Online Privacy

Tips For Staying Private In The Age Of Internet Surveillance

Questions? Email us: info@hamdenlibrary.org

Agenda

1. **Privacy and the web browser**
   a) Cookies
   b) Private browsing

2. **Privacy and online commerce**
   a) Privacy policies
   b) Search engines
   c) Google privacy controls

3. **Privacy and mobile devices**
   a) iOS settings and apps
   b) Android settings and apps

4. **Privacy and email: ProtonMail**

5. **Privacy and social media: Facebook**

Privacy and the Web Browser

Cookies

Cookies are small packets of data stored on your computer by your web browser. They are used by web sites to keep track of many different things, depending on the site: items in your shopping cart, login status, etc. Without cookies, many websites (particularly e-commerce sites such as Amazon) couldn't function.

There are many different types of cookies, but the main one to be concerned about from a privacy perspective are what's called "tracking cookies." These are used to track your web browsing habits. The *Wall Street Journal* found that America's top fifty websites installed an average of sixty-four pieces of tracking technology onto computers, resulting in a total of 3,180 tracking files.[30] The data can then be collected and sold to bidding corporations.

EU legislation on cookies: http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm

Hiding the Cookie Trail

There are a number of things you can do to curb the use of tracking cookies:

1. Disable cookie option - From time to time, you will visit a website that politely informs you that it uses cookies and gives you the option to disable them. This may prevent tracking, but also will usually disable certain site features, like videos. (Note that this is required for all EU-based sites since May 2018 under the new GDPR law (see: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation)

2. Enable the 'Do Not Track' option in your browser settings - This asks websites not to track you with cookies. Unfortunately, it is voluntary and websites don't have to comply.

3. Other privacy and security settings that are more browser-specific. For example, Safari has an option to prevent cross-site tracking. Google Chrome has options that mainly involve turning off Google-based analytics and tracking services. See this Wired article for details: https://www.wired.com/story/how-to-lock-down-websites-permissions-access-webcam/

Private Browsing

Web browsers have recently implemented a feature called private browsing (in Chrome this is known as “incognito”). While browsing privately, your search history and any cookies and other data aren't saved in the browser. This means that nobody else using your computer will be able to see what websites you visited.

However, private browsing does nothing to stop websites from tracking you. If you do a Google search while browsing privately, Google will still be able to keep track of your searches.

Search Engines

Google and search engines like it keep track of your search results for two main reasons:

- To improve your experience by tailoring the results specifically to you
- To learn about your preferences to target specific advertisements at you

What can you do about it? There are two ways to go:

If you want to keep using Google you can go into your Google Account settings and turn off a lot of the tracking features. For maximum privacy:

- Turn off (Pause) all Google activity controls
- Turn Off Ad Personalization
- Remove Geo-tags in shared Google Photo links

You can use a different search engine that prioritizes privacy like DuckDuckGo.com or Startpage.com

Duckduckgo.com

Search engine doesn't track users. Gets its search results from over 400 sources, including its own webcrawler (https://help.duckduckgo.com/duckduckgo-help-pages/results/sources/)

Has a browser extension (DuckDuckGo Privacy Essentials) and a mobile app (DuckDuckGo Privacy Browser) that grades each website with a privacy rating ("A" is best) and blocks tracking cookies.

Has a blog that focuses on online privacy issues. (https://spreadprivacy.com/)

Duckduckgo makes money from (non-targeted) advertising and affiliate revenue. Affiliates include Amazon and eBay. When a user visits one of those sites from DuckDuckGo and makes a purchase, DuckDuckGo makes a small commission. This mechanism operates anonymously and there is no personally identifiable information exchanged between DuckDuckGo and Amazon or eBay. (https://help.duckduckgo.com/duckduckgo-help-pages/company/advertising-and-affiliates/)

Startpage.com

Search engine pays Google to use their search results but doesn't track users.

Doesn't offer apps but does have an optional "Privacy view" that allows users to visit other websites without being tracked. It works well but is slower because it uses a proxy server. In addition, logging in and sending information (i.e. filling out forms) is disabled while in privacy view.

Owned by a private Dutch company. They take privacy so seriously, they don't reveal the last names of their employees!

Also makes money (99% of their profits, according to their website) from non-targeted ads.

Google Privacy Controls

Turning off data tracking:

1. Login to Google and Click on the “Google Account” button.
2. Go to Personal Info & Privacy and click on “Manage Your Google Activity”
3. Go to “Activity Controls”
4. Turn off all the monitoring activity's that you want; they should say “Paused” if off
5. Google should stop tracking them from that point on

You can also use Google’s “Privacy Checkup” feature to go through and see what your settings are on your account. The Checkup will review the privacy settings in your Activity Controls, Google Photos page, the public About You section of the account, and Ad Personalization settings. You can change these settings by following the links in the checkup screen.

Mobile Privacy - iOS

You can take steps to increase your privacy on iPhone and iPad. Open the Settings app and scroll down to find the Privacy settings. You can decide whether you want Location Services to be on or off, and which apps are allowed to access your location. You can also decide which apps, if any, have access to your contacts, calendar, microphone, camera, photos and more.

In addition, you can increase your privacy by using the Safari browser to access sites like Facebook instead of using the Facebook app. Safari privacy settings can be set to disallow cross-site tracking and can ask websites not to track you. Safari also has Apple's Intelligent Tracking Prevention (ITP), which tries to limit the amount of tracking that can be done by advertisers.

You can also download the DuckDuckGo Privacy Browser from the Apple Store. It works just like the browser extension on desktop.

