SECURITY GUIDE

The McAfee Safety Series

Digital Privacy Guide

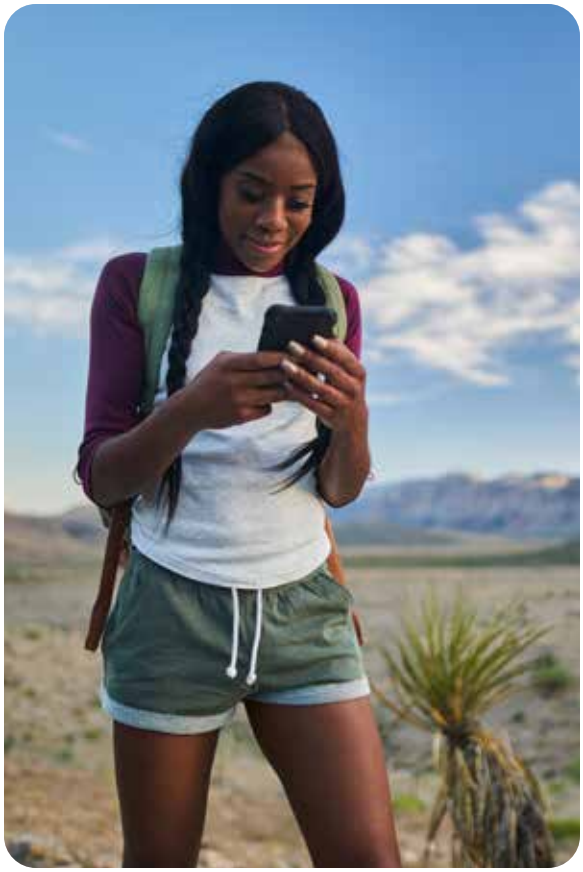


Table of Contents

Putting privacy back in your hands

There's a price tag on your privacy.

Personal information about you, your habits, your preferences, where you go, what you do, when you do it, and how often you do it all have a dollar value. Businesses, hackers, and scammers alike have an interest in it because there's money in it, and they'll use digital means to extract this information. Some are entirely legal, others illegal, and yet others fall into a gray area where collecting data is technically permitted yet ethically questionable.

Granted, different people hold different ideas about what's private and what's not. Some people will live their life on social media like an open book for all to see, while others are far more reserved about what they share. Moreover, individually, people will see some areas of their life as more private and other areas less so. They may not share that they just paid a friend $25 for pizza on a mobile payment app like Venmo, yet they will let a retailer track their shopping history in exchange for a loyalty card with a store discount.

Meanwhile, people are creating data about themselves, either actively or passively, simply by spending time online. As they bank, shop, game, or simply surf around, that data is getting collected for business or illicit purposes, with or without their knowledge or consent.

The one constant in this digital mix is this: your privacy is yours. Whether or not you want to share your personal information, and with whom and for what reasons, should be your decision. In this way, privacy is both a right and a choice.

In this guide, we'll show you ways that you can take control of your digital privacy, all while giving you insight into what information you may be creating and how you may be passing it along—whether you are aware of it or not.

Let's start with an overview of businesses, hackers, and scammers alike with an eye on why they are so quick to put that price tag on your privacy.

Section One—What makes your privacy so precious?

At the root of your privacy is your personal data.

Personal data is information about you that others can use to identify you either directly or indirectly. Thus, that info could identify you on its own, or it could identify you when it's linked to other identifiers.

