BILL'S HOME TECH
Home & Small Business Tech Solutions

BILL'S COMPLETE MANUALS

Privacy Checkup
Google, Facebook & Your Phone

Ad settings, location history, app permissions and what to turn off — explained in plain English, one step at a time

A plain-English privacy tune-up for every household

Take your time — every setting here can be changed back

Written for you by Bill — Bill's Home Tech

(330) 200-8042 · BillsHomeTech.com

For Google, Facebook, iPhone (iOS 26) and Android 16 · facts current November 2026

What's Inside

This is your guide to taking back a little control over what Google, Facebook and your phone collect about you. Part 1 gives you a calm plan and a list of what to turn off. Then pick the part for your account or your phone. Read it in any order and at your own pace. If a screen looks a little different on your device, the idea is still the same.

Part 1 — Getting Started

1 A Note from Bill
2 What Privacy Settings Actually Control
3 Your First Privacy Checkup: A Calm Plan
4 What to Turn Off, What to Leave On

Part 2 — Your Google Account

5 Google's Privacy Checkup
6 My Activity: See What Google Saved
7 Auto-Delete: Set It Once and Forget It
8 Web & App Activity and Google's Newer Search Settings
9 Google Maps Timeline: Your Location History
10 YouTube Watch and Search History
11 My Ad Center: Google's Ad Settings
12 Google Security Checkup and Connected Apps

Part 3 — Facebook & Meta

13 Facebook's Privacy Checkup
14 Who Can See Your Posts
15 Your Profile, Friends List and Who Can Find You
16 Meta Accounts Center in Plain English
17 Facebook and Instagram Ad Preferences
18 Your Activity Off Meta Technologies
19 Apps, Games and Quizzes Connected to Facebook

Part 4 — Your iPhone

20 The Privacy & Security Screen
21 iPhone Location Services, App by App
22 Ask App Not to Track
23 Contacts, Photos, Camera and Microphone
24 Safety Check: When Someone May Be Watching

Part 5 — Your Android Phone

25 The Android Privacy Dashboard

26 Android App Permissions
27 Android Location Settings
28 Delete Your Android Advertising ID
29 Unused Apps Lose Their Permissions

Part 6 — Beyond the Settings

30 Data Brokers and People-Search Websites
31 Fake Privacy Apps, Quizzes and Scare Pop-ups
32 Helping a Parent with a Privacy Checkup
33 Your Twice-a-Year Privacy Routine
34 When to Call Bill
35 Your Privacy Checkup Cheat-Sheet

PART 1

Getting Started

What "privacy settings" really control, a calm plan for your first checkup, and a plain list of what to turn off and what to leave alone.

CHAPTER 1

A Note from Bill

Hello, and welcome. I'm Bill, and for more than 30 years I've helped people make technology behave. Here in Portage County, privacy comes up again and again, usually as a question: "How did my phone know I was at the hardware store?" or "Why am I seeing ads for the thing I talked about yesterday?" or "Can strangers see my Facebook?"

Those are fair questions, and the answers are less spooky than they feel. Google, Facebook and your phone each keep records, mostly to show you ads and to make their services work better. Each one also gives you a set of switches to see those records, delete them, and stop collecting some of them. The switches are just hard to find. This guide finds them for you.

WHAT THIS DOES FOR YOU

What this guide does for you

It walks you through a full privacy checkup, one account and one phone at a time: Google's Privacy Checkup and history settings, Facebook's Privacy Checkup and ad settings, location and app permissions on iPhone and Android, plus the bigger picture: data brokers and the fake "privacy" apps and quizzes that do more harm than good. Chapter 4, *What to Turn Off, What to Leave On* gives you the short list if you only have a few minutes.

Who this guide is for

- Anyone who feels watched by their phone or by the ads that follow them around.
- Anyone who uses Facebook to keep up with family and wants strangers kept out.
- Grown children setting up a parent's phone who want sensible privacy settings from day one.
- Anyone who just wants to know what's being saved, without becoming a computer expert.

The big promise: nothing here breaks your phone

Every switch in this guide can be turned back on. Turning off ad personalization doesn't cancel anything. Limiting an app's location doesn't delete the app. The one thing to slow down for is **deleting history**: once Google or Facebook erases it, it's gone for good, and some deleted location history can't be recovered at all. This guide flags those spots clearly.

You're never stuck alone

Take this at your own pace, one section at a time. You don't have to do it all in one sitting. If you get stuck or something doesn't look right, call or text me at **(330) 200-8042**.

— Bill

CHAPTER 2

What Privacy Settings Actually Control

Before flipping switches, it helps to know what's being collected and why. There are three main kinds of information that companies keep about everyday people, and each has its own settings.

Kind of information	What it means
Your activity	What you search, watch, click and buy. Google keeps it in My Activity; Facebook keeps it in your Activity Log.
Your location	Where your phone has been. Stored on your phone, and sometimes in your account.
Your app permissions	What each app on your phone is allowed to touch: camera, microphone, contacts, photos, location.
Your ad profile	The interests a company guesses about you, used to choose which ads you see.
Public information	Your name, address and phone number collected by data brokers and people-search websites.

Why they collect it

Mostly for two reasons. First, to make things work: Google Maps needs your location to give you directions, and your photos app needs access to the camera. Second, to sell advertising. Free services like Google Search, YouTube and Facebook are paid for by ads, and ads that match your interests earn the company more money.

What privacy settings can and can't do

- **They can** stop a company from saving new history, delete what it already saved, and stop ads based on your interests.
- **They can** keep apps from using your location, camera or microphone when they don't need to.
- **They can't** make ads disappear. You'll still see ads; they'll just be less personal.
- **They can't** remove information that other people or other companies already have, such as people-search websites. Chapter 30, *Data Brokers and People-Search Websites* covers those.

GOOD TO KNOW

Privacy is a dial, not a switch

You don't have to choose between "everything on" and "live in a cave." Most people are happiest keeping the features they enjoy, like Maps directions and photo backups, while turning off the collection they never asked for. This guide helps you set the dial where it feels right to you.

HEADS UP

Privacy and security are cousins

Privacy is about who can *see* your information. Security is about who can *get into* your accounts. A strong password and two-step verification matter just as much. Chapter 12, *Google Security Checkup and Connected Apps* touches on the security side for your Google Account.

CHAPTER 3

Your First Privacy Checkup: A Calm Plan

A full checkup takes about an hour if you do everything. You can split it into short sittings over a week. Here's the order that makes the most difference for the least effort.