Mobile Privacy - Android

Android was developed by Google, so many of the privacy controls for Android devices are accessed through your Google account, which we will look at later.

However, when it comes to controlling what various 3rd party apps have access to, you should go to Settings and select Apps & Notifications, then scroll down and tap App permissions. This will give you a list of all available access permissions, from sending or receiving SMS messages to using your phone's microphone and camera. Tap into each to see which apps have these permissions, and individually withdraw them if you see fit.

You can also download the DuckDuckGo Privacy Browser from the Apple Store. It works just like the browser extension on desktop.

Privacy Policies

Most companies that operate a website have a Privacy Policy in place in order to inform you about how the data you give to them is stored, what it is used for, who has access to it, and if the website shares or sells that data to anyone.

In general, privacy polices are useful for finding out if a company is sharing/selling your data (these policies will rarely fully disclose *who* your data is being shared with due to how often data relationships between companies change), and what they are using it for.

Often when you are creating an account you must read (most people skip through) the website's privacy policy. During this part of the sign-up process the company will sometimes have optional checkboxes enabled that allow you to opt out of some of their data tracking procedures.

Privacy policies tend to be very long and loaded with legalese making reading through them a long and tedious process.

https://www.condenast.com/privacy-policy

ProtonMail - Free encrypted email

Most companies who provide free email services are not doing so out of the goodness of their hearts. They want to make money, and they do so by gathering data about you and selling it to advertisers.

ProtonMail is a free alternative email service that uses end-to-end encryption to ensure that nobody (even ProtonMail themselves) can read your emails. Even if you don't care about the extra security provided, you also won't get any ads and you won't have Google or another big company looking at your data and selling it to third parties.

The downside to ProtonMail is that storage is limited for free accounts to 500MB. But with judicious pruning, that should be more than enough space for most personal email accounts.

Privacy and Facebook

Social media is inherently not geared toward privacy. However, there are some steps you can take to make sure you're only sharing what you want to share, and only with those you wish to share it with.

For example, on Facebook, go to Settings and select Privacy. From here, you can choose who can see your posts, who can send you friend requests, who can see your friends list, who can look you up using your email address or phone number, and whether search engines can link to your profile.

You can also go to Timeline and Tagging to control who can post on your timeline, who can see what others post on your timeline, who can see posts you're tagged in, and decide whether to review posts you're tagged in and any tags people add to your posts.

Privacy and Facebook, continued

Still in Settings, the Location tab lets you control whether Facebook can track the full history of precise locations you've been using geotagging data. They say that this information is private.

Next, there is Face Recognition. This is again a simple on/off switch. If it's on, Facebook will try to automatically detect your face in photos or videos uploaded to Facebook. If it's off, it won't do that.

Facebook and Ads, Pt. 1

If you click on Ads in the Settings menu, you'll be taken to an entirely new page in which you can view and edit your ad preferences.

Before we go through these settings, it makes sense to pause here to explain exactly how Facebook uses the data they've collected about you to make money. Facebook doesn't sell your data. Instead, what it sells is access to your News Feed. Advertisers buy ad space targeted to Facebook users with specific interests or demographics. Facebook will then display the ad in the News Feed of users who match the interests/demos that the advertiser is trying to reach. (https://www.recode.net/2018/4/11/17177842/facebook-advertising-ads-explained-mark-zuckerberg)

There is no setting or preference that will stop Facebook from selling ad space in your News Feed or from using the data in your profile and in every interaction you make on Facebook to sell that ad space. The only method that works is to delete your account and stop using Facebook.

Facebook and Ads, Pt. 2

Now that you understand how Facebook makes money, you can see why the “Ad Preferences” page is designed to give you control over what ads you will see, rather than control over what information Facebook can see about you.

The first tab on this page is called “Your interests.” Anything you’ve liked or commented on in Facebook - websites, products, services, celebrities, films, books, or almost anything else - can show up here as something you’ve indicated that you’re interested in. Here you can individually remove each one of these interests, which may take some time.

The next tab is “Advertisers you’ve interacted with.” This has several subcategories: “Who use a contact list added to Facebook,” “Whose website or app you’ve used,” “Whom you’ve visited,” “Whose ads you’ve clicked” and “Whom you’ve hidden.” You may be surprised how many companies have you on their contact lists. Again, you can remove these individually, but it would take a while.

Next on the Ad Preferences page, we have “Your information”. Facebook lets you manage whether they can show you ads based on four profile fields: relationship status, employer, job title and education. These are obviously very limited because, again, Facebook needs to make money and they couldn’t do so if they couldn’t promise access to users with specific interests and demographics.

Finally, we come to “Ad settings.” Essentially, none of these settings affects what information Facebook has about you. The only thing they affect is whether you allow them to use the information they already have to show you more targeted ads or not.

Further resources

Goodwill Community Foundation's Privacy Tutorials: https://edu.gcfglobal.org/en/internetsafety/understanding-browser-tracking/1/

https://edu.gcfglobal.org/en/internetsafety/social-media-privacy-basics/1/

Facebook Advertising Explained: https://www.recode.net/2018/4/11/17177842/facebook-advertising-ads-explained-mark-zuckerberg

Google Privacy Policy: https://policies.google.com/privacy?hl=en

Electronic Frontier Foundation's Panopticlick tool: https://panopticlick.eff.org/

Wired - How To Lock Down What Websites Can Access On Your Computer: https://www.wired.com/story/how-to-lock-down-websites-permissions-access-webcam/