THE UNIVERSITY OF CHICAGO | Biological Sciences Information Security Office

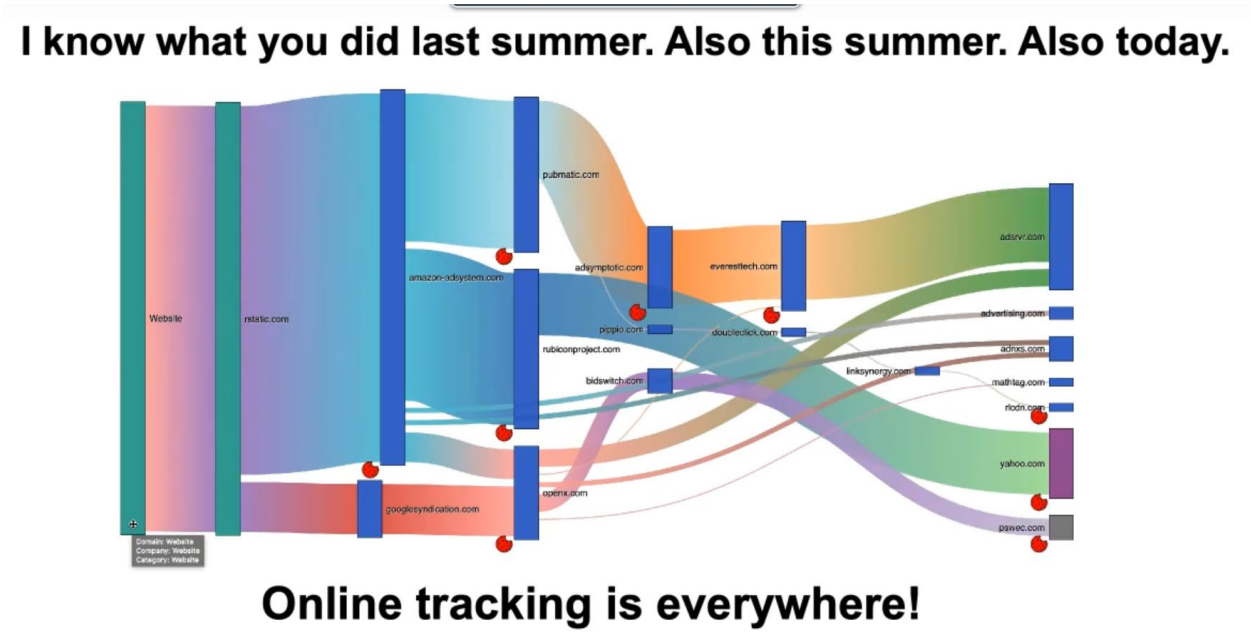
February 2022

Cyber Security Awareness Newsletter

Protecting yourself and information from cyber security threats

Data Privacy

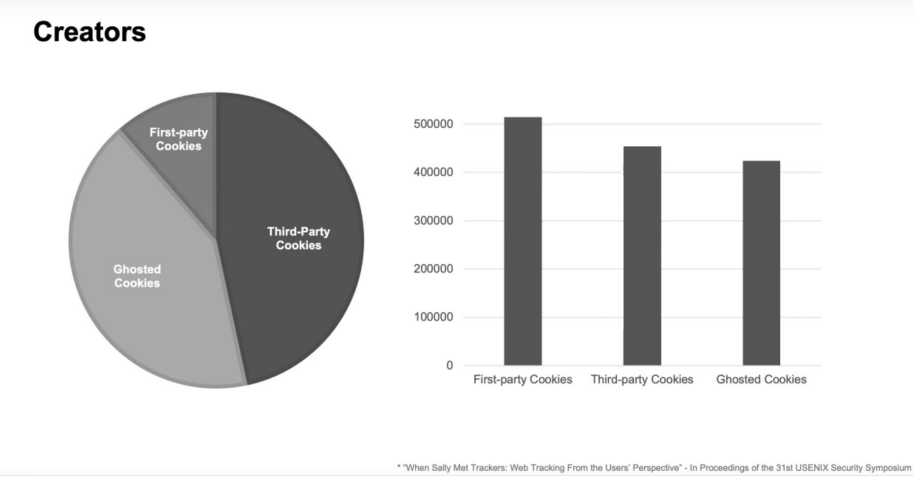
Everything we do online generates data. Data about our activities, behavior, interests, etc., is all logged by someone, somewhere. Internet service providers, search engines, online stores, streaming services, free or paid web applications, etc., all gather information when we surf the web online. It is very easy to feel like we lack control about the information being gathered about us, but there are steps we can take to learn about the types of data we are generating online, how it is collected, shared, and used by businesses, and how to prevent it from being gathered in some cases.