1. **Your phone first (15 minutes).** Check which apps can see your location, and turn off the ones that don't need it. iPhone: Chapter 21, *iPhone Location Services, App by App*. Android: Chapter 27, *Android Location Settings*.
2. **Google next (15 minutes).** Run Google's Privacy Checkup and set auto-delete on your history. See Chapter 5, *Google's Privacy Checkup* and Chapter 7, *Auto-Delete: Set It Once and Forget It*.
3. **Facebook (15 minutes).** Run Facebook's Privacy Checkup and set who can see your posts. See Chapter 13, *Facebook's Privacy Checkup* and Chapter 14, *Who Can See Your Posts*.
4. **Ads (10 minutes).** Turn down ad personalization at Google and Facebook, and on your phone. See Chapter 11, *My Ad Center: Google's Ad Settings*, Chapter 17, *Facebook and Instagram Ad Preferences* and Chapter 22, *Ask App Not to Track* or Chapter 28, *Delete Your Android Advertising ID*.
5. **Put a reminder on your calendar** to look again in six months. Chapter 33, *Your Twice-a-Year Privacy Routine* has the short version.

Before you start

- Have your phone charged and nearby.
- Know your Google password and your Facebook password. Some settings ask you to sign in again.
- Use a computer if you have one. Google's and Facebook's settings are easier to read on a big screen, and they apply to your phone too.
- Have a cup of coffee. None of this is urgent, and none of it needs to be rushed.

TIP

Settings follow your account, not your device

When you change a Google or Facebook setting on a computer, it applies wherever you're signed in, including your phone and tablet. You don't have to repeat it on each device. Phone settings, like location permissions, are different: those live on each phone.

STAY SAFE

Only use the real settings pages

Every step in this guide happens inside the real Google, Facebook, Apple or Android settings. You never need to download a special "privacy" app, and nobody will call you to help with your privacy settings. If someone does, hang up. Chapter 31, *Fake Privacy Apps, Quizzes and Scare Pop-ups* explains why.

CHAPTER 4

What to Turn Off, What to Leave On

If you only read one chapter, read this one. These are sensible starting choices for most people. The chapters that follow have the steps for each one. You can always change your mind later.

Setting	My usual suggestion	Why
Google history (Web & App Activity)	Leave on, set auto-delete	Keeps search and Maps helpful, but old records erase themselves.
Google Maps Timeline	Off, unless you use it	A diary of everywhere you've been. Useful for some, unwanted by many.
YouTube history	Leave on, set auto-delete	Recommendations get worse without it.
Google personalized ads	Your choice; off is fine	Ads keep coming either way; they're just less personal.
Facebook future posts	Friends	Strangers can't see your trips, family photos or birthdays.
Facebook off-Meta activity	Disconnect future activity	Stops shopping sites from feeding your Facebook ad profile.
iPhone app tracking	Ask App Not to Track	Apps can't follow you across other apps and websites.
Phone location for each app	"While using" or Never	Only maps, weather and ride apps really need it.
Precise location	Off for most apps	Weather and shopping apps don't need your exact house.
Android advertising ID	Delete it	Removes the tag ad companies use to recognize your phone.

What to leave alone

- **Location Services as a whole.** Don't switch it off entirely. Find My and Find Hub, Maps and weather depend on it. Limit individual apps instead.
- **Find My (iPhone) or Find Hub (Android).** These help you find a lost phone. Keep them on.
- **Software updates.** Updates fix security holes. Keep them on automatic.
- **Two-step verification.** It protects your accounts. Never turn it off to make sign-in easier.

TIP

One setting at a time

If something stops working after a change, like a weather app that can't find your town, it's easy to tell which switch did it when you change one thing at a time. Just turn that one back on.

FROM BILL

These are suggestions, not rules

Some people love Google Maps Timeline because it reminds them where they parked or which restaurant they visited on vacation. If a feature makes your life easier, keep it. The goal is that *you* decide, instead of the default deciding for you.

PART 2

Your Google Account

If you use Gmail, an Android phone, YouTube or Google Maps, you have a Google Account. Here's how to see what it saves and decide what it keeps.

CHAPTER 5

Google's Privacy Checkup

Google has a guided tour of its most important privacy settings called **Privacy Checkup**. It walks you through your history settings, your ad settings and what others can see about you, one screen at a time, with a plain explanation of each. It's the best place to start.

To run Google's Privacy Checkup

1. On a computer, open your web browser and go to **myaccount.google.com**. Sign in if asked. On an Android phone, you can also open **Settings > Google > Manage your Google Account**.
2. Click the **Data & privacy** section on the left (on a phone, it's a tab across the top).
3. Look for **Privacy Checkup** near the top and click **Take Privacy Checkup** or the arrow beside it. If you don't see it, type **Privacy Checkup** into the search box at the top of the page.
4. Go through each card. Each one shows a setting, says what it does, and lets you change it right there.
5. When you reach the end, you're done. Nothing is saved until you change a switch, so you can leave at any time.

What you'll see in it

Card	What it controls
History settings	Web & App Activity, Timeline and YouTube History, with on/off and auto-delete choices.
Ad settings	A link to My Ad Center, where you can turn personalized ads on or off.
What others see	Which personal details, like your birthday or phone number, show on your Google profile.
Third-party connections	Apps and websites you've let into your Google Account.

GOOD TO KNOW

Google is changing some Search settings

Google's own help pages say it is updating the settings for Google Search services, so a few labels may not match exactly what you see. The ideas stay the same: see it, turn it off, or set it to erase itself. Chapter 8, *Web & App Activity and Google's Newer Search Settings* explains the newer Search settings.

TIP

Security Checkup is its sister tool

Google also has **Security Checkup** at **myaccount.google.com/security-checkup**. It checks your recovery phone, sign-in methods and connected devices. Run both. Chapter 12, *Google Security Checkup and Connected Apps* covers it.

SCAM ALERT

Google won't call you about this

Google doesn't phone, text or email people to walk them through privacy settings. If someone claiming to be from Google offers to "secure your account" over the phone, it's a scam. Hang up.

CHAPTER 6

My Activity: See What Google Saved

My Activity is Google's diary of what you've done while signed in: searches, websites visited in Chrome, videos watched on YouTube, places looked up in Maps, questions asked to the Google Assistant or Gemini. It's yours to look through and yours to erase.

To look through it

1. Go to **myactivity.google.com** on a computer or phone, and sign in.
2. Scroll down. Your activity is listed newest first, grouped by day.
3. To find something specific, type a word into the **Search your activity** box at the top.
4. To narrow it down, use **Filter by date & product** and choose, for example, only YouTube or only Maps.

To delete some or all of it

1. To delete one item, click the three dots next to it and choose **Delete**.
2. To delete a whole day, click the trash can icon next to that day's date.
3. To delete a time range, click **Delete** above the list and choose **Last hour**, **Last day**, **All time** or **Custom range**.
4. Confirm when asked.

HEADS UP

Deleting is for keeps

Google says that when you delete activity, it first removes it from view and then begins deleting it from its storage. You can't undo it. Some data may be kept longer for business or legal reasons, as Google's help pages explain.

TIP

Deleted history by accident?

If you erased your history and now Maps or YouTube seem to have "forgotten" you, that's normal. Suggestions will slowly fill back in as you use them. Nothing else on your account is harmed.

GOOD TO KNOW

Gemini has its own history

If you use Google's Gemini assistant, its conversations are kept under **Gemini Apps Activity**, a separate setting. Google's help page says it auto-deletes after 18 months by default, and you can change that to 3 or 36 months or turn it off.

