



**NATIONAL
CYBERSECURITY
ALLIANCE**

You Have a Say in Your Data Privacy!

How you can take control of what data you share in 2024

Data privacy might seem abstract, but it couldn't be more personal. You generate lots of data every time you access the internet, and sometimes, when you don't – your home address, health records, and Social Security are all pieces of data. While you can't control the fact that your data is collected, you can take charge of **how and with whom** you share data with in many cases.

Your data is worth a lot of money to many different people, businesses, and organizations, but we often don't value our own data story as much as they do. We can all be more aware of who we share our data with and what we expect in return. Fortunately, there are a few simple, repeatable behaviors you can adopt. It appears people are becoming more aware: a recent [McKinsey survey](#) found that **71%** of consumers said they would stop doing business with a company if it gave away sensitive data without permission.

There's an old Silicon Valley adage that if you're not paying for it, you aren't the customer, you're the product. In many cases, this proves true. To be more accurate, your data is the product. Who's buying? Advertisers, mostly, but also others like software developers. You and your data make up a slice of this multibillion bonanza.

Here are some tips on how to take charge of your data privacy in 2024!

1. Know what you can't control





The truth is, you can't control who has access to every scrap and byte of your data. The IRS, for example, will find out how much money you make. And many online services require some of your data to function – a maps app cannot suggest directions if it doesn't know where you are located (at least while you are using it). An image-sharing site needs access to your photos.

Understand that there is a tradeoff between convenience and privacy. To use all the features of your devices, apps, and software, you will often have to share more and more data. By understanding this balance, you can make better informed data decisions.

2. Cultivate an onlive privacy habit

Apps, websites, devices, and software will often seek out more data than you would think is necessary – why does a Solitaire app need to know your location? Why does a social media app need to know the phone numbers of everyone you know? Here is where you can really take charge of your data.

Fortunately, many web browsers, computers, and devices will ask you if you want to share certain types of data with a new app or website. Strike up a habit of paying attention to these requests and actually thinking about your answers. Here are common types of data you might be asked for:

-  Your location
-  Your contacts
-  Your photos and camera
-  Data about your behavior and use of a service

At this point, think about what you want to share. On mobile devices, you can often decide if you want an app to only have access to this data while using it.





If an app or software program refuses to function unless you share certain data that you don't think it needs (like the Solitaire app demanding your location), **find another app**.

Generally, you might feel more secure erring on always limiting how much data you share when asked.

3. Check your settings

Even if an app or software program never asks you for data, you should assume it is still collecting it. Routinely (every month or so) check your **privacy settings** and ensure everything fits within your comfort level.

You can access app and software permissions through your device's general settings. Remember, apps will often ask for you to give them access permissions at all times, but you usually only need to give them permissions for **while you are using** the app. Here are some default settings you should usually turn off, unless you need it for the app to function and you trust the app.

-  Camera — off
-  Microphone — off
-  Location — off
-  Sync contacts — off

4. Delete apps you don't use

Every 3 months or so, go through your devices and think about each app you have downloaded — we call this an **“app audit.”**

You might think that the real estate on your phone is pretty limitless, but an app audit isn't just about decluttering. Many apps will collect and share your device-use data even when you don't use them; you're basically giving away your data, and you don't even like the app! Why should that food delivery app you used once a year ago get access to all your precious data?

If you haven't used the app in months, delete it from your device. Don't be afraid to be ruthless, you can always download the app again!