Direct identifiers

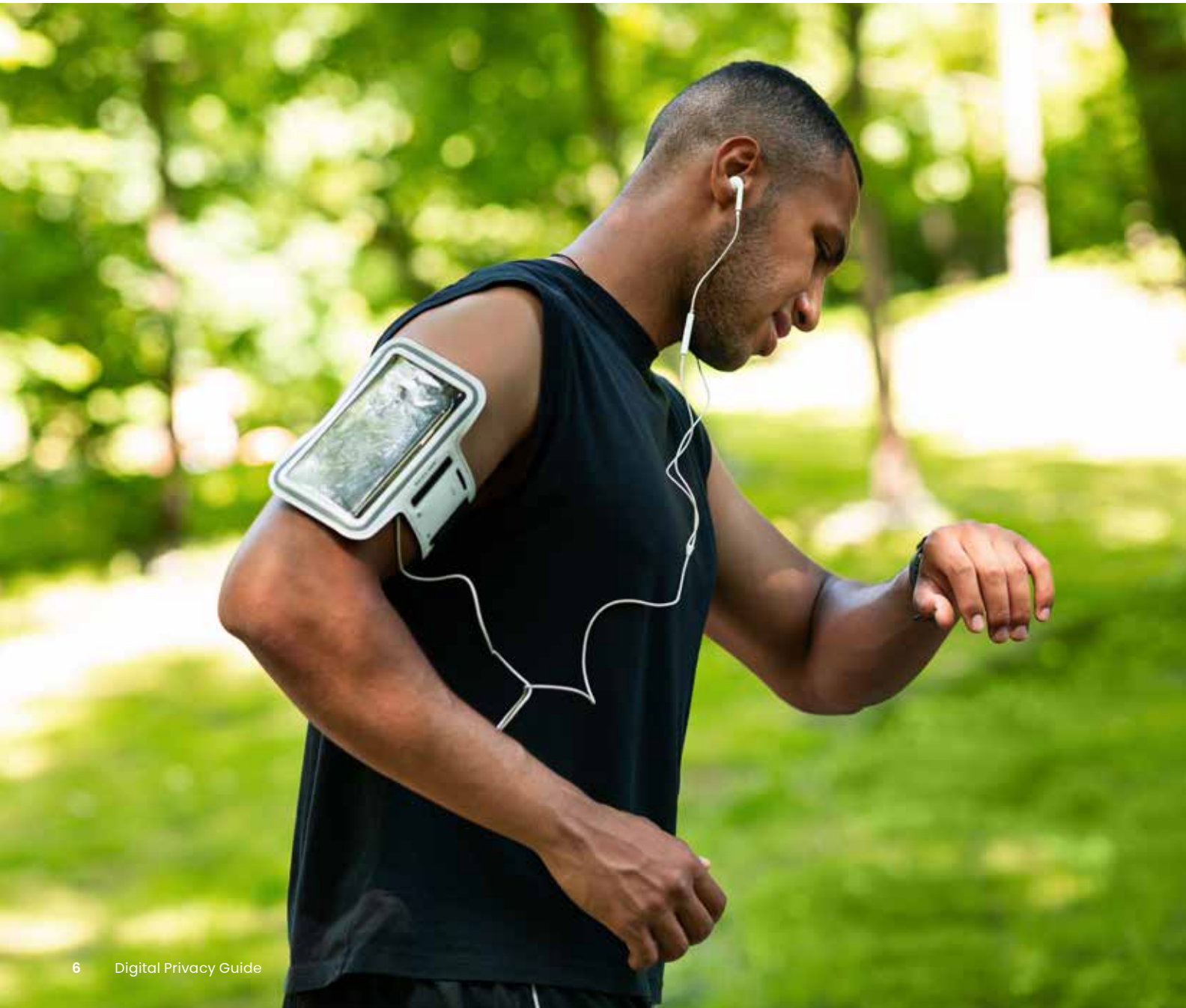
A prime example of a direct identifier is your tax ID number because it's unique and directly associated with your name. Further instances include your email address, residential address, driver's license number, and your phone number because each of these can be easily linked back to you.

Indirect identifiers

Then there are those indirect pieces of personal data that act as helpers. While they may not directly identify you on their own, a few of them can when they're added together. These helpers include things like zip codes, gender, date and place of birth, internet protocol addresses, or the unique device ID of your smartphone. Together, indirect identifiers are like pieces of a puzzle. The more pieces someone has, the more they know about you.

You can also find pieces of your personal data in the accounts you use, like your Google or Apple IDs, which can be linked to your name, your email address, and the apps you have. You'll also find it in the apps you use. For example, there's personal data in the app you use to map your walks and runs, because the combination of your smartphone's unique device ID and GPS tracking can be used in conjunction with other information to identify who you are, not to mention where you typically like to do your 5k hill days. The same goes for messenger apps, which can collect how you interact with others, how often you use the app, and your location information based on your IP address, GPS information, or both.

In all, if enough personal data gets gathered in one place, it can create a pretty clear picture of you—which can be highly useful for businesses and bad actors alike, depending on who holds it.



Your personal data in the hands of businesses and brands

Some years ago, a story broke[1] about how a major retailer in the U.S. effectively predicted a woman's pregnancy before she shared the news with the rest of her family. How so? The retailer suddenly began sending her coupons for baby clothes and cribs. So suddenly and with such focus that a family member called it into question. It was only weeks later the woman officially shared the news with her family.

Now how on earth did that retailer predict that pregnancy and then market their products with such uncanny accuracy? Data. Data from that woman and millions of customers like her.

The article explains the specifics. The retailer assigned a unique ID number to its customers. Tied into that ID was information ranging from credit card numbers, personal information that they collected, information that they bought from other sources, and, of course, shopping histories. With that, in addition to millions of other data-rich IDs, the retailer could make predictions about customers based on their purchases. For example, they knew that purchases of unscented body lotion and nutritional supplements like magnesium, calcium, and zinc were often made by expecting mothers. From there, they could market to those customers accordingly.