CHAPTER 7

Auto-Delete: Set It Once and Forget It

Deleting history by hand is a chore. **Auto-delete** does it for you: Google erases anything older than the time you choose, on a rolling basis, forever. It's the single most useful privacy switch in your Google Account, because you keep the helpful recent history while the old pile disappears.

To turn on auto-delete for Web & App Activity

1. Go to **myactivity.google.com**.
2. Click **Web & App Activity** (it may also appear as a bar near the top that says the setting is on).
3. Find **Auto-delete** and click it.
4. Choose **Auto-delete activity older than** and pick **3 months**, **18 months** or **36 months**.
5. Click **Next**, then **Confirm**.

Which length to choose

Choice	What it means
3 months	The most private. Recent searches and Maps places still help you; anything older vanishes.
18 months	A middle ground: about a year and a half of history.
36 months	Keeps the most history while still clearing the oldest records.
Don't auto-delete	Keeps everything until you delete it yourself.

TIP

Do the same for YouTube and Timeline

YouTube History has its own auto-delete (Chapter 10, *YouTube Watch and Search History*), and Google Maps Timeline has one too (Chapter 9, *Google Maps Timeline: Your Location History*). Setting all three takes about five minutes.

WHAT THIS DOES FOR YOU

Why this matters

Old history is the kind most likely to embarrass or expose you if your account were ever broken into, and the least useful to you. Auto-delete trims it without you ever thinking about it again.

CHAPTER 8

Web & App Activity and Google's Newer Search Settings

Web & App Activity is the main Google history switch. When it's on, Google saves your searches, Maps lookups, and activity in other Google apps to your account, and uses it to give you better suggestions. When it's off, new activity isn't saved to your account.

To pause it, if you choose

1. Go to **myactivity.google.com** and click **Web & App Activity**.
2. Click **Turn off**, or choose **Turn off and delete activity** if you also want the old history erased.
3. Read the screen that explains what changes, then confirm.

Many people find a better middle ground is to leave it on and set auto-delete to 3 months (Chapter 7, *Auto-Delete: Set It Once and Forget It*). You keep helpful suggestions without a long trail.

The newer Search history settings

During 2026 Google has been rolling out separate settings for its Search services, which its help page says include Search, Maps, Shopping, Flights, Hotels, Translate and News. Google says these newer settings start out matching the choices you'd already made, and that until the new settings reach your account, Search history is still controlled by Web & App Activity.

1. In **myactivity.google.com**, look at the list of controls near the top.
2. If you see a separate setting with **Search** in its name, open it too.
3. Choose on or off, and set its auto-delete the same way you did for Web & App Activity.

HEADS UP

Turning off one may not turn off the other

News reports this year say that once the new Search setting arrives, turning off Web & App Activity no longer covers Search on its own. If privacy in Search matters to you, check both.

GOOD TO KNOW

Incognito mode isn't invisible

Chrome's Incognito window doesn't save history on your device, but it doesn't hide you from websites, your internet provider or your employer's network. It's handy for a quick private search, not a privacy shield.

CHAPTER 9

Google Maps Timeline: Your Location History

Google Maps **Timeline** (once called Location History) is a day-by-day diary of places you've been and routes you've taken. Some people find it handy for remembering a restaurant or adding up miles. Others are surprised to learn it exists. Either way, it's yours to keep, limit or erase.

What changed recently

Google moved Timeline off its servers and onto your phone. Your Timeline is now stored on the device itself, so you manage it in the **Google Maps app** on your phone, not on a website. Google's help says you can still turn off or delete all of your Timeline from My Activity on a computer, but to delete only part of it you use the Maps app.

To see, limit or delete it

1. Open the **Google Maps** app on your phone.
2. Tap your profile picture in the top corner, then **Your Timeline** to see what's there.
3. To change settings, tap your profile picture, then **Settings**, and look for **Location and privacy** (labels vary a little between iPhone and Android).
4. Choose to turn Timeline off, set it to **automatically delete** after **3 months**, **18 months** or **36 months**, or delete all Timeline data.
5. To delete just one day or one visit, open that day in Your Timeline and use the delete option there.

HEADS UP

Timeline deletion can't be undone

Google warns that deleted Timeline data is permanently deleted and can't be recovered. If you use Timeline for mileage or records, write down what you need first.

GOOD TO KNOW

Other location records can still exist

Google notes that turning off Timeline doesn't erase location saved by other settings, such as a search for a store in Web & App Activity. If you also want those gone, delete them in My Activity (Chapter 6, *My Activity: See What Google Saved*). Also, a factory reset of the phone deletes the Timeline stored on it.

TIP

Timeline backup

Google offers an optional backup of Timeline so it survives a phone change. Google's help notes that deleting the backup doesn't delete the Timeline on your devices; delete both if that's your goal.

CHAPTER 10

YouTube Watch and Search History

YouTube remembers the videos you watch and the things you search for. It uses them to suggest what to watch next. That's helpful when it suggests more of the church choir or woodworking videos you enjoy, and less helpful when the grandkids' cartoons take over your recommendations.

To pause or auto-delete YouTube history

1. Go to **myactivity.google.com** and click **YouTube History**.
2. To stop saving new history, choose **Turn off** (YouTube calls this pausing).
3. To erase old history automatically, click **Auto-delete** and choose **3**, **18** or **36 months**.
4. To delete everything now, use **Delete** and choose **All time**.

What pausing does

- Videos you watch while history is paused won't show in your history or affect your recommendations.
- Searches you enter while search history is paused won't be saved.
- The watch history setting is shared between YouTube and YouTube Music.

TIP

Remove one video instead

If one odd video is skewing your suggestions, you don't need to wipe everything. In your history, tap the three dots beside that video and choose the option to remove it from your watch history.

GOOD TO KNOW

Shared TV, shared history

If the whole family watches YouTube on the living room TV under your account, all of it lands in your history. Signing the TV in to a separate account, or pausing history on it, keeps your suggestions your own.

CHAPTER 11

My Ad Center: Google's Ad Settings

My Ad Center is where Google lets you see and change how it picks ads for you. You can turn personalized ads off completely, or keep them on and tell Google which topics and brands you'd like to see more or less of.

To turn personalized ads off

1. Go to **myadcenter.google.com** and sign in.
2. Find the **Personalized ads** switch near the top.
3. Turn it **Off** and confirm.

What changes when it's off

- You still see ads, but Google picks them using general things like the time of day, the topic of the page and your general location.
- Your saved topic and brand choices in My Ad Center are deleted.
- Personalized ads are also turned off on Google's partner sites and apps where you're signed in.
- It doesn't affect ads from other ad networks, and it doesn't stop personalized recommendations in services like Search.

Or fine-tune instead

If you'd rather keep personalized ads but steer them, stay on the My Ad Center page and look through the topics and brands Google thinks you like. Choose **See fewer** for anything unwanted, like ads for something you already bought or a topic that's painful to see.

TIP

Signed out? Change it there too

Google's help notes that when you're not signed in, ad settings are saved in that browser or device. If you use YouTube or Search without signing in, you'd change those settings separately.

