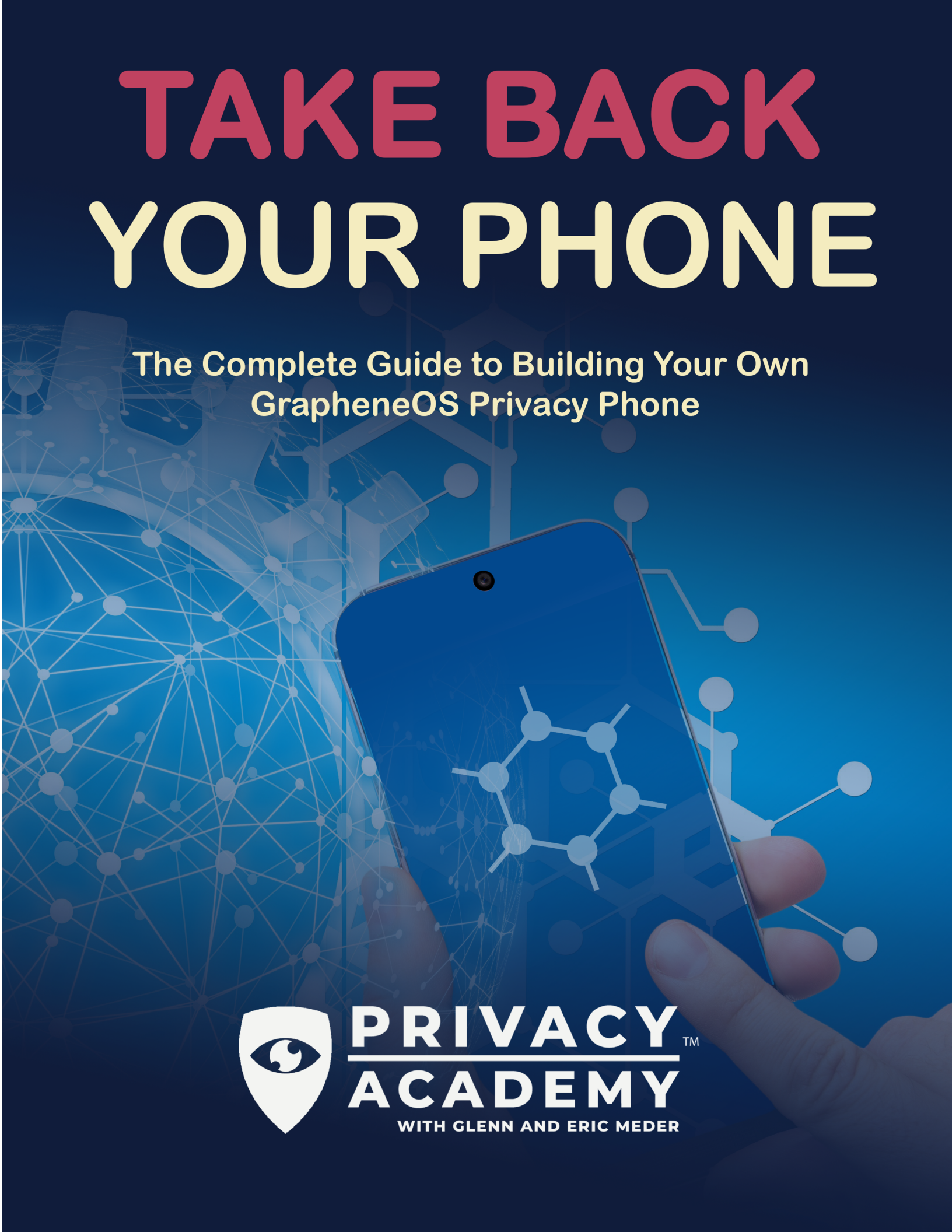
TAKE BACK YOUR PHONE

The Complete Guide to Building Your Own GrapheneOS Privacy Phone



PRIVACY™ ACADEMY

WITH GLENN AND ERIC MEDER

TAKE BACK YOUR PHONE

The Complete Guide to Building Your Own GrapheneOS Privacy Phone

A Privacy Academy Companion Guidebook

Written by the Privacy Academy Expert Team

The information in this book reflects publicly available research, official GrapheneOS documentation, and independent reporting as of the date of publication (April 2026). Mobile operating systems, device support, and security landscapes evolve rapidly. Always verify current details — especially device compatibility and installation steps — at the official GrapheneOS website (https://grapheneos.org/) before making purchases or beginning installation.