In this way, one person's shopping history, matched against millions of others, can make some terrifically accurate predictions—ones that can feel somewhat intrusive, which a statistician at the retailer openly acknowledged at the time when he said, "We are very conservative about compliance with all privacy laws. But even if you're following the law, you can do things where people get queasy." (And as the article noted,[2] the retailer had since changed its data-driven marketing practices.)

If you've come across the term "big data" before, these are all examples of it in action. The American Oxford Dictionary defines it as *extremely large data sets that may be analyzed computationally to reveal patterns, trends, and associations, especially relating to human behavior and interactions*. And big data is big business. To the tune of hundreds of billions of dollars each year.

That story actually dates back to 2012 when data collection and analysis was in its relatively early stages. Since then, those collection and analysis technologies have matured into more powerful forms. Likewise, we create more data now than ever before. Consider:

- There's a good chance that you own a smartphone now, given that the rate of ownership has nearly tripled since 2012.
- And with that, there's a good chance you're using plenty of apps—apps that help you keep up with your health, travel, finances, fitness, and even hail a rideshare to and from the airport.
- You're also likely a user of social media, possibly several platforms.
- With a built-in data connection, GPS technology, and a unique device ID, data from your smartphone can not only show what you're doing, but where you're doing it and when.
- Then there's the streaming you do. The movies, the shows, also across multiple platforms.
- Maybe you have a smart assistant in the home. Controlling all kinds of smart devices like washers, refrigerators, and even the lock on your front door.

All these devices and apps create data about you as you use them. And over time, massive pools of it, compiled by device manufacturers, operating system developers, social media companies, app developers, online retailers, brick-and-mortar retailers, search companies, even your grocery store if you use a loyalty card are all collecting data.

Needless to say, not everyone is comfortable with this, particularly that their habits and everyday behaviors may be building an eerily accurate profile of themselves that companies can keep, buy, or sell.

In this way, one person's shopping history, matched against millions of others, can make some terrifically accurate predictions—ones that can feel somewhat intrusive...

Your personal data in the hands of hackers and scammers

Someone else who finds great value in your privacy are hackers and scammers, who will highjack or flat-out steal your personal data for illicit purposes.

A favorite point of entry of theirs is the smartphone. It's a treasure trove of personal info and photos, in addition to credentials for banking and payment apps, all of which are valuable to loot or hold for ransom. Add in other powerful smartphone features like cameras, microphones, and GPS, a compromised phone may allow a hacker to:

- Snoop on your current location and everyday travels.
- Hijack your passwords to social media, shopping, and financial accounts.
- Drain your wallet by racking up app store purchases or tapping into payment apps.
- Read your text messages or steal your photos.

Each of these are tremendous invasions of privacy, not to mention theft in some cases. How do bad actors get this kind of access? One way is through malicious apps. By posing as legitimate apps, they can end up on your phone and gain broad, powerful permissions to files, photos, and functionality—or sneak in code that allows hackers to gather personal info. As a result, this can lead to all kinds of headaches, ranging from a plague of popup ads to costly identity theft.

Here are a few examples of malicious apps from recent years include:

- Fake ad blocking programs[3] that ironically serve up ads instead.
- Phony VPN apps[4] that charge a subscription and offer no protection in return.
- Utility apps[5] such as image editors that hijack system privileges and permissions, which expose users to further attacks.

Consider the cases of malicious flashlight apps,[6] some of which requested up to more than 70 different permissions, such as the right to record audio, video, and access contacts. No flashlight app needs access to all of that.

Hackers have other tools for harvesting your personal data, such as spyware. Spyware can take on various forms, yet as the name suggests it's designed to gather otherwise private information, almost as if it were looking right over your shoulder as you use your computer, tablet, or smartphone. The difference here is that the information goes right into the hands of the hacker or bad actor, again for potentially profitable and damaging use.

Protect what's precious

Whether it's a business or a bad actor, there are plenty of parties ready to tap into the data and personal information you create as you go online.

In the case of businesses, they look to profit from your personal data. The fact is that we leave plenty of data and information in our wake as we simply go about our day, which gets collected, analyzed, and used in several ways. Companies can use it for sales and marketing purposes as the retailer example showed us above. Other companies will sell it to data brokers that then resell it to other parties for profit. And social media companies that let you use their platforms for free have built entire businesses on personal data by charging advertisers access to highly targeted customers.