HEADS UP

"Talking about something" and then seeing an ad

Many people feel their phone is listening. The usual explanation is ordinary tracking: a search someone in the house made, a store you visited with location on, or a website you browsed. Turning down ad personalization in this chapter and in Chapter 18, *Your Activity Off Meta Technologies* reduces those spooky coincidences.

CHAPTER 12

Google Security Checkup and Connected Apps

Privacy and security go hand in hand. Google's **Security Checkup** looks at who and what can get into your account: your recovery phone and email, the devices signed in, and apps you've given access to. It gives you personalized tips to fix anything weak.

To run Security Checkup

1. Go to **myaccount.google.com/security-checkup** and sign in.
2. Work through each section. A green check means it's fine; a yellow or red mark has a suggested fix.
3. Under **Your devices**, look for any phone, tablet or computer you don't recognize. If you see one, choose to sign it out and change your password.
4. Under third-party access, review the apps and websites connected to your Google Account. Remove any you no longer use.

Why connected apps matter for privacy

Over the years you may have clicked **Sign in with Google** on games, shopping sites or quiz apps. Each one may have permission to see your name, email address, or more. Removing old ones closes doors you forgot were open. The app simply loses access; you can sign in again later if you need it.

TIP

Turn on two-step verification

If Security Checkup suggests two-step verification or a passkey, say yes. It means a stolen password alone isn't enough to get into your account.

SCAM ALERT

"Unusual activity" messages

Real Google security alerts appear inside your Google Account and in the Gmail app. A text or email that says your Google account is "locked" and gives a number to call or a link to click is a scam. Go to **myaccount.google.com** yourself instead.

FROM BILL

Want a second set of eyes?

If Security Checkup shows a device you don't recognize, or you're not sure which connected apps are safe to remove, this is exactly what I go through in a Digital Safety Check-Up. See Chapter 34, *When to Call Bill*.

PART 3

Facebook & Meta

Keep family photos among friends, keep strangers out, and turn down the ads that seem to know too much. Facebook, Instagram and Messenger are all owned by Meta and share some settings.

CHAPTER 13

Facebook's Privacy Checkup

Like Google, Facebook has a guided tour of its main privacy settings, called **Privacy Checkup**. It groups the settings by topic and explains each one in plain words. It's the quickest way to cover the basics.

To open Privacy Checkup

1. On a computer, go to **facebook.com** and click your profile picture in the top right corner.
2. Click **Settings & privacy**, then **Privacy Checkup**.
3. In the Facebook phone app, tap **Menu** (your picture or the three lines), then **Settings & privacy**, then look for **Privacy Checkup** in Settings.
4. Pick a topic card and follow the prompts. Each card ends with a summary; click **Next** or **Review another topic**.

The topics it covers

Topic card	What it covers
Who can see what you share	Your posts, your profile details and your friends list. See Chapter 14, *Who Can See Your Posts*.
How to keep your account secure	Password, login alerts and two-factor authentication.
How people can find you on Facebook	Who can send you friend requests or look you up by phone or email. See Chapter 15, *Your Profile, Friends List and Who Can Find You*.
Your data settings on Facebook	Apps and websites you've logged into with Facebook. See Chapter 19, *Apps, Games and Quizzes Connected to Facebook*.
Your ad preferences on Facebook	What information is used to show you ads. See Chapter 17, *Facebook and Instagram Ad Preferences*.

TIP

Can't find it?

Facebook's help says some Privacy Checkup settings can only be managed from your main Facebook profile. If you also manage a Page or a second profile, switch back to your main profile first.

GOOD TO KNOW

Menus move around

Facebook rearranges its menus often, and the app and website can look different. If a label in this guide doesn't match, use the search box at the top of the Settings screen and type the setting's name.

CHAPTER 14

Who Can See Your Posts

Every post on Facebook has an **audience**: the people allowed to see it. The most common choices are **Public** (anyone, on or off Facebook), **Friends** (only your Facebook friends) and **Only me**. For most people, **Friends** is the right everyday choice.

To choose the audience of a new post

1. Start a new post as usual.
2. Under your name, tap the small audience button (it shows a globe for Public or two people for Friends).
3. Choose **Friends**, or another audience, then go back and finish your post.
4. Facebook remembers this choice for your next post, so you usually set it only once.

To limit all your old posts at once

1. Go to **Settings & privacy > Settings**, then find the section for your posts or privacy.
2. Look for **Limit who can see past posts** (often shown as **Limit Past Posts**).
3. Read the explanation and confirm. Every past post that was Public or friends-of-friends becomes Friends only.

HEADS UP

This one is hard to reverse

Facebook says you can't undo Limit Past Posts in one step. To make an old post Public again, you'd change it one post at a time. Posts you had shared with a custom audience, like Close Friends, aren't changed.

Posts you're tagged in

If a friend tags you in a photo, *they* control who sees their post. You can turn on **tag review** so you approve tags before they show on your profile, and you can remove a tag from any photo of you.

STAY SAFE

Vacation posts can wait

A public post saying the whole family is in Florida for two weeks tells the world your house is empty. Share the beach photos when you're home, or keep the audience to Friends.

CHAPTER 15

Your Profile, Friends List and Who Can Find You

Your profile shows details about you: where you live, where you went to school, your birthday, your family members. Scammers love these details because they're the answers to common security questions. You choose who sees each one.

To review what's on your profile

1. Go to your profile and choose **Edit profile** or the **About** section.
2. Next to each detail, such as your birthday, hometown or relationship, tap the audience button.
3. Set it to **Friends** or **Only me**. Remove anything you'd rather not share at all.
4. Do the same for your **friends list**. Fake profiles use public friends lists to find your relatives and send them friend requests pretending to be you.

Who can look you up

In Privacy Checkup's **How people can find you** topic (Chapter 13, *Facebook's Privacy Checkup*) you can choose who can send you friend requests and who can look you up using your email address or phone number. Setting these to **Friends** or **Friends of friends** cuts down on strangers finding you.

Locking your profile

Facebook offers a **Lock profile** option, but its help page says it's only available in certain countries. When a profile is locked, people who aren't your friends see only a limited view, and posts you'd shared publicly switch to Friends. If you don't see the option, the settings in this chapter and in Chapter 14, *Who Can See Your Posts* get you most of the same protection.

SCAM ALERT

The "cloned" profile

If a friend gets a new friend request from "you," someone has copied your name and photo. Don't accept it, report it, and tell your friends to ignore it. Hiding your friends list makes this scam much harder.

CHAPTER 16

Meta Accounts Center in Plain English

Meta owns Facebook, Instagram and Messenger. **Accounts Center** is the shared settings area that connects them. If your Facebook and Instagram are linked there, some settings, especially ad settings, apply to both at once.

To open Accounts Center

1. In Facebook, go to **Menu > Settings & privacy > Settings**.
2. Tap **Accounts Center**, usually near the top of the Settings screen.
3. You'll see sections such as **Your information and permissions**, **Ad preferences**, and **Password and security**.