TABLE OF CONTENTS

CHAPTER 1

Welcome to the Privacy Revolution

You're holding (or about to hold) one of the most powerful tools for personal privacy that exists today — a phone running GrapheneOS.

If you're reading this, you've already taken the most important step: you've decided that your personal data, your location history, your private conversations, and your digital life should belong to you — not to a trillion-dollar corporation designed to spy on you.

This guidebook is designed to walk alongside you through our full GrapheneOS Course (*Create Your Own Privacy Phone*). Think of it as your quick-reference companion — something you can flip open while you're setting up your phone, or revisit when you need a refresher. We wrote it in plain language, free of unnecessary jargon, because privacy shouldn't require a computer science degree.

This book will explain what GrapheneOS is and why it matters in terms anyone can understand. It will show you exactly which phone to buy, where to buy it, and what to look for. It will walk you through the installation process from start to finish. It will guide you through setup and help you find the apps you need through alternative app stores like F-Droid, Accrescent, and Aurora Store. And it will give you the confidence to make this switch and never look back.

Let's get started.

CHAPTER 2

What is Graphene OS?

GrapheneOS is a free, open-source operating system for your smartphone. It's based on Android — so it looks and feels familiar — but it has been rebuilt from the ground up with one goal: to protect your **privacy and security.**

The Simple Explanation

Think of it this way: if a regular Android phone is a house with the doors unlocked and the windows wide open, GrapheneOS is that same house with reinforced doors, deadbolt locks, security cameras, and bulletproof glass — except you hold all the keys.

Who Made It?

GrapheneOS was originally founded by Daniel Micay, a respected security researcher, in late 2014.

The project grew out of his earlier open-source privacy and security work, including the development of CopperheadOS.

In May 2023, Micay stepped down as lead developer, citing escalating harassment and safety concerns.

Since then, the project has transitioned to a small, distributed core team of multiple full-time and part-time developers, supported by donations and organizational collaborators, operating under the GrapheneOS Foundation — a Canadian non-profit.

This matters because GrapheneOS isn't made by a company trying to sell your data. It's made by a dedicated team of security-focused developers who genuinely believe your phone should work for you, not for advertisers.

The project is entirely open-source, which means anyone on Earth can inspect the code. There are no hidden trackers. No secret data collection. No backdoors. Everything is transparent and verifiable. When GrapheneOS says it doesn't collect your data, you don't have to take their word for it — anyone with the technical skill can verify it themselves.

What Makes It Different?

Zero telemetry. Your phone doesn't secretly send data about you to anyone — not to Google, not to GrapheneOS, not to advertisers, not to anyone. Period.

Hardened security. GrapheneOS includes advanced security features that go far beyond what stock Android or even Apple's iOS offers. It uses a hardened memory allocator (hardened_malloc), enhanced sandboxing between apps, and aggressive exploit mitigations.

The technical details are deep, but the result is simple: your phone is significantly harder to hack, exploit, or compromise than any stock smartphone on the market.

You control permissions. Want to deny an app access to your camera, microphone, contacts, or location? GrapheneOS gives you granular control that stock phones simply don't offer. You can even revoke network access from individual apps — meaning you can install an app but prevent it from ever connecting to the internet. Neither Apple nor Google gives you this capability natively. This single feature alone is a game-changer for privacy.

No Google services baked in. Out of the box, there are no Google services running in the background collecting data. If you need Google apps for compatibility, you can install them in a special "sandbox" that prevents them from accessing your personal data. GrapheneOS pioneered this sandboxed Google Play approach — it was the first operating system to offer truly sandboxed Google Play services, and it remains the gold standard for this capability.

Verified boot with a locked bootloader. Your phone verifies its own integrity every time it starts up. If anyone has tampered with the software — whether a hacker, a government, or anyone else — the phone will detect

it and alert you. Most other custom phone operating systems do not offer this by default, which disables this critical protection.

Is It Hard to Use?

