



## Don't part with more data than you need to

Consider this: Data brokers you've probably never heard of hold up to 1,500 individual pieces of data for around 10% of the world's population, says Ray Walsh, a digital privacy expert at ProPrivacy.com.

"That is a staggering amount of data, and data brokers are constantly in the process of acquiring that data in order to sell it to third parties for a profit," he says. "Consumers often willingly part with more data than they strictly need to. This is unwise because once that data has been uploaded, it is potentially going to disseminate further afield."

## Minimize your exposure

Apps on your mobile device are spying on you, compiling information about your behavior, habits and movements. So don't download every single app that catches your eye.

Still want to check out new apps but don't want them tracking you? Buy a cheap, secondhand pay-as-you-go phone and download them there.

## Use an alias

You usually have to cough up an email address and phone number when signing up for [internet services](#). But there's a workaround there, too. Use an alias email address and a forwarding phone number. If you really want to go undercover, don't use your real name, only a pseudonym.

"Using a secure private email service that provides disposable alias email addresses is a great way to sign up to a service and receive an email without having to provide your primary email address," Walsh says.

The same goes for services such as Google Voice. "By using a temporary phone number that forwards an SMS to your real phone, you can sign up to services without having to divulge your real phone number," he says. "This will massively reduce the potential for your real phone number and email to be disseminated online to data brokers."

## Cut out the middleman

When making online purchases, shoppers often reflexively reach for PayPal, Walmart Pay and Google Pay. But involving a third party in your transaction isn't the savviest privacy move, Walsh says. Now the bank, the store and the app can all collect your information and track your purchases.

Is that so bad? It depends. Third parties can get a pretty good idea of your income and spending power. They can also create a database of your purchases and potentially sell your data to insurance companies, mortgage brokers or any other firms interested in you. Walsh says if a purchase is important or sensitive, use cash.

## Location, location, location

Location data is very valuable to businesses snooping on you. Refuse GPS data tracking by apps whenever possible, Walsh says.

"If apps have invasive permissions that allow it to access your contacts, photo roll, and sensitive device data including your location, think twice before installing that app," he says.

## Don't tell Facebook and Instagram everything

When you join a social media platform like Facebook or Instagram, you have to provide your real name, [email address](#), gender and date of birth. Beyond that, you don't have to tell Facebook any other details about your life, not your mobile phone number or where you live, what movies you like or who you're in a relationship with.

Think twice about what information you provide, Walsh says. Even your likes can be used to infer sexual preferences, religious beliefs and political affiliations.

And, technically it's against Facebook's rules to use a pseudonym, but doing so could also help obscure your identity, Walsh says.

"The best way to use Facebook is to be hyper-aware that Facebook is always watching in the background, and that anything you post is being harvested by the company," he says. "If you provide photos of yourself with a person, Facebook

facial recognition will know you have spent time with that person. If you provide your phone number in a private message, Facebook now has your [phone number](#). So, if you don't want Facebook to find out sensitive details about you, it is vital that you never share those details on the platform, anywhere."

## Invest in privacy

There's a tired adage in the tech world: If you aren't paying for the product, you are the product. Free mobile apps, [social media](#) platforms and giant online retail operations are all costly to build and maintain, so they make money off your data.

A good way to give them the slip: Pay for the services you can afford to, such as email and cloud storage. Walsh says there are a growing number of secure private email providers that use end-to-end encryption including Posteo, ProtonMail, and Tutanota on the market. Look for end-to-end encryption in secure storage providers, too, he recommends.

If you are feeling extra paranoid, you can sign up anonymously for added privacy and use a VPN both at sign-up and when accessing the account to conceal your IP address, Walsh says. This will ensure that the email header does not contain an IP address that can be traced back to you. If you want to really hide your tracks, pay for the secure storage using cryptocurrency.

(c)2020 U.S. Today

Distributed by Tribune Content Agency, LLC.

APA citation: Want to take back your online privacy? 7 easy steps to stop Facebook and others from spying on you (2020, February 5) retrieved 16 May 2021 from

<https://techxplore.com/news/2020-02-online-privacy-easy-facebook-spying.html>

*This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.*