Data Generation and Data Collection Cookies

From the moment our web browser hits a search engine, the information we type goes to our service provider. This is where the birth of a web cookie (sometimes a web beacon or other tracker) usually starts. **What is a web cookie?** A web cookie (also known as an internet or browser cookie) is a file that contains a small snippet of code that tracks our browsing history and display ads based on this

information. Visiting a website can generate one, or lots of cookies.

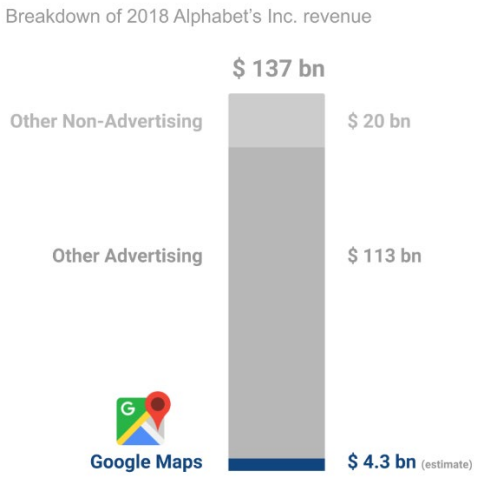


Once we type a search query, it gets sent to our search engine's database for an index of results. When we click on a link from our search results, the owners of that site also now have our information. If we click on a link from the page we visited, each business and user from the original request now has this information, and exponentially more businesses/users can potentially know what we clicked on too. This is an example of web search data generation. All the major search engines (like Google, Bing, or Yahoo) track search history and build profiles on us based on the above.

So, what kind of data is collected?

- IP Address
- Location
- Your first and last name
- Any searches you have done
- Website interaction
- Time spent on a website
- Your browser version
- Your OS version
- Activity across different websites

Each search engine has its own way of determining relevance for the results we receive, but the main factors they use are based on the above information, page content information, title tag (also known as the web browser tab description), description of the content that is normally displayed on a search result, the URL name we are visiting, other pages advertising that page (through # amount of links indexed by a search engine provider) and many more. It is important to know that this is all very valuable information. *How valuable?* Well… Google makes billions every year on its search engine and advertisements alone.



Understanding the privacy/convenience tradeoff

Before we present the mitigating and managing of privacy settings, it is important to understand and weigh the benefits we may receive in return from the data that is being gathered. Here is a short list:

Benefits	Downsides
Increased Personalization (Name, content…)	Can cause a privacy risk. (identity, hobbies, habits)
Easier device integration (Phone, car, watch, tv..)	We may not want devices to talk to each other
Easier Communication (E-mail, e-commerce, Social..)	Targeted Spam and Advertisement
Banking (apps, finances…)	If someone else uses our device they may have access.
Marketing (job finding, funding support..)	Negative reputation can haunt us.
Better relevant content online searches	We may have less control of the content we receive
Online convenience (autoform fill, relevant location…)	

Mitigating and Managing Privacy

It should be noted that our institutionally owned and managed systems may have privacy settings already in place for web browsers, and in some cases locked to a preferred protected setting. However, there are many more settings you can review on your browser of choice as well as other site owned settings. Information about managing privacy settings in web browsers, e-commerce, mobile banking, e-mail and voice communication, health applications, food delivery services, mobile/location services, online conferencing, online dating, photo and video sharing, rideshare services/scooter rental, search engines, social networks, streaming platforms and more items can be found here:

https://staysafeonline.org/stay-safe-online/managing-your-privacy/manage-privacy-settings/

