
- **With its Speed Dial and sidebar of quick-access buttons to things like messaging services and frequently visited sites, Opera still stands apart from most browsers in offering unique conveniences.**
- **Platforms: Android, iOS, macOS, Windows**

Vivaldi

- **Vivaldi, an offshoot of Opera that also uses the Chromium browser code, is the ultimate in customizability among browsers. It includes innovative features like built-in translation, split-window view, tab groups, notes, a link sidebar, and mouse gesture support.**
- **Vivaldi includes built-in ad blocking and tracker blocking, though it doesn't specifically attempt to thwart fingerprinting. As with the rest of the browser's features, privacy settings are deep, broad, and granular. The EFF's 'Cover Your Tracks' test reported "*strong protection against Web tracking*" for Vivaldi with tracking protection on, though it still reported a unique fingerprint.**
- **Platforms: Android,Linux, macOS**

Apple Safari

- **Apple was one of the first major tech vendors to raise the profile of fingerprinting as a privacy concern. The default browser for Apple devices, Safari, offers some protection against this type of tracking by presenting "*a simplified version of the system configuration to trackers so more devices look identical, making it harder to single one out*“ according to the company's documentation.**
- **Safari offers minimal settings for privacy and only gets a result of "*some protection*" and "*some gaps*" on the EFF ‘Cover Your Tracks’ test. The "nearly" unique fingerprint result, however, is better than most browsers (even Firefox), for which the test reports "*Your browser has a unique fingerprint*“.**
- **Platforms: macOS, iOS, iPadOS**
- **Learn more about increasing Safari security and privacy.**

Privacy On the Internet: Browsers

Some of the above descriptions of browsers have a link to info on privacy protection. This is not enough.

Search for "*privacy settings*" or "*privacy extensions*" for the browser you are interested in (e.g. Firefox) and look at a few of the top results (ignoring the Paid results at the top).

Privacy On the Internet: Browsers

You can also use browser plug-ins and extensions that may help protect your privacy, such as DuckDuckGo, Decentraleyes, PrivacyBadger, or uBlock Origin.

Coming Up

In upcoming Q&A sessions we'll look at:

- **Search engines**
- **Some of the ways you can be tracked**
- **Anti-tracking and add blocker software**