MATT BURGESS   SECURITY   JAN 3, 2022 7:00 AM

6 Ways to Delete Yourself From the Internet

You'll never be able to get a clean slate—but you can significantly downsize your digital footprint.

PHOTOGRAPH: CAROL YEPES/GETTY IMAGES

DEPENDING ON WHEN you were born, there's a good chance you've spent either several decades online or have never known an offline world. Whatever the case, the internet and its advertising giants know a huge amount about your life.

Amazon, Facebook, and Google all have reams of data about you—including your likes and dislikes, health information and social connections—but they're not the only ones. Countless murky data brokers that you've never heard of collect huge quantities of information about you and sell it on. This data is then used by other companies you've likely never heard of to nudge you into buying more stuff. On top of that, all your ancient web forum comments and ill-advised social media posts are still out there, waiting to turn you into a milkshake duck.

At this stage it's going to be very difficult to completely delete yourself from the internet, but there are some steps you can take to remove a lot of it. Removing personal information and deleting accounts is a fiddly process, so it's better to break it down into a few smaller steps and tackle them over time.

Opt Out From Data Brokers

Collecting and selling your data is big business. In 2019 the US state of Vermont passed a law requiring all companies buying and selling third-party personal information to register: In response, more than 120 firms logged their details. They included companies building search tools to look up individuals, firms handling location data, and those specializing in your health data. These companies collect everything from your name, address, and date of birth to your social security number, buying habits, and where you went to school and for how long.

Among the biggest data brokers are Acxiom, Equifax (yes, that one), Experian, Oracle, and Epsilon. Some, but not all, data brokers let people opt out of having their personal information processed—this also depends on where you are in the

world—but the process isn't straightforward. You'll often have to contact them via email, fill in online forms, and provide extra identification information.

The US-based nonprofit Privacy Rights Clearinghouse has created a database of data brokers that contains their email addresses, links to their privacy policies, and info about whether they let you opt out. There are 231 US companies on the list, which gives you an idea of how big the data brokerage industry is.

If you're covered by Europe's GDPR or California's Consumer Privacy Act, you can also send requests for your data to be deleted. Privacy-focused group YourDigitalRights has created opt-out forms for 10 of the biggest data brokers to speed up the process of getting your information deleted. It's probably best to start opting out of the biggest companies first.

Get Google Search Results Updated

You can't change the way that Google displays its search results, but there are some limited steps you can take to make sure that what's displayed is up to date and to remove harmful details, such as doxing attempts. If a web page has been updated by its owner but it isn't reflected in Google's search results, you can use its tool to remove outdated content. Google will update its search results for pages that no longer exist or are significantly different to the versions it has indexed previously.

Google will also consider requests to remove harmful content. If there are non-consensual explicit images; fake pornography; financial, medical, or national ID data; doxing; or images of children on websites then you can ask for them to be removed. To do so, you'll have to submit a form and provide evidence of the content.

There's also the Right to be Forgotten, a principle that was established in European courts in 2014 and was incorporated into GDPR in 2018. This allows certain specific information to be removed from search results, including Google, when relevant criteria are met. Generally, if information about you is in the public interest then it will be very difficult to get it removed from search results.

Delete Old Online Accounts

There's no real shortcut to finding and deleting accounts that you don't use anymore. But if you really want to minimize your online presence then you need to track down those old Myspace and Tumblr accounts and remove all traces of them. For that you're going to need a web browser—preferably on a laptop or desktop—and a good chunk of time.

Start by making a list of all the old accounts you remember using—email addresses and usernames you've used can be helpful—and then work through them one by one. For each you'll need to sign in or recover the account and navigate through the deletion process. As a handy starting point, Justdelete.me has a list of links that point to the deletion pages of everything from Gumtree to Vimeo.

If your list of accounts to delete is running short, then it's worth checking saved logins in your password manager or browser to refresh your memory. Alternatively, you can search your inbox for old subscriptions and online accounts. Entering your email or phone number into the data-breach-notification service Have I Been Pwned? will trawl more than 500 data beaches for your details and is also likely to remind you of some obscure old accounts you've forgotten about. You'll still have to do the hard work of shutting down the accounts, though.

You should also search for your name online and combine it with some other pieces of personal data—for instance your email address or where you live—to see what comes up. If you're diving deep into your online history and attempting to remove old posts on forums or similar services you may have to email web administrators. If the contact details aren't clear, as might be the case with really old pages, one starting point is to check the web registration details through a WHOIS lookup. Alternatively, if the Wayback Machine has archived the page you're looking for it may have preserved old contact details.