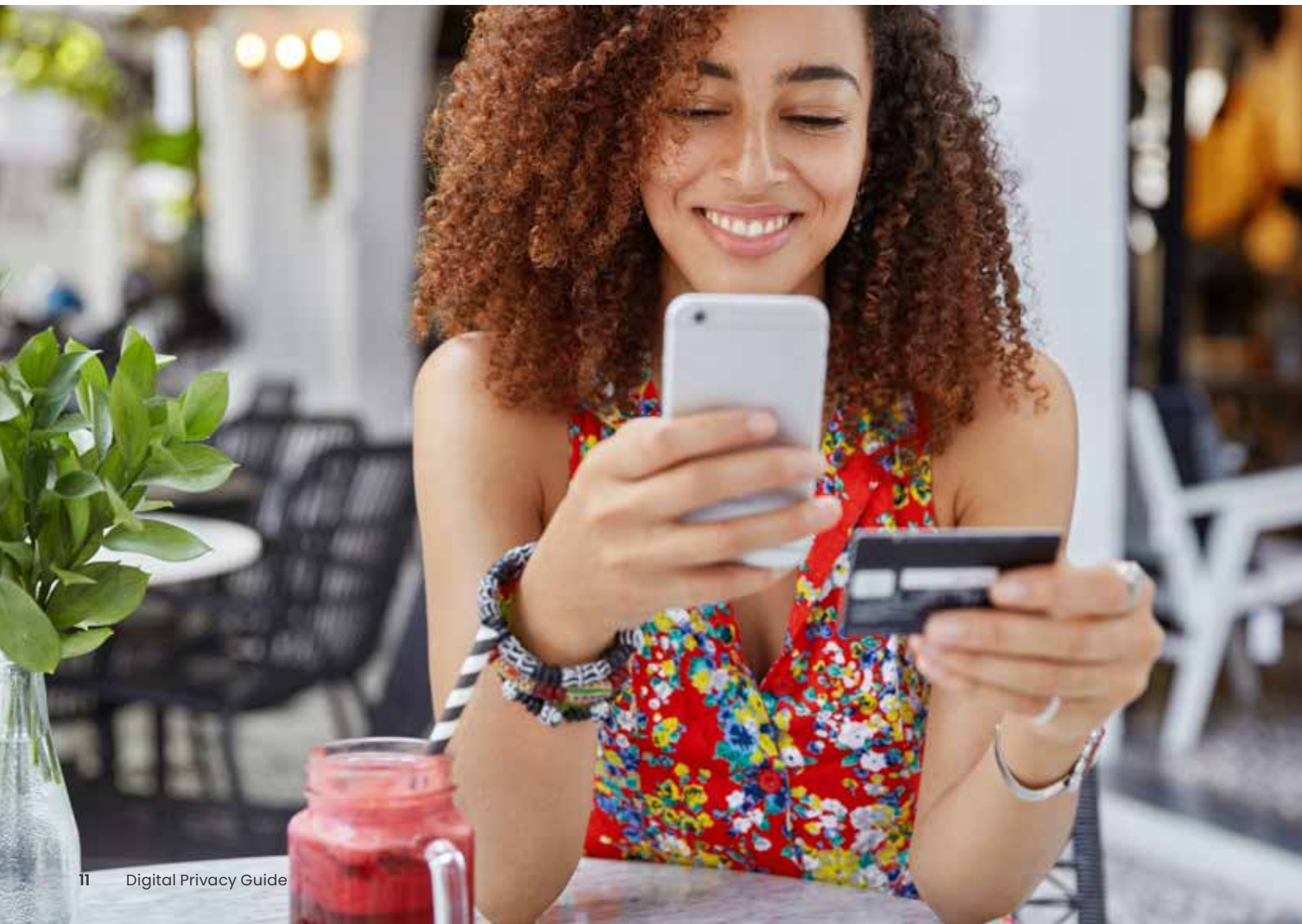
Whether it's a business or a bad actor, there are plenty of parties ready to tap into the data and personal information you create as you go online.

Worth noting in this equation is the idea of a "value exchange." For example, social media platforms let you connect and share with others for free. In exchange for that value, you get exposed to those highly targeted ads. Another example is a loyalty card. In exchange for tracking your shopping history and potentially other personal information about you, you get a discount on a retailer's products. While not all businesses collect personal data as part of a value exchange, several do, which then lets you decide if that value exchange is indeed truly valuable to you.

As for hackers and scammers, what do they do with the personal data they gather? Several things. One may be to spam you and your contacts with ads, they may install adware that serves up ads on your devices, or they may simply use your personal data to steal your identity, drain your accounts, or sell it to other parties who will.

Beyond that, bad actors have also posted such private information online to harass their victims—an act known as doxing—not to mention posting files and photos intended to embarrass those victims as well.

No question about it, your privacy is absolutely precious. Now with a sense of what's at stake, you can decide how you'd like to protect it—from whom and in which ways.