Section	What's inside
Your information and permissions	Download your information, see your activity off Meta technologies, manage connected apps.
Ad preferences	Ad topics, and whether information from partners is used for ads.
Password and security	Change your password, two-factor authentication, where you're logged in.
Accounts	Which Facebook, Instagram or Messenger accounts are linked together.

GOOD TO KNOW

The name may be changing

Meta's own help pages say some people are being moved from Accounts Center to settings called **Meta Account**. If you see Meta Account instead, the same sections live there.

TIP

Check where you're logged in

Under **Password and security**, look for where you're logged in. If you see a phone or computer you don't recognize, log it out and change your password.

CHAPTER 17

Facebook and Instagram Ad Preferences

Facebook shows ads based on what you do on Facebook and Instagram, plus information that advertisers and websites share with Meta. You can't turn ads off, but you can choose topics to see less of, and stop ads based on activity from Meta's partners.

To see fewer ads about a topic

1. Open **Accounts Center** (see Chapter 16, *Meta Accounts Center in Plain English*) and choose **Ad preferences**.
2. Find **Ad topics** and tap **See all** or **View and manage topics**.
3. Choose a topic you don't want, like gambling or alcohol, and select **See less**.
4. To undo it later, choose the topic again and pick **No preference**.

To stop ads based on partner information

1. In **Ad preferences**, open **Ad settings** (on some accounts the tab is called **Manage info**).
2. Tap **Activity information from ad partners**.
3. Tap **Review setting** and choose the **No** option, which stops Meta using that partner information to pick your ads.

GOOD TO KNOW

What this does and doesn't do

Meta says the partner setting applies to all your profiles in the same account. You'll still see ads, and they may still be based on what you do on Facebook and Instagram. Meta also notes not everyone can reach this setting yet.

TIP

Hide a single ad

On any ad, tap the three dots and choose to hide it or say why you don't want to see it. It's a quick way to teach Facebook what you don't care about.

CHAPTER 18

Your Activity Off Meta Technologies

Many shopping sites, news sites and apps send Meta information about what you do there, like viewing a product or adding something to a cart. Facebook calls this **your activity off Meta technologies** (it used to be called Off-Facebook Activity). It's the main reason you see a Facebook ad for the exact lamp you looked at yesterday.

To see it and disconnect it

1. Open **Accounts Center** and choose **Your information and permissions**.
2. Tap **Your activity off Meta technologies**. You'll see a list of businesses that shared your activity.
3. To clear what's there, choose the option to clear or disconnect your previous activity, and confirm.
4. To stop it going forward, tap **Manage future activity**, then **Disconnect future activity**, and confirm.

HEADS UP

You may be logged out of some sites

Disconnecting may log you out of apps and websites where you used **Log in with Facebook**. You can log back in. The change can also take a day or two to settle in.

GOOD TO KNOW

Disconnected isn't the same as deleted

Meta's help explains that disconnected activity is no longer tied to your account, but businesses may still use it without your name attached, for example to measure how their ads perform.

WHAT THIS DOES FOR YOU

Why it's worth doing

This is one of the few settings that reaches beyond Facebook itself. It cuts the link between your shopping and browsing elsewhere and the ads in your Facebook and Instagram feeds.

CHAPTER 19

Apps, Games and Quizzes Connected to Facebook

Every time you clicked **Continue with Facebook** to play a game, take a quiz or sign up for a website, that app may have been given access to some of your Facebook information. Over the years these pile up, and many belong to apps you haven't touched in a decade.

To review and remove connected apps

1. Open **Privacy Checkup** (Chapter 13, *Facebook's Privacy Checkup*) and choose **Your data settings on Facebook**.
2. Or go to **Settings & privacy > Settings** and find **Apps and websites**.
3. Look through the list of active apps. For any you don't use, select it and choose **Remove**.
4. If asked, you can also delete posts or activity that app made on your behalf.

SCAM ALERT

"Fun" quizzes collect real answers

"What was your first car?" "Name your first pet and the street you grew up on!" These quizzes look harmless, but they ask exactly the questions banks use for security. Skip them, and don't answer them in the comments either.

SCAM ALERT

"See who viewed your profile"

Facebook doesn't let anyone see who looked at their profile. Any app or link promising that is a trick to get your password or get access to your account. Don't click it.

TIP

Logging in with Facebook going forward

Using **Log in with Facebook** is convenient, but it links that site to your Facebook account. For shopping sites and games, using your email and a password is often the more private choice.

PART 4

Your iPhone

Apple puts nearly every privacy switch in one place. Here's how to read that screen, decide which apps get your location, and stop apps from tracking you. Written for iOS 26.

CHAPTER 20

The Privacy & Security Screen

On an iPhone, almost everything about privacy lives under one heading: **Settings > Privacy & Security**. Think of it as the control room. The top part lists kinds of information, like Location Services, Contacts, Photos, Camera and Microphone. Tap any one to see which apps have asked for it.

To open it

1. Open the **Settings** app (the gray gear).
2. Scroll down and tap **Privacy & Security**.
3. Tap any item in the list to see which apps can use it.

Item	What it controls
Location Services	Which apps can see where you are. See Chapter 21, *iPhone Location Services, App by App*.
Tracking	Whether apps can ask to follow you across other apps. See Chapter 22, *Ask App Not to Track*.
Contacts, Calendars, Photos	Which apps can read your address book, calendar and pictures. See Chapter 23, *Contacts, Photos, Camera and Microphone*.
Microphone, Camera	Which apps can listen or see through the camera.
Safety Check	A guided review of who and what you share with. See Chapter 24, *Safety Check: When Someone May Be Watching*.
App Privacy Report	A seven-day log of which apps used your data and sensors.

Two more privacy features worth knowing

App Privacy Report (at the bottom of the Privacy & Security screen) shows how often each app used your location, camera, microphone, contacts and photos over the past seven days. Apple says it starts collecting only after you turn it on, and the report stays on your iPhone.

Mail Privacy Protection, at **Settings > Apps > Mail > Privacy Protection**, hides your IP address and stops senders from learning whether you opened their email. Apple notes it doesn't cover links or attachments.

GOOD TO KNOW

App settings moved in recent iOS

On current iPhones, the settings for individual apps are under **Settings > Apps**, then the app's name. Older guides that say "Settings > Mail" mean the same place.

CHAPTER 21

iPhone Location Services, App by App

Location Services lets apps use your iPhone's GPS, Wi-Fi and cell signals to know where you are. Maps needs it. Your weather app likes it. Your solitaire game doesn't need it at all. The trick is to leave Location Services on, and decide app by app.

To change one app's location access

1. Open **Settings > Privacy & Security > Location Services**.
2. Scroll down to the list of apps and tap one.
3. Choose **Never**, **Ask Next Time Or When I Share**, **While Using the App** or **Always**.
4. If the app doesn't need your exact spot, turn off **Precise Location**. The app then gets only your approximate area.
5. Go back and repeat for the next app.