No. If you've ever used an Android phone, GrapheneOS will feel immediately familiar. The home screen, the settings menu, the notification shade, the app drawer — it all works the way you'd expect. You swipe, tap, and navigate just like before. The difference is what's happening (or rather, not happening) behind the scenes. Instead of your phone quietly reporting your every move to corporate servers, it simply does what you tell it to do — nothing more, nothing less.

CHAPTER 3

Why Your Current Phone Can't Be Trusted

This information is challenging — but essential. Take your time with it.

Your smartphone is the most intimate surveillance device ever created. It knows where you sleep, live, and work, what you search for and buy, what you read, what you photograph, who you talk to, and what you believe. Right now, that information is being collected, stored, analyzed, and monetized — whether you use an iPhone or a standard Android device.

The Android Problem

Google's Android operating system powers the vast majority of smartphones on Earth. It is, by design, a data-collection platform. Google's primary business is advertising, and advertising requires data — your data.

When you use a stock Android phone, Google services are deeply embedded into the operating system. They run continuously in the background, collecting enormous amounts of data about you. This includes your precise GPS location — often even when you've turned location services "off." It includes every search you make, every app you open, and how long you spend using it. It includes your contacts, calendar entries, and emails if you use Gmail. It includes voice data from Google Assistant interactions. It includes the Wi-Fi networks you connect to and persistent device identifiers that track your activity across different apps and websites, building a profile of your behavior.

Independent research has repeatedly documented that Android devices transmit data to Google servers frequently throughout the day — even when the phone is sitting idle in your pocket, not being actively used. This isn't speculation or conspiracy theory. This is publicly documented, independently verified, reproducible behavior.

Here's what makes it worse: even when users go into their settings and try to limit data collection, research has repeatedly shown that Google's collection is extremely difficult — and in some cases functionally impossible — to fully disable on a stock Android device. The privacy controls that exist often reduce the visibility of data collection to the user without actually stopping the collection itself. You think you've turned it off. You haven't.

The Apple Problem

Many people assume iPhones are the "private" choice. Apple has spent billions of dollars on marketing campaigns telling you exactly that. However, the reality is considerably more complicated than the commercials suggest.

While Apple's business model is less directly dependent on advertising revenue than Google's, Apple devices still collect substantial amounts of user data. Independent security researchers have documented that iPhones transmit analytics and telemetry data to Apple servers, including location-related information, device usage patterns, and detailed app activity data — even when users have explicitly opted out of analytics sharing in their settings. The opt-out toggle, in practice, does not stop all data collection.

Apple's ecosystem is also a tightly controlled "walled garden." Apple decides what software you're allowed to install. Apple decides what you can do with your device. Apple decides what repairs are permitted and who can make them. You paid for your iPhone, but you don't truly own it in any meaningful sense — you are permitted to use it under Apple's terms and conditions, which Apple can change at any time.

Apple stores iCloud data — including backups, photos, messages, contacts, and documents — on its servers. While Apple has introduced some end-to-end encryption options in recent years, they've historically complied with government and law enforcement data requests and retain the technical ability to access much of the data stored in its cloud infrastructure. Your "private" data sitting in iCloud is only as private as Apple decides.

Perhaps most critically: **Apple's software is entirely proprietary and closed-source.** No independent researcher, no security auditor, no journalist, and no government regulator can fully examine what an iPhone is doing behind the scenes. When Apple tells you your privacy is protected, you are trusting their word — and their word alone. That trust has been challenged

numerous times by independent security research that revealed data collection practices Apple had not publicly disclosed.

Third-Party App Tracking

Beyond the operating system itself, the apps you install on a conventional smartphone are often just as invasive — sometimes more so. Popular apps contain many embedded software trackers that monitor your behavior, build detailed advertising profiles, and share your data with large networks of third-party companies you've never consented to share information with.

These trackers can record which screens you view within an app, how long you spend on each one, what you tap on, what you search for, what you purchase, and even how you hold your phone. This data is combined with information from other apps and other devices to build a shockingly detailed portrait of who you are.

On a stock Android or iOS phone, you have limited ability to control this. You can deny some permissions, but trackers are often embedded so deeply in app code that they function regardless. On GrapheneOS, you have powerful tools to fight back — including the ability to completely cut off an app's network access while still using its offline features. An app can't send your data to a tracker if it can't connect to the internet.

The Bottom Line

The question is no longer whether your current phone is collecting your data. It is — aggressively, continuously, and in ways you almost certainly haven't fully consented to or even been informed about.

