

5 Ways to Curb Google's Data Sharing

So, Google isn't the Skynet of our nightmares, (... yet) but you still should be careful. As amazing as Google services are, they still come at a cost to your privacy, and they can become very invasive. With all of the services and products Google provides: Search, Maps, Gmail, Drive, Chrome, and more, it has the ability to collect so much information about you and use it to target ads from third parties or to train its artificial intelligence systems. This seems harmless now, but this could reach a point where Google knows more about you than you do, which opens up the possibility for them to abuse this data to convince you to buy or do things you normally wouldn't do. Even if you've read about these dangers before, it's likely you didn't quit Google, because, let's be honest; its services are very useful. Articles may keep telling you that this situation is horrible and there's nothing you can do, but the good news is that there is. Check out these five steps you can take today to protect yourself from Google's third-party data sharing. Most of these steps will involve going through Google's settings page at myaccount.google.com.

1. Turn off Ad Personalization

In this step, you will turn off Google's service that recommends advertisements to you based off your information. You'll still get ads, but Google will not use your data to learn what it should show you. To turn this setting off:

- Go to your Google account settings page
- Click on "Personal info & privacy" in Google's account settings page and then click on "GET STARTED" under "Privacy Checkup".
- Go to the end of the list, you will find the 6th item called "Make ads more relevant to you".
- Click on "MANAGING YOUR AD SETTING" to turn off Google's ad personalization.

Those steps are all it takes to put yourself in a much better position to keep Google from using your data for advertising. The next steps will focus on preventing Google from having that information in the first place.

2. Check “Activity Controls” page

Now, if you go back to Google’s “Personal info and privacy” page, you will see a “GO TO MY ACTIVITY CONTROLS” link under the “Manage your Google activity” page. On the resulting page, you will find the kind of data that Google tracks. The list includes web and app activity, location history, device information, voice and audio activity, YouTube search history, and YouTube Watch History. There is a toggle for each of these where you can turn them off to stop Google from collecting each kind of information, which now means you can be sure that the data cannot be used or provided to third-parties. The goal is to have all of them turned off, but it may limit you from certain Google services. The best way to go about this is to turn them all off and only turn one back on if it prevents you from using a Google service you really need.

3. My Activity and Timeline

So now that you have turned off whatever data collection you want, you’ll want to remove any data that Google has on you that you do not want. To do this, go back to the “Personal info and privacy” page and click on the “GO TO MY ACTIVITY” link, which will be under the “GO TO ACTIVITY CONTROLS” link. There, you will find all of the information that Google has about you from the controls mentioned in step two. From there, you can click on the three dots in the top right-hand corner to delete the activity data by type, date, or all of it. In addition, you can delete individual items in the list that is provided on the page.

There is one piece of info that you will not find here, which is a map of your location data. To get this, click on “Other Google activity”, on the left-hand side, and then click “View Timeline”. This is

arguably the coolest and scariest page because it will show you every address Google has that you have been to. Don't worry though, you can delete all of this information by clicking the trash can icon in the bottom right.

4. Block trackers in your browser

These next few steps are things you can do outside of Google's account control center to help protect yourself from their third-party sharing network. The main way companies, like Google, track users across the internet is by using cookie trackers. Some browsers, like Firefox, can block these trackers on their own. Just go to their settings page and turn on any tracker blocker and/or third-party cookie blocker settings that you can find. Be careful, though, as this may cause some websites to not work properly, and you will have to allow cookies for those sites if problems arise. To avoid some of these issues, you can install a browser add-on to do this protection for you. Most major browsers, including Firefox and Chrome have a browser add-on webstore. Search for how to get to it and download "Privacy Badger" or "Disconnect". Both will do a good job, but "Privacy Badger" is a good one to try first due to the fact that it is managed by a reputable non-profit.

5. Protect Your Searches

Another easy thing you can do is to be logged out of your Google account when you make searches online. This can be done in a few ways. First, you can log out of your Google account whenever you're done using its services or set the login page to not keep you logged in after you exit. Second, you can use a different browser or private tab to perform the search. Another way you can protect your searches from being used in third-party data sharing is to use a different search engine. Now I know that sounds crazy, but there are good private focused alternatives available. One notable one is DuckDuckGo, which was made to be a non-tracking version of Google search. It isn't as good as Google, but it definitely gets the job done.

Bonus

For those that want to go a little further, there is a way for you to download your Google data. You can find this setting on Google's "Personal info and privacy page" under "Download or transfer your content". Click "CREATE ARCHIVE" and follow the steps to get a zip download of the Google account information that you want to see. From there, you can then unzip the file and have fun seeing all of the weird and interesting information that Google may have about you. Depending on how much information is in your account, it may take some time for it to be ready and downloaded to your computer, but Google will send you an email when it is ready.

Hopefully, now you have more confidence in your ability to protect yourself online, and definitely explore more settings for Google and other companies, such as Facebook, Snapchat, and Microsoft, if you can. You'll be surprised with what you may find. However, even if these five steps are the only things you do, you will be in a much better position.

Works Cited

- www.google.com (accounts page is what the instructions refer to)
- disconnect.me (add on suggested)
- www.eff.org/privacybadger (add on suggested)
- duckduckgo.com (search engine suggested)