Kind of app	Suggested setting	Precise Location
Maps and navigation	While Using the App	On
Ride and delivery apps	While Using the App	On
Weather	While Using the App	Off is usually fine
Store and restaurant apps	Ask Next Time or Never	Off
Games, puzzles, news	Never	Off
Family locator apps you chose	Always (if you want it to work)	On

HEADS UP

Don't turn off Location Services entirely

Apple warns that many iPhone features stop working when Location Services is off, and Find My can't locate a lost phone. Limiting individual apps gives you almost all the privacy with none of the hassle.

TIP

Spot an app using location right now

Apple says that when an app set to While Using the App is actively using your location, the status bar at the top of the screen may turn blue. It's a handy clue.

GOOD TO KNOW

Photos can carry your location too

Pictures you take may include where they were taken. When you share a photo, tap **Options** at the top of the share screen and turn off **Location** to send it without that information.

CHAPTER 22

Ask App Not to Track

Apps on your iPhone must ask your permission before they track you across other companies' apps and websites for advertising. You've probably seen the pop-up: **Allow "App" to track your activity across other companies' apps and websites?** Choosing **Ask App Not to Track** is almost always the right answer.

To review apps that asked

1. Open **Settings > Privacy & Security > Tracking**.
2. You'll see each app that asked to track you, with a switch beside it.
3. Turn off the switch for any app you'd rather not let track you.

To stop all apps from even asking

1. On the same **Tracking** screen, turn off **Allow Apps to Request to Track**.
2. Apple says any app that asks after that is treated as if you chose Ask App Not to Track.

WHAT THIS DOES FOR YOU

What it does for you

Apple says that with the switch off, apps can't get your phone's advertising identifier, the tag ad companies use to connect your activity from one app to the next. Fewer companies building a profile of you means fewer eerily specific ads.

GOOD TO KNOW

Why the switch may be gray

Apple lists a few reasons you can't change it: child accounts, accounts managed by a school or business, a configuration profile on the phone, or an Apple Account created in the last three days.

TIP

Saying no doesn't break the app

Apps must work the same whether you allow tracking or not. You may see a pop-up promising "more relevant ads" if you allow it. That's all it means.

CHAPTER 23

Contacts, Photos, Camera and Microphone

Location gets the headlines, but your contacts and photos are just as personal. Your address book holds the phone numbers of everyone you know, and your photos hold your family, your house and sometimes your paperwork. Check which apps can see them.

To review an iPhone permission

1. Open **Settings > Privacy & Security**.
2. Tap **Contacts**. Turn off any app that doesn't need your address book.
3. Go back and tap **Photos**. For each app, you can choose no access, limited access to selected photos, or full access.
4. Go back and check **Camera** and **Microphone** the same way.

Good questions to ask about each app

- Do I still use this app? If not, delete it; that removes its access completely.
- Does the app's job need this? A video-calling app needs the camera. A flashlight app doesn't need contacts.
- Would "limited" work? Most apps that want photos only need the few you pick.

TIP

Let the iPhone keep score

Not sure which apps actually use your camera, microphone or contacts? Turn on **App Privacy Report** at the bottom of the Privacy & Security screen (Chapter 20, *The Privacy & Security Screen*), wait a week, and look. Apps that never use a permission they were given are easy candidates to switch off.

HEADS UP

Only you can grant permissions

Permissions are given by tapping Allow on your own phone. No company, bank or "support agent" needs you to change them over the phone. If someone on a call asks you to allow access to your screen or your phone, hang up.

CHAPTER 24

Safety Check: When Someone May Be Watching

Safety Check is an iPhone tool for a harder situation: when you're worried that someone you used to trust, like a former partner or a relative, can see your location, messages or photos. It shows you everything you share and with whom, and lets you stop it quickly.

To open it

1. Open **Settings > Privacy & Security**.
2. Scroll down and tap **Safety Check**.
3. Choose **Manage Sharing & Access** to go through people and apps one at a time, or **Emergency Reset** to stop all sharing at once.

Option	What it does
Manage Sharing & Access	Review who you share location, photos and notes with, and which apps have access. Stop any of it.
Emergency Reset	Immediately stops sharing with all people and apps, and helps you change your passcode and Apple Account password.
Quick Exit	A button that closes Safety Check instantly if someone walks in.

GOOD TO KNOW

What it needs and what it can't do

Apple says Safety Check needs iOS 16 or later and an Apple Account with two-factor authentication. It doesn't cover accounts outside Apple, such as Facebook or Google, or social media sharing.

STAY SAFE

Think before you stop sharing

If you're in a dangerous situation, the other person may notice that sharing stopped. Think about your safety first, and if you're in danger, call 911.

TIP

Android has similar tools

On Android, review shared location in Google Maps and the apps in Chapter 25, *The Android Privacy Dashboard*. Checking your Google Account's devices in Chapter 12, *Google Security Checkup and Connected Apps* helps too.

PART 5

Your Android Phone

Android puts privacy under Settings, with a dashboard that shows what apps have been up to. Written for Android 16 on Google Pixel; Samsung Galaxy and other brands use similar names.

CHAPTER 25

The Android Privacy Dashboard

The **Privacy dashboard** answers a simple question: which apps have been using my location, camera and microphone lately, and when? It shows a timeline for each permission, so an app quietly checking your location in the middle of the night stands out.

To open the Privacy dashboard

1. Open the **Settings** app.
2. Tap **Security & privacy** (on some phones just **Privacy**), then **Privacy** if there's a second step.
3. Tap **Privacy dashboard**.
4. Tap a permission, such as **Location**, to see a timeline of which apps used it and when.
5. Tap an app in the timeline to go straight to its permission and change it.

GOOD TO KNOW

How far back it looks

Google's help says the dashboard shows the last 24 hours on Android 12 and the last seven days on Android 13 and later, which includes Android 16.

TIP

On a Samsung Galaxy

Samsung puts the same tools under **Settings > Security and privacy**, where you'll find the privacy dashboard and **Permission manager**. Samsung's menus vary a little by model and software version.

HEADS UP

Seeing an app you don't recognize

If the dashboard shows an app you never installed using your camera, microphone or location, don't panic, but don't ignore it. Remove its permissions, then uninstall it. If you're unsure, that's a good reason to call me.

CHAPTER 26

Android App Permissions

Every Android app has to ask before it uses your camera, microphone, contacts, photos or location. The **Permission manager** shows each kind of permission and every app that has it, so you can sweep through them in one sitting.

To review by permission

1. Open **Settings > Security & privacy > Privacy** (or **Settings > Privacy**).
2. Tap **Permission manager**.
3. Tap a permission, such as **Contacts** or **Microphone**.
4. Tap any app under **Allowed** and choose a stricter option, such as **Don't allow**.

To review one app

1. Touch and hold the app's icon, then tap **App info** (the small "i").
2. Tap **Permissions**.
3. Tap each permission and change it as you wish.

TIP

Camera and microphone master switches

Pixel phones also have **Camera access** and **Microphone access** switches under privacy controls, which block those sensors for every app at once. They're handy when you want to be sure.