The question is: **what are you going to do about it?**

GrapheneOS is the answer.

CHAPTER 4

What to Expect When You Switch

Switching to GrapheneOS is one of the best decisions you can make for your digital privacy. But let's set honest expectations so you're fully prepared and never caught off guard.

What Stays the Same

GrapheneOS is based on Android, so the interface is immediately familiar to anyone who's used an Android phone. You'll swipe, tap, and navigate the same way you always have. All core functionality works perfectly — calling, texting, Wi-Fi, Bluetooth, NFC, and the camera. Web browsing works great with the included Vanadium browser (a security-hardened version of Chromium), and you can install alternatives like Brave or Firefox. The vast majority of apps work perfectly on GrapheneOS, especially if you install Sandboxed Google Play services.

What Changes

You don't need a Google account to use your phone. You can set up and use your device without ever signing into Google — something that's practically impossible on a stock Android phone. If you do need Google services for specific apps, you can install them in a sandboxed environment where they have no special privileges.

You'll be more in charge of permissions. GrapheneOS will ask you to make explicit decisions about what each app can access. This is a feature, not a burden — but it does mean you'll be more hands-on during the first few days as you configure your apps.

A small number of apps that are deeply dependent on Google services may not work perfectly without Sandboxed Google Play, or may require minor adjustments. Banking apps, for example, generally work fine — but the occasional outlier may need troubleshooting.

If you choose not to install Google Play services, some apps won't deliver push notifications. Installing Sandboxed Google Play resolves this for most apps.

Your phone won't come loaded with bloatware — no carrier apps, no manufacturer apps, no pre-installed social media. It's clean, minimal, and fast.

Why Switch?

Because every day you wait is another day your current phone is harvesting your personal data. Because the tools exist right now to take back your privacy and they're free. Because you deserve a phone that works for you instead of against you. And because once you experience what a truly private phone feels like, you'll wonder why you didn't do this sooner.

The Adjustment Period

Most people report a brief adjustment period of three to five days as they install apps, configure permissions, and learn the new features. After that, using GrapheneOS feels completely natural. The overwhelming majority of users say they would never go back to a stock phone.

CHAPTER 5

Choosing and Buying Your Pixel Phone

Why It Has to Be a Pixel

GrapheneOS currently runs on Google Pixel phones.

This surprises people — "Why a *Google* phone for a *privacy* operating system?" The answer is hardware security.

Pixel phones include a dedicated **Titan security chip** (the Titan M on the Pixel 6 series, and the upgraded Titan M2 on the Pixel 7 and newer). This is a dedicated security processor that protects your encryption keys, verifies

your operating system's integrity at boot, and resists physical tampering attempts. Pixel phones also support **verified boot with bootloader re-locking** — meaning you can unlock the bootloader to install GrapheneOS, then lock it again afterward. This is critical because a locked bootloader means the phone cryptographically verifies that the software hasn't been tampered with every single time it starts up. Most other Android phones don't support re-locking after installing a custom operating system, which makes them fundamentally less secure.

Google also provides **consistent, timely security updates** for Pixel hardware, which the GrapheneOS team integrates rapidly.

Once you wipe the stock operating system and install GrapheneOS, there is zero Google software on the device. You're using Google's excellent, security-focused hardware paired with privacy-respecting software. It's the best of both worlds.

Note: GrapheneOS has indicated it is in discussions with other device manufacturers about expanding device support in the future.

Always check the official GrapheneOS website for the latest supported device information.

New vs. Used — Both Work Great

Buying new gives you the longest possible support lifespan. Google provides up to 7 years of security updates for the Pixel 8 and newer models, and 5 years for the Pixel 6 and 7 series. GrapheneOS supports devices for the full duration of Google's security update commitment. You also get no risk of prior hardware damage or tampering, and a full manufacturer warranty.

Buying used is significantly more affordable and still perfectly functional for GrapheneOS. Many people buy a used Pixel specifically for this purpose and save hundreds of dollars. The key consideration is the remaining support timeline — an older model will reach end-of-life sooner, meaning it will eventually stop receiving security updates. Check the support timeline before buying and make sure you're comfortable with how long the device will remain supported.