Section Two—Locking down your digital privacy

One of the concerns people have about their digital privacy is that it can feel like it's out of their hands, that giving up chunks of their privacy is inevitable when you live life online. The reality is that going online inherently creates PII in some form or other, yet there are ways you can curb it and control it.

So, while total privacy online is more of an ideal rather than an attainable goal, you have several tactics and tools that can help make you far more private than you would be without them.

Privacy basics

Lock your devices

Let's start with a simple one. By locking your devices, you protect yourself that much better from data theft in the event your device is lost, stolen, or even left unattended for a short stretch. Use your password, PIN, facial recognition, thumbprint ID, or other form of locking your device.

Also, learn how you can remotely lock or wipe your devices in the event of loss or theft. Android owners can see how it's done here,[7] and owners of Apple iOS devices can find out here.[8] For locating and locking a Windows device, Microsoft offers this how-to page.[9] Likewise, Apple has its own page for locating, locking, and remotely wiping your Mac.[10]

Use a complete security platform that includes a firewall

Another simple yet powerful step is to protect your devices with comprehensive online protection software. This will defend you against the latest virus, malware, spyware, and ransomware attacks plus further protect your privacy and identity. In addition to this, it will also offer strong password protection and web protection that can help steer you clear of sketchy websites that may try to steal your data.

Look for HTTPS when you browse

The "S" in the "HTTPS" web address stands for secure. Any time you are shopping, banking, or sharing any kind of sensitive information, look for "https" at the start of the web address. (Some browsers will also indicate HTTP by showing a small "lock" icon.) Doing otherwise on plain HTTP sites exposes your PII for hackers who may be monitoring the traffic there.

Steer clear of those internet "quizzes"

Which Marvel Universe superhero are you? Does it really matter? After all, such quizzes and social media posts are often grifting your personal data in a seemingly playful way. While you're not giving up your SSN, you may be giving up things like your birthday, your pet's name, your first car … things that people often use to compose their passwords or use as answers to common security questions on banking and financial sites. The way to pass this kind of quiz is not to take it.

Protecting your private data, files, and documents

Digitally "shred" sensitive documents instead of deleting them

For things like electronic tax forms, financial records, and other sensitive data on your computer, simply deleting a file is not enough. That data remains on the drive until it is written over or otherwise removed permanently. One way to go about that is with a digital document shredder that renders the data practically unusable when you're ready to trash the file. Comprehensive online protection software will often include such a feature, such as our own file shredder.

Use a VPN

Also known as a "virtual private network," a VPN helps protect your personal information and other data with bank-grade encryption. Think of it as a sort of private browsing where a "tunneled" connection shields you from prying eyes, which can minimize the data that gets exposed as it transmits to and from your device.

Physical security is important too

Be aware of your surroundings

While it's necessary to talk about the many ways a criminal can digitally skim your PII, it's important to remember that physical security is important as well. Being aware of your surroundings in the coffee shop, securing you smartphone from pickpockets, and not leaving your laptop in the car when you quickly pop into the store, can protect your digital devices from physical theft—along with the data, information, photos, and files on them.

Watch out for "shoulder surfers"

Just like you covered your work while taking that math test in grade school, cover your work when you're out in public. Or better yet, do your shopping, banking, and other sensitive work strictly at home or in another controlled situation. Crooks will happily lower themselves to peeping over your shoulder to get the information they want.

Invest in a paper shredder

Sensitive documents come in all forms. Top-of-the-line examples include things like tax returns, bank statements, and financial records. Yet there are also things like your phone and utility bills, statements from your doctor's office, and offers that come to you via mail. Together, these things can contain personal information such as account numbers and other information that may uniquely identify you.

Protect your SSN number

This is one of the most prized possessions a thief can run away with because it is so closely associated with you and things like your tax returns, employment, and so on. Keep it stored in a safe location rather than on your person or in your wallet. Likewise, be careful about giving it out. For example, in the U.S., many organizations may ask for a Social Security Number as a form of identification. (Doctor's offices are a prime example.) However, only organizations like the IRS, your bank, employer, and state ID/drivers license issuer require it. If an organization other than these requests it, you can ask if another form of identification will work instead.

Reduce your digital footprint

Review your privacy settings for the devices, platforms, and apps you use

Different devices, platforms, and apps will have their own settings, so give them a look and see what your privacy options are. For example, some social media platforms may let you determine which information advertisers are allowed to use to serve up ads to you. Other apps may allow you to enable or disable GPS location information.

As for devices, both Windows[11] and Mac OS[12] have extensive privacy controls available. Android[13] provides visual guides on the topic, and Apple has a similar resource for iOS users[14] as well. A quick search about privacy on any device, platform, or app should turn up some helpful results that can get you started if you have questions.