HEADS UP

Think twice about these permissions

Be careful with any app that asks for **Accessibility**, **Display over other apps** or **Install unknown apps**. These are powerful permissions that scam apps abuse. Unless you clearly know why the app needs them, say no.

CHAPTER 27

Android Location Settings

Android lets you decide, app by app, whether it can see your location all the time, only while you're using it, or never. It also lets you give an app just your **approximate** area instead of your exact address.

To change an app's location access

1. Open **Settings > Location**.
2. Tap **App location permissions**.
3. Tap an app and choose **Allow all the time**, **Allow only while using the app**, **Ask every time** or **Don't allow**.
4. Turn off **Use precise location** for apps that only need your town, like weather or shopping apps.

GOOD TO KNOW

How approximate is approximate?

Google's help says approximate location places your phone in an area of about 3 square kilometers, roughly a square mile. That's plenty for a weather forecast, and not enough to find your house.

TIP

Use the same suggestions as iPhone

The table in Chapter 21, *iPhone Location Services, App by App* works for Android too. "While Using the App" on iPhone matches "Allow only while using the app" on Android.

HEADS UP

Keep the main switch on

Turning off **Use location** entirely stops Google Maps directions and keeps Find Hub from locating a lost phone. Limiting individual apps is the better approach.

GOOD TO KNOW

Timeline is separate

These permissions control apps on your phone. Google Maps Timeline, the history of places you've been, has its own settings in the Maps app. See Chapter 9, *Google Maps Timeline: Your Location History*.

CHAPTER 28

Delete Your Android Advertising ID

Every Android phone has an **advertising ID**, a string of letters and numbers that apps use to recognize your phone for advertising. Deleting it removes that tag. Apps still show ads, but they can't use the ID to connect what you do in one app with another.

To delete it

1. Open **Settings**.
2. Tap **Security & privacy**, then **Privacy** (or just **Privacy** on some phones).
3. Tap **Ads**. On some phones it's under **Settings > Google > All services > Ads**.
4. Tap **Delete advertising ID**, then confirm.

WHAT THIS DOES FOR YOU

What it does for you

Google says deleting the ID doesn't create a new one, and apps that try to read it get only zeros. It's the Android cousin of iPhone's Ask App Not to Track (Chapter 22, *Ask App Not to Track*).

GOOD TO KNOW

Ads will still appear

Google's help says apps can still show you ads after you delete the ID; they just may be less relevant. Individual apps can have their own ad settings, too.

TIP

Older phones

On some older Android versions there's no delete button. Instead, look for **Opt out of Ads Personalization** under **Privacy > Advanced > Ads** and turn it on.

CHAPTER 29

Unused Apps Lose Their Permissions

Android has a quiet helper built in: when you haven't opened an app for a long time, Android can take away its permissions, delete its temporary files, and stop it from running in the background. It's like a housekeeper tidying up the apps you forgot about.

To check the setting for one app

1. Touch and hold the app's icon and tap **App info**.
2. Scroll down to **Unused apps** (or **Unused app settings**).
3. Make sure **Pause app activity if unused** is on for apps you rarely use.
4. Turn it off only for an app you want to keep working even when you don't open it, such as a medical-alert or family-locator app.

TIP

If an old app asks for permission again

That's this feature at work. When you open the app again, just allow what it needs. Nothing was lost.

GOOD TO KNOW

Samsung does this too

Samsung says Galaxy phones also remove permissions from apps you haven't used in a while, and you can restore them from the privacy settings.

WHAT THIS DOES FOR YOU

Even better: delete what you don't use

An app you've deleted can't collect anything. Once a year, scroll through your apps and uninstall the ones you don't recognize or don't use. Fewer apps means fewer permissions to worry about.

PART 6

Beyond the Settings

People-search websites, fake privacy apps and quizzes, helping a parent, and a simple twice-a-year routine. Then how to reach me, and a cheat-sheet to keep.

CHAPTER 30

Data Brokers and People-Search Websites

Type your name and town into a search engine and you may find a website listing your address, phone number, age and relatives. These come from **data brokers**: companies that gather public records, marketing lists and other sources, then sell or publish the results. None of the settings in this guide reach them, because they aren't Google or Facebook.

The honest truth

- Much of what they list comes from public records, like property and voter records, so it can't be erased at the source.
- Most people-search sites let you ask them to remove your listing. That's usually called an **opt-out**.
- There are a lot of these sites, and listings can come back after a few months as new records arrive.
- Removing yourself takes patience, not money. You never have to pay to opt out of a site yourself.

To remove a listing yourself

1. Search for your name and town, and note which people-search sites show your information.
2. On each site, scroll to the very bottom of the page and look for a link such as **Opt out**, **Do not sell my info** or **Privacy**.
3. Follow its steps. Many ask you to find your listing and confirm by email. Use an email address you check, but not your main banking email if you'd rather not.
4. Keep a simple list of which sites you contacted and when.
5. Check again in about six months. Repeat if a listing has come back.

Paid removal services

Several companies will do these opt-outs for you for a yearly subscription. They save time, and some people find that worth paying for. Know three things first: no service can remove public records at the source, no service reaches every site, and prices and what's included change often, so read the current price and cancellation terms before you sign up. I don't recommend or earn anything from any of them.

SCAM ALERT

Pay-to-remove demands

If a website demands money to take down your information, or an email says your data "has been found on the dark web" and asks you to pay right now, slow down. Real opt-outs are free, and pressure to pay immediately is a classic scam sign.

TIP

Freeze your credit too

A credit freeze with the three credit bureaus doesn't hide your address, but it stops anyone from opening new credit in your name with the details these sites show. It costs nothing and can be lifted any time.

CHAPTER 31

Fake Privacy Apps, Quizzes and Scare Pop-ups

Privacy worries are big business for scammers. They know people feel watched, so they offer to fix it, for a fee or for your password. The real fixes are the free settings in this guide. Here's what the fakes look like.

Warning signs

What you see	What it really is
"Your phone is being tracked!" pop-ups	A web page can't scan your phone. It's an ad trying to scare you into installing something or calling a number.
"Privacy cleaner" or "anti-tracking" apps with big subscriptions	Your phone's own settings do the same job. Watch for weekly charges after a short trial.
"Facebook privacy notice" posts	Copy-and-paste posts declaring you don't give permission don't change anything. Facebook's settings are the only switches that count.
"See who viewed your profile" apps	Facebook doesn't offer this. These are trying to get into your account.
Personality and memory quizzes	"Your first car + your birth month = your rock star name." They collect answers to security questions.
A caller offering to fix your privacy	Nobody from Google, Apple, Facebook or Microsoft calls to fix your settings. Hang up.

If you already clicked or installed something

1. Don't panic, and don't call any number the pop-up gave you.
2. Close the web page or app. If a page won't close, close the browser completely or restart the phone.
3. If you installed an app, delete it. Then check its subscription: iPhone, **Settings**, tap your name, then **Subscriptions**; Android, open the **Play Store**, tap your picture, then **Payments & subscriptions**.
4. If you typed a password into it, change that password right away and turn on two-step verification.
5. If you gave a card number or let someone onto your computer, call your bank using the number on your card, then call me.