When buying used, purchase from reputable sources and inspect the phone carefully for signs of water damage, screen damage, or battery degradation. If buying in person, power the phone on and test basic functions before completing the purchase.

Where to Buy — It MUST Be Unlocked

Whether you buy new or used**, the phone must be carrier-unlocked**. This is absolutely non-negotiable. A carrier-locked phone (one tied to Verizon, AT&T, T-Mobile, or any other carrier) may prevent you from enabling OEM unlocking in Developer Options, which means you cannot install GrapheneOS. Don't learn this the hard way — verify before you buy.

For new phones: The **Google Store** is the safest option — every phone sold directly by Google is unlocked. **Best Buy** sells unlocked Pixels, but you must specifically select the unlocked version rather than a carrier model — they are listed separately and it's easy to grab the wrong one. **Amazon** also carries unlocked models, but verify the seller is reputable and double-check that the listing explicitly says "unlocked." **B&H Photo** is another reliable source for unlocked devices.

For used phones: Swappa is a well-regarded marketplace specifically for used phones, and listings clearly indicate whether the device is unlocked. **eBay** works well if you buy from sellers with high ratings and positive

feedback — confirm the phone is unlocked before bidding. **Local marketplaces** like Facebook Marketplace and Craigslist can offer excellent deals, but exercise caution — verify the phone is unlocked, check that it's not reported stolen, and always meet in a public place. **Refurbished sellers** like **Back Market** can be a good middle ground between new and used pricing.

What to Verify Before You Buy

First, confirm the phone is carrier-unlocked. Ask the seller explicitly. If buying in person, insert your SIM card and confirm it works on your carrier.

Second, check that the phone isn't reported lost or stolen. Dial *#06# on the phone to display the IMEI number, then run it through a free online IMEI checker.

Third, verify the phone model is on GrapheneOS's supported device list (covered in the next chapter).

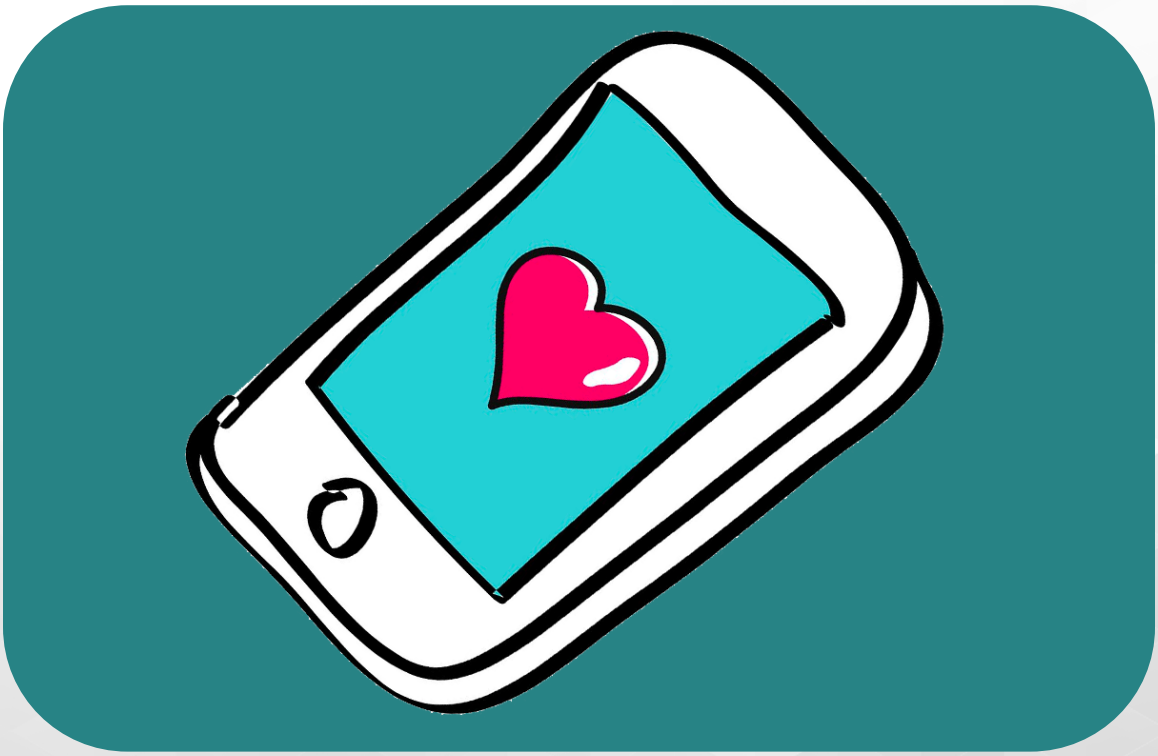
Fourth, if buying used, ask the seller to confirm that "OEM unlocking" can be toggled on in Developer Options. Some carriers permanently disable this setting even on phones that are otherwise "unlocked," which would prevent GrapheneOS installation.