Check out their privacy policies as well

Privacy policies spell out what data a company may be collecting, for what purpose, what they do with it, and if they may share or otherwise sell it to third parties. Needless to say, the language in privacy policies can get somewhat long and complex. However, several companies have been making good faith efforts to explain their privacy policies in plain language on user-friendly websites. Google provides a good example[15] of this, which includes a link to their Privacy Checkup experience.[16] Additionally, Apple offers users on iOS 15.2 or higher an app privacy report[17] that shows what iPhone features and data apps have recently accessed. Once again, a web search will help point you to similar resources for the devices, platforms, and apps you use.

What you find may surprise you. For example, you may find out that your messaging app collects location information from you when you share your location with a friend on your smartphone. You may also want to know what's done with that information. Does the company only use it for internal purposes, or do they also have the right to sell that location information to third parties like advertisers? Here, you'll have to weigh the pros and cons of that convenience and decide if it's right for you.

Clean up the personal data posted about you online

Earlier, we mentioned data brokers that collect and resell PII online. Additionally, there are so-called "White Pages" and "people finder" sites that post information like names, addresses, and other public records that anyone can access. With all this information collected in a central location that's easily searched and accessed, these sites can be an ideal resource for hackers, spammers, and thieves.

McAfee's Personal Data Cleanup can help you clean that up. It scans high-risk data broker sites and lets you know which ones are selling your data, and depending on your plan, it can remove it for you too.

Deactivate you old accounts—and delete their data

Whether you've been on the internet for five, ten, or even twenty years, there's a good chance that you have plenty of accounts that you don't use anymore or that you've simply forgotten about. Some of these accounts may contain your PII or info in some form or fashion, which could unnecessarily expose it to hackers or thieves, whether as part of a breach or via information that any user can access.

Section Three—What do social media companies really know about you?

The quick answer is this: the more you use social media, the more those companies likely know.

The moment you examine the question more closely, the answer takes on greater depth. Consider how much we use social media for things other than connecting with friends. While that was the original intent behind social networks, the role of social media has since evolved into something far more expansive.

We use it to get our news, stay up to date on when artists will drop a new release, and sometimes reach out for customer service on a company's social media page. In some cases, we use our social media accounts to log into other sites and apps[18] or we even make payments through social media.[19]

Taken together, all those likes, taps, clicks, links, and time spent reading or watching videos can add up and paint a detailed picture of who you are.

Why are they collecting all this information? Largely, it's for two reasons:

1. To make improvements to their platform, by better understanding your behavior and ways you like to use their service.
2. To create an exacting user profile that advertisers can use for targeting ads that they think will interest you.

That's the value exchange we covered earlier. You use the company's social media service for free, and in return they gain rights to gather specific information about you, which you consent to by agreeing to their terms of service.

As for what social media companies may specifically know about you, and for ways you can limit what data and information they gather, requires a much closer look.

Using social media means sharing information with social media companies

Different social media platforms have different user agreements that cover what types of information they collect and use. So for starters, it helps to know what social media companies may know in general, along with some examples from select privacy policies:

Basic information about you and the devices you use

This includes personal information that people include in their profiles, such as names, birthdates, locations, relationships, and gender. This can extend to other identifiers like IP addresses, unique device ID numbers, connection type, connection speed, your network, other devices on your network. Also, device behavior can get tracked as well. That may include whether a window is open in the foreground or background and what mouse clicks and finger taps you make while using the service.

What interests you

People, pages, accounts, and hashtags that are associated with you and that you interact with in some way can get tracked. Likewise, how those people, pages, and accounts associate themselves with you in return get tracked as well. All of it builds up a profile with increasing levels of detail the more you engage with others and as they engage with you.

What makes you stick around

Social media companies may measure the frequency and duration of your interactions. The more you interact, the more likely you are to have a strong connection to certain topics and opinions—and subsequently social media companies may suggest similar content that they believe you will engage with just as strongly. For example, Meta (including Facebook and Instagram) puts it this way on their privacy page[20] (as of July 2022):

We collect your activity across our Products and information you provide, such as:

- *Types of content you view or interact with, and how you interact with it.*
- *Apps and features you use, and what actions you take in them.*
- *The time, frequency, and duration of your activities on our Products.*

Who you're chatting with

Depending on the platform and its terms of use, information about direct messages you send using the platform may be collected as well. For example, Twitter does the following[21] (as of June 2022):

We collect information about your activity on Twitter, including:

- *Your interactions with other users' content, such as retweets, likes, shares, replies, if other users mention or tag you in content or if you mention or tag them, and broadcasts you've participated in (including your viewing history, listening, commenting, speaking, and reacting).*
- *How you interact with others on the platform, such as people you follow and people who follow you, and when you use Direct Messages, including the contents of the messages, the recipients, and date and time of messages.*
- *If you communicate with us, such as through email, we will collect information about the communication and its content.*
- *We collect information on links you interact with across our services (including in our emails sent to you).*