SCAM ALERT

The rule that covers them all

Real privacy protection never needs your password, never needs remote access to your computer, and never needs to be paid for with gift cards. If any of those come up, it's a scam.

TIP

Feeling embarrassed? Don't be

These tricks are designed by professionals to catch smart people on a busy day. The faster you act, the less harm they do.

CHAPTER 32

Helping a Parent with a Privacy Checkup

Grown children often ask how to help a parent tighten their privacy. The best checkup is one you do *together*, with the phone in your parent's hands, so they understand each change and can make their own choices.

A gentle way to do it

1. Ask first. "Would you like me to show you how to keep strangers off your Facebook?" goes over better than taking the phone.
2. Start with what matters to them: grandkid photos staying private, fewer creepy ads, no more scam calls.
3. Make one change at a time, and explain it in a sentence. Let them tap the switch.
4. Write down what you changed, so they know where to look later.
5. Leave Find My or Find Hub and location sharing with family on if everyone agrees it's useful.

STAY SAFE

Respect their choices and their passwords

It's their account. Don't change passwords without them knowing, and don't turn on location sharing with yourself without asking. Trust matters more than any setting.

TIP

Doing it from far away

Google's and Facebook's settings can be checked together over a video call, with your parent sharing the screen of their computer. Phone settings are easier in person, or with clear written steps from this guide.

FROM BILL

When it's easier to have someone else do it

Sometimes a parent is more comfortable with an outside helper than with their kids. That's part of what I do in a Digital Safety Check-Up, in your parent's home or remotely.

CHAPTER 33

Your Twice-a-Year Privacy Routine

Privacy settings aren't one-and-done. Apps update, new apps get installed, and companies add new settings. A short look twice a year keeps everything where you want it. Pick two easy-to-remember dates, like the weekends the clocks change.

The 20-minute routine

1. **Phone:** open the Privacy dashboard (Android, Chapter 25, *The Android Privacy Dashboard*) or App Privacy Report (iPhone, Chapter 20, *The Privacy & Security Screen*). Remove permissions from apps that surprise you.
2. **Phone:** scroll through your apps and delete ones you no longer use.
3. **Google:** run Privacy Checkup and Security Checkup (Chapter 5, *Google's Privacy Checkup*, Chapter 12, *Google Security Checkup and Connected Apps*). Check for any new Search settings.
4. **Facebook:** run Privacy Checkup (Chapter 13, *Facebook's Privacy Checkup*) and look over connected apps (Chapter 19, *Apps, Games and Quizzes Connected to Facebook*).
5. **Search yourself:** look up your name and town and opt out of any new people-search listings (Chapter 30, *Data Brokers and People-Search Websites*).

TIP

Set a calendar reminder

Add a repeating event to your phone's calendar called "Privacy checkup" every six months. When it pops up, open this guide and go down the list.

GOOD TO KNOW

New phone? Start fresh

When you set up a new phone, it asks about location, tracking and analytics during setup. Take your time on those screens; that's when it's easiest to say no.

WHAT THIS DOES FOR YOU

What you get for 20 minutes

Fewer apps watching you, fewer ads following you, and the peace of mind that comes from knowing what's shared and with whom.

CHAPTER 34

When to Call Bill

Most of this guide you can do yourself, one setting at a time. But some situations are easier with someone sitting beside you, or on the phone with you, who has done it many times.

Good reasons to call

- You'd like the whole checkup done with you, start to finish, on your phone, computer and accounts.
- Security Checkup or Accounts Center shows a device or login you don't recognize.
- You think someone may be tracking your phone or reading your messages.
- You installed a "privacy" app or clicked a pop-up, and now there are charges or strange behavior.
- You're helping a parent and would like an outside helper to walk them through it.
- The menus on your phone don't match this guide and you can't find a setting.

The Digital Safety Check-Up

This guide pairs with my **Digital Safety Check-Up**. We go through your phone, computer, Google, Apple and Facebook accounts together: privacy settings, app permissions, passwords and two-step verification, and the scam warning signs to watch for. You make every choice; I explain and do the tapping if you'd like.

SCAM ALERT

I'll never call you out of the blue

I don't make surprise calls about your privacy or your accounts. If someone calls saying they're from "Bill's Home Tech" or any tech company and you didn't call them first, hang up and call me at the number below.

FROM BILL

How to reach me

Call or text **(330) 200-8042**, or book online at **billshometech.com/book**. Bill's Home Tech serves Portage County, Ohio, with 30+ years of professional experience. If you reach my assistant **Sophie** on the main line, she can answer simple questions and get you on my schedule. My help is **$49 remote · $99 in your home**. The guides themselves are always yours to read and share.

— Bill

CHAPTER 35

Your Privacy Checkup Cheat-Sheet

The most-used steps in one place. Each one has full directions in its chapter.

Google

I want to…	Go here
Privacy Checkup	myaccount.google.com > Data & privacy > Privacy Checkup
See or delete history	myactivity.google.com > Delete
Auto-delete history	myactivity.google.com > Web & App Activity > Auto-delete > 3 months
Location history	Google Maps app > profile picture > Your Timeline / Settings
YouTube history	myactivity.google.com > YouTube History > Auto-delete
Personalized ads	myadcenter.google.com > Personalized ads > Off
Security Checkup	myaccount.google.com/security-checkup

Facebook

I want to…	Go here
Privacy Checkup	Profile picture or Menu > Settings & privacy > Privacy Checkup
Old posts to Friends	Settings > Limit who can see past posts
Ad topics	Accounts Center > Ad preferences > Ad topics
Off-Meta activity	Accounts Center > Your information and permissions > Your activity off Meta technologies
Connected apps	Settings > Apps and websites > Remove

iPhone and Android

I want to…	Go here
iPhone location by app	Settings > Privacy & Security > Location Services
iPhone tracking	Settings > Privacy & Security > Tracking
iPhone Safety Check	Settings > Privacy & Security > Safety Check
Android permissions	Settings > Security & privacy > Privacy > Permission manager
Android location by app	Settings > Location > App location permissions

I want to…	Go here
Android ad ID	Settings > Security & privacy > Privacy > Ads > Delete advertising ID

Five safety rules

1. Change privacy settings only inside the real settings, never through an app or a caller.
2. Skip quizzes that ask about your first car, pet, school or street.
3. Never pay to opt out, and never pay with gift cards.
4. Keep Find My or Find Hub, updates and two-step verification turned on.
5. If you clicked something you shouldn't have, change the password and call for help.

Keep this handy

Item	My notes
Date of my last checkup	_____
Next checkup due	_____
Google account email	_____
Facebook login email or phone	_____
People-search sites I opted out of	_____
Bill's Home Tech	(330) 200-8042 · billshometech.com/book

FROM BILL

You did it

A privacy checkup is one of the most worthwhile hours you can spend on your devices. Do it once, glance at it twice a year, and call me if anything looks off.