The New York Times

Everyone Wants Your Email Address. Think Twice Before Sharing It.

Your email address has become a digital bread crumb for companies to link your activity across sites. Here’s how you can limit this.

By Brian X. Chen

Brian X. Chen is the lead consumer technology writer for The New York Times.

Jan. 25, 2023, 5:00 a.m. ET

When you browse the web, an increasing number of sites and apps are asking for a piece of basic information that you probably hand over without hesitation: your email address.

It may seem harmless, but when you enter your email, you’re sharing a lot more than just that. I’m hoping this column, which includes some workarounds, persuades you to think twice before handing over your email address.

First, it helps to know why companies want email addresses. To advertisers, web publishers and app makers, your email is important not just for contacting you. It acts as a digital bread crumb for companies to link your activity across sites and apps to serve you relevant ads.

If this all sounds familiar, that’s because it is.

For decades, the digital advertising industry relied on invisible trackers planted inside websites and apps to follow our activities and then serve us targeted ads. There have been sweeping changes to this system in the past few years, including Apple’s release of a software feature in 2021 allowing iPhone users to block apps from tracking them and Google’s decision to prevent websites from using cookies, which follow people’s activities across sites, in its Chrome browser by 2024.

Advertisers, web publishers and app makers now try to track people through other means — and one simple method is by asking for an email address.

Imagine if an employee of a brick-and-mortar store asked for your name before you entered. An email address can be even more revealing, though, because it can be linked to other data, including where you went to school, the make and model of the car you drive, and your ethnicity.

"I can take your email address and find data you may not have even realized you've given to a brand," said Michael Priem, the chief executive of Modern Impact, an advertising firm in Minneapolis. "The amount of data that is out there on us as consumers is literally shocking."

Advertising tech is continuing to evolve, so it helps to understand what exactly you're sharing when you enter in an email address. From there, you can decide what to do.

Your email address has become a potent piece of data.

For many years, the digital ad industry has compiled a profile on you based on the sites you visit on the web. Information about you used to be collected in covert ways, including the aforementioned cookies and invisible trackers planted inside apps. Now that more companies are blocking the use of those methods, new ad targeting techniques have emerged.

One technology that is gaining traction is an advertising framework called Unified ID 2.0, or UID 2.0, which was developed by the Trade Desk, an ad-technology company in Ventura, Calif.

Say, for example, you are shopping on a sneaker website using UID 2.0 when a prompt pops up and asks you to share your email address and agree to receive relevant advertising. Once you enter your email, UID 2.0 transforms it into a token composed of a string of digits and characters. That token travels with your email address when you use it to log in to a sports streaming app on your TV that uses UID 2.0. Advertisers can link the two accounts together based on the token, and they can target you with sneaker ads on the sports streaming app because they know you visited the sneaker website.

Since your email address is not revealed to the advertiser, UID 2.0 may be seen as a step up for consumers from traditional cookie-based tracking, which gives advertisers access to your detailed browsing history and personal information.

"Websites and apps are increasingly asking for email authentication in part because there needs to be a better way for publishers to monetize their content that's more privacy-centric than cookies," Ian Colley, the chief marketing officer of the Trade Desk, said in an email. "The internet is not free, after all."

A New Direction for Tech Fix
Our tech problems have become more complex, so Brian X. Chen has rebooted his column to focus on the societal implications of the tech we use.

However, in an analysis, Mozilla, the nonprofit that makes the Firefox web browser, called UID 2.0 a "regression in privacy" because it enabled the type of tracking behavior that modern web browsers were designed to prevent.

There are simpler ways for websites and apps to track your web activity through your email address. An email could contain your first and last name, and assuming you've used it for some time, data brokers have already compiled a comprehensive profile on your interests based on your browsing activity. A website or an app can upload your email address into an ad broker's database to match your identity with a profile containing enough insights to serve you targeted ads.

The bottom line is that if you're wondering why you are continuing to see relevant ads despite the rise of privacy tools that combat digital tracking, it's largely because you are still sharing your email address.

So what to do?

There are various options for limiting the ability of advertising companies to target you based on your email address:

- **Create a bunch of email addresses.** Each time a site or an app asks for your email, you could create a unique address to log in to it, such as, for example, netflixbrianchen@gmail.com for movie-related apps and services. That would make it hard for ad tech companies to compile a profile based on your email handle. And if you receive spam mail to a specific account, that will tell you which company is sharing your data with marketers. This is an extreme approach, because it's time-consuming to manage so many email addresses and their passwords.
- **Use email-masking tools.** Apple and Mozilla offer tools that automatically create email aliases for logging in to an app or a site; emails sent to the aliases are forwarded to your real email address. Apple's Hide My Email tool, which is part of its iCloud+ subscription service that costs 99 cents a month, will create aliases, but using it will make it more difficult to log in to the accounts from a non-Apple device. Mozilla's Firefox Relay will generate five email aliases at no cost; beyond that, the program charges 99 cents a month for additional aliases.
- **When possible, opt out.** For sites using the UID 2.0 framework for ad targeting, you can opt out by entering your email address at https://transparentadvertising.org. (Not all sites that collect your email address are using UID 2.0, however.)

You could also do nothing. If you enjoy receiving relevant advertising and have no privacy concerns, you can accept that sharing some information about yourself is part of the transaction for receiving content on the internet.

I try to take a cautious but moderate approach. I juggle four email accounts devoted to my main interests — food, travel, fitness and movies. I’ll use the movie-related email address, for example, when I’m logging in to a site to buy movie tickets or stream videos. That way, those sites and apps will know about my movie preferences, but they won’t know everything about me.