Things you purchase on the platform

In some cases, social media companies will track information about transactions you make on their platform. For example, Instagram includes the following language in its terms of use[22] (as of July 2022):

We collect information when you use our Products to buy or sell things or make other financial transactions. Some examples are:

- *Purchases within an online game.*
- *Donations to a friend's fundraiser.*
- *Purchases in Marketplace, Shops, or groups.*
- *Money transfers to friends and family (where available).*

The following gets collected in addition:

When you buy things or make other payments in Marketplace, Shops or groups, we collect information about your purchase or other financial transactions, like:

- *Credit or debit card number and other card information.*
- *Billing, shipping, and contact details.*
- *Items you bought and how many.*
- *Other account and authentication information.*

Where you are and where you go

Simply disabling location sharing or GPS functionality on your device does not rule out other ways that social media companies can determine your whereabouts. They can infer your location to some extent when you log in by looking at your IP address and public Wi-Fi networks, along with nearby cellular towers if you're on mobile.

By the way, none of what we've listed here is secret. What's listed here can be found by simply reading the terms of use posted by various social media companies. Note that these terms of use can and do change. Checking up on them regularly will help you understand what is being collected and how it may be used.

What your content says about you too

This nearly goes without saying, yet another layer of data and information collection comes by way of the pictures and updates you post. Per Instagram (as of July 2022), this includes:

- *Content you create, like posts, comments, or audio.*
- *Content you provide through our camera feature or your camera roll settings, or through our voice-enabled features.*
- *Messages you send and receive, including their content, subject to applicable law. We can't see the content of encrypted messages unless users report them to us for review.*
- *Metadata about content and messages, subject to applicable law.*

Additionally, the content you interact with on other sites may be shared with social media companies in return. Some social media companies partner with other third parties to gather this data, which is used to round out your user profile in yet more detail. That information can include purchases you made, how often you visited that third party's site, and so on.

In the case of Facebook, they refer to this as "Off-Facebook Activity."[23] In their words:

- *Off-Facebook activity includes information that businesses and organizations share with us about your interactions with them. For example, your interactions could be visiting their website or using their app.*
- *We use your activity to show you things you might be interested in, like events you might want to go to. We also use your activity to show you relevant ads that introduce you to new products and services.*

The good news is that you can take control of the Off-Facebook Activity setting with a few clicks.[24] Likewise, you can review any Off-Facebook activity associated with your account with a visit to their help center page.[25]

So no doubt about it, the content you create and interact with, both on the social media sites and sometimes off them as well, can generate information about you that's collected by social media companies.

Limiting what social media companies know about you

Short of deleting your accounts altogether, there are several things you can do to take control and limit the amount of information you share.

1. **You can access, update, correct, move, and erase your data, depending on the platform.** For example, you can visit your Facebook Settings,[26] Instagram Settings,[27] and Twitter Settings,[28] which each give you options for managing your information—or download it and even delete it from their platform outright if you wish. (Note that this will likely only delete data associated with your account. Content you posted or shared with other people on their accounts will remain.)
2. **Disable location sharing.** As noted above, this isn't an absolute fix because social media companies can infer your location other ways. Yet taking this step gives them one less piece of exacting information about you.
3. **Consider using other messaging platforms.** Using direct messaging on social media platforms may tell social media companies even more about you and who you interact with. When possible, think about using text messaging instead or other means of communication that aren't tied to a social media company.
4. **Decouple your social media account from other apps and sites.** Some apps and sites will allow you to use your social media login instead of creating a new one. While convenient, this can provide the social media company with more information about you. Check your settings and look for "Apps and Websites" to see what's connected to your social media account, what's being shared, and how you can disable it.
5. **Watch what you share.** Aside from social media companies gleaning information about what you post, as outlined just above, there are two more ways you can protect your digital privacy on social media. One, think twice about what PII you might be sharing in that post or photo—like the location of your child's school or the license plate on your car. Two, set your profile to private so that only friends can see it.

Digital privacy: You have more control than you may think

Beyond the advent of big data and the continued rise of data breaches that have made billions of pieces of personal information public, further forces have shaped the digital privacy landscape in recent years—changes that now offer you more protections than before.

One undeniable force is legislation. The European Union's General Data Protection Regulation (GDPR), which governs the collection, use, transmission, and security of data collected from residents of EU member countries, can levy fines of up to 20 million Euro or 4% of total global turnover for organizations that fail to comply with the regulation. Further measures such as the Electronic Privacy Regulation are also on the horizon, designed to keep pace with advances in technology and to extend protection to users of platforms like WhatsApp, Facebook Messenger, and Skype.