There are some dedicated services that will attempt to look for and delete your old accounts by scanning your emails. But it's often unclear how they're using your data—the parent company of email unsubscription service Unroll.Me was found selling user data in 2017—so it's best to avoid them if you can.

Clean Up Your Digital History

Even if you're not deleting your online accounts you can still clean up what data you store online. It's likely your email account contains thousands of old messages (and attachments) dating back years; your Facebook and Twitter accounts might still have posts on them that you'd rather didn't resurface publicly.

We've run down some of the best ways to clean up your digital health here. But if you're using Gmail you can bulk-delete old messages by using the search command "older_than:" and adding a time period (1y or 6m, for instance), and then selecting all messages and deleting them.

Publicly posted data—either photos or text—is obviously far more likely to be found by others. If you're considering making the plunge and deleting your current profiles or existing posts, consider downloading and backing up your posts first. Almost all major social media platforms have backup options in their settings.

Twitter doesn't have any tools to easily delete all your old tweets in bulk, but third-party services do. Both Tweet Deleter and TweetDelete will get rid of your old tweets. If you're deleting in bulk, both services can be a little glitchy when handling years of data. Forking out TweetDeleter's monthly $5.99 cost—you can cancel after one month—may be worth it to delete an unlimited number of tweets at once. Keep in mind that by allowing any third-party service access to your online accounts, they may be able to access information stored within them, such as your direct messages. Both company's privacy policies detail what they do with your data. Alternatively, if you just want to delete your Twitter account entirely you'll need to follow these steps.

Google doesn't index your individual Facebook posts, so they won't show up in its search results. But if you're trying to remove as much of your history from the internet as possible you should also delete your old posts or at least stop people from seeing them. In Facebook head to **Settings & privacy**, **Activity log** and select the type of activity you want to delete—ranging from posts, to photos you're tagged in. The tool isn't the most streamlined if you want to delete years of Facebook usage, but as with all efforts to wipe yourself from the internet you'll get better results if you spend more time doing it. Alternatively, you can just delete your Facebook account entirely.

Go Nuclear

A lot of the ways to remove yourself from the web are time-consuming and involve a lot of paperwork. There may be some instances where you may want to try to speed things up a little or use legal muscle. It may be sensible to seek legal advice and help removing your data from the web if it involves defamatory statements, explicit photographs, and other harmful content.

While you should treat any third-party data-removal service with caution—make sure you read their privacy policies before using them—there are some paid options for helping remove yourself from the web. DeleteMe will try to remove your data from data brokers selling your information, for example. And Jumbo can alert you to data breaches and automatically delete new social media posts after a certain number of days.

Future Protections

It's pretty much impossible to keep your data off the internet entirely, but there are some steps you can take going forward. First, consider how much information you want to proactively put online. When you're signing up for new online accounts, consider whether you need to enter your personal details or whether it would be better to use a burner account to mask your identity.

Where possible avoid using Big Tech for all your online activities. Pick a web browser and search engine that don't collect your data; use end-to-end-encrypted apps and disappearing messages when appropriate; and understand what data WhatsApp, Instagram, Google, Amazon, Spotify and others collect about you.

Finally, it's not just on you. If you're keen to be invisible online then you should also consider discussing your position with friends and family. Most people are likely to be considerate to requests not to post your photo or location on social media. After all, the head of Google's smart speakers has said people should disclose whether they have the devices when guests visit their homes.

More Great WIRED Stories

- ✉️ The latest on tech, science, and more: Get our newsletters!

- [Amazon's dark secret](#): It has failed to protect your data
- Need to [test a space suit](#)? Head to Iceland
- [This digital bank](#) is designed for the LGBTQ+ community
- Picture-perfect ["graze boxes"](#) are taking over Facebook
- Hacker Lexicon: What is a [watering hole attack](#)?
- 👁 Explore AI like never before with [our new database](#)
- 📱 Torn between the latest phones? Never fear—check out our [iPhone buying guide](#) and [favorite Android phones](#)

[Matt Burgess](#) is a senior writer at WIRED focused on information security, privacy, and data regulation in Europe. He graduated from the University of Sheffield with a degree in journalism and now lives in London. Send tips to Matt_Burgess@wired.com.

SENIOR WRITER   𝕏

TOPICS   PRIVACY   DATA   PASSWORDS   SEARCH   HOW-TO

MORE FROM WIRED