Incognito/Privacy Browsing Mode

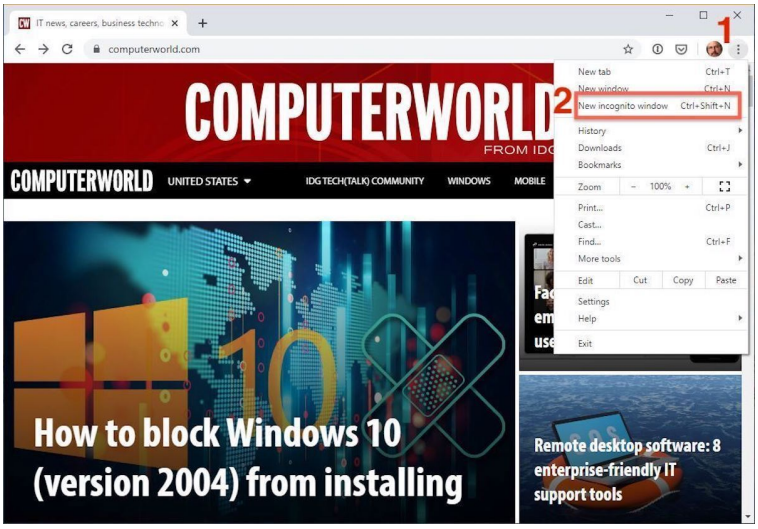
If you are looking to help protect your browsing activities or personal data from other users of your devices, private browsing can be effective.

While the exact implementation varies from browser to browser, what private browsing modes have in common is that once you close your private browsing window, your browser no longer stores the websites you visited, cookies, usernames, passwords, and information from forms you filled out during that private browsing session. Some browsers, including Safari and Firefox, offer additional protection against web trackers, but private browsing mode does not guarantee that your web activities cannot be linked back to you or your device. Notably, private browsing mode does not prevent websites from learning your internet address, and it does not prevent your employer or internet service provider from seeing your web activities by tracking your IP address.

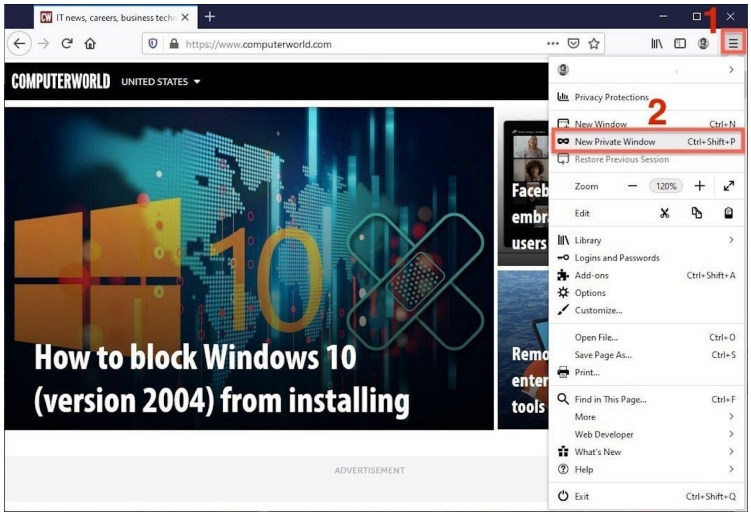
Here is how to enable private browsing mode for the most popular web browsers:

Microsoft Edge - At the keyboard, the combination of **Ctrl-Shift-N** (Windows) or **Command-Shift-N** (macOS) opens an InPrivate window. A slower way to get there is to click on the menu at the upper right -- it's three dots arranged horizontally -- and choose **New InPrivate Window** from the menu.

Google Chrome - The easiest way to open an Incognito window is with the keyboard shortcut combination **Ctrl-Shift-N** (Windows) or **Command-Shift-N** (macOS). Another way is to click on the menu on the upper right - it's the three vertical dots - and select **New Incognito Window** from the list.



Mozilla Firefox - From the keyboard, a private browsing session can be called up using the combination **Ctrl-Shift-P** (Windows) or **Command-Shift-P** (macOS). Alternately, a private window will open from the menu at the upper right of Firefox -- three short horizontal lines -- after selecting **New private window**.



Safari - To open what Safari calls a Private Window on a Mac, users can do a three-key combination of **Command-Shift-N**. Alternatively, a private window will open from the **File** menu and clicking on New Private Window.