Although the U.S. does not have similarly sweeping legislation, states such as California, Colorado, New York, and Virginia have enacted data privacy laws to protect consumers, with several other states poised to follow suit. Pending their passage, collectively they may make a significant national impact.

Meanwhile, people have made their concerns about digital privacy known. They want to know what data is being collected, how it's being used, and how it all gets protected, particularly as they realize how businesses are profiting off it, not to mention falling victim to various forms of data crime like identity theft and fraud.

In response to legislation and public pressure alike, tech companies have put up websites dedicated to user-friendly privacy guidance, "privacy check-ups" in their platforms and apps, along with hosts of features that allow their users to exercise varying degrees of control. Some device manufacturers have even made privacy a core selling point.[29]

In all, you have a growing body of privacy protections falling into place, regulatory and legislative, along with a similarly growing body of tactics and tools that can help you maintain your digital privacy.

We created McAfee+ in that same spirit, by putting your privacy front and center. With next-level, all-in-one privacy and identity protection, it helps remove your personal data from risky websites and proactively monitors the dark web for your info and helps restore your identity should the unexpected happen. With the protection of McAfee+ and the steps this guide, you can live a safer and more private life online.

For more about staying safe and getting the most out of life online, our blog offers you and your family a terrific resource across a wide range of topics from online banking, gaming, and shopping to tough yet important topics like cyberbullying and which apps are safe for kids.

Our aim is to help you think about what's best for your family and the steps you can take to see it through so that you can make everyone's time online safer and more enjoyable.

Visit us any time!

https://www.mcafee.com/blogs

About McAfee

McAfee is a worldwide leader in online protection. We're focused on protecting people, not devices. Our solutions adapt to our customers' needs and empower them to confidently experience life online through integrated, easy-to-use solutions.

www.mcafee.com

For more information about online protection, visit us at mcafee.com/blogs

Endnotes

1 https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did
2 https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=133c32656668#:~:text=%E2%80%9CThen%20we%20started,her%2C%20it%20works.%E2%80%9D
3 https://www.zdnet.com/article/android-malware-disguises-as-ad-blocker-but-then-pesters-users-with-ads/
4 https://www.techradar.com/news/dont-be-fooled-by-these-fake-vpn-apps-they-could-leave-you-penniless
5 https://thehackernews.com/2022/07/these-28-android-apps-with-10-million.html
6 https://www.tomsguide.com/news/these-android-flashlight-apps-could-be-spying-on-you
7 https://support.google.com/accounts/answer/6160491?hl=en
8 https://support.apple.com/guide/deployment/lock-and-locate-devices-depb980a0be4/web
9 https://support.microsoft.com/en-us/account-billing/find-and-lock-a-lost-windows-device-890bf25e-b8ba-d3fe-8253-e98a12f26316
10 https://support.apple.com/en-us/HT204756
11 https://support.microsoft.com/en-us/windows/change-privacy-settings-in-windows-55466b7b-14de-c230-3ece-6b75557c5227#:~:text=Choose%20how%20much%20information%20you,the%20left%20of%20the%20page.
12 https://support.apple.com/guide/mac-help/change-privacy-preferences-on-mac-mh32356/mac#:~:text=Use%20the%20Privacy%20pane%20of,%26%20Privacy%20%2C%20then%20click%20Privacy.
13 https://www.android.com/safety/
14 https://www.apple.com/privacy/control/
15 https://policies.google.com/privacy?hl=en-US#infocollect
16 https://myaccount.google.com/privacycheckup?utm_source=pp&utm_medium=Promo-in-product&utm_campaign=pp_intro&hl=en_US
17 https://www.apple.com/privacy/control/#:~:text=entirely%20in%C2%A0Settings.-,App%20Privacy%20Report,-See%20at%20a
18 https://www.experian.com/blogs/ask-experian/is-it-safe-to-use-facebook-to-login-on-other-sites/
19 https://pay.facebook.com/
20 https://www.facebook.com/about/privacy/update
21 https://twitter.com/en/privacy
22 https://help.instagram.com/519522125107875/?helpref=hc_fnav
23 https://www.facebook.com/off_facebook_activity/activity_list
24 https://www.facebook.com/help/287199741901674/?helpref=related_articles
25 https://www.facebook.com/help/fblite/2207256696182627
26 https://facebook.com/settings
27 https://www.instagram.com/accounts/privacy_and_security/
28 https://twitter.com/settings/safety
29 https://www.apple.com/privacy/#:~:text=Privacy is a fundamental human right. At Apple, it's also one of our core values.

McAfee

6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com

gd-digital-privacy_1222 DECEMBER 2022