A Privacy Tip for Maximum Anonymity

If your goal is maximum privacy and you don't want the phone linked to your identity at all, consider purchasing it with cash at a physical retail store. This avoids creating a record connecting you to the device through a credit card or online order. This step is entirely optional and goes beyond what most people need — but if you're serious about operational security, it's the gold standard.

CHAPTER 6

Which Devices Are Compatible?



GrapheneOS maintains an official list of supported devices on its website. **Always check this list before purchasing a phone** — it is updated as new devices are added and older ones reach end-of-life. The following reflects the landscape as of early 2026, but may have changed by the time you read this.

Pixel 10 Series (released 2025): GrapheneOS has released experimental builds for the Pixel 10 series.

Check the official website for the current status of Pixel 10 support — by the time you're reading this, stable builds may be available. These newest devices will have the longest remaining support windows.

Pixel 9 Series (released 2024, approximately 7 years of support): This includes the Pixel 9, Pixel 9 Pro, Pixel 9 Pro XL, and Pixel 9 Pro Fold. These are fully supported with stable builds and have excellent long-term support ahead.

Pixel 8 Series (released 2023–2024, approximately 7 years of support): This includes the Pixel 8, Pixel 8 Pro, and Pixel 8a. Excellent devices with many years of support remaining. The Pixel 8 was the first generation where Google committed to 7 years of updates.

Pixel 7 Series (released 2022–2023, approximately 5 years of support): This includes the Pixel 7, Pixel 7 Pro, and Pixel 7a. Still well-supported with a few years of updates remaining as of this writing.

Pixel 6 Series (released 2021–2022, approximately 5 years of support): This includes the Pixel 6, Pixel 6 Pro, and Pixel 6a. These are nearing or at end-of-life for security updates. Check the official GrapheneOS website to confirm whether these devices are still actively supported before purchasing one.

Pixel Tablet (released 2023, approximately 5 years of support): This is supported and makes a great secondary device for home use, but note that it's Wi-Fi only with no cellular capability.

Our Recommendations

For the **best value**, look at the Pixel 8a. It offers excellent performance, a long support window (through approximately 2031), and is available at a very reasonable price.

For the **best overall experience**, the Pixel 9 Pro or a supported Pixel 10 model gives you top-tier hardware, an excellent camera, and the longest remaining support.

For **budget buyers**, a used Pixel 7 or Pixel 8 is widely available, well-supported, and can often be found for a fraction of the original retail price.

We recommend avoiding the Pixel 6 series for new purchases since these devices are at or approaching end-of-life for security updates. If you already own one, it may still be worth installing GrapheneOS — but plan to upgrade soon.

CHAPTER 7

Installing Graphene OS Step By Step

This is the part that intimidates most people — but we promise, it's far simpler than you think. The GrapheneOS team has built a **web-based installer** that handles almost everything automatically. You don't need to type commands into a terminal. You don't need programming knowledge. If you can plug in a USB cable and click a few buttons, you can do this.

What You'll Need

You need your Pixel phone charged to at least 80%. You need a computer — Windows, macOS, Linux, or ChromeOS all work. You need a USB-C data cable, and this is important: it must be a data cable, not a charge-only cable. Many cheap cables only carry power and won't work for this. If your cable came in the box with a Pixel phone, it's a data cable. You need a web browser — specifically Chrome, Chromium, Brave, or Edge. Firefox and Safari may not support the WebUSB technology that the installer requires. On Linux - avoid Flatpak and Snap versions of browsers, which can cause problems. You need an internet connection. And you need approximately 30 to 45 minutes of uninterrupted time.

Prepare Your Phone

Step 1: If this is a new phone, go through the minimal stock Android setup. You do not need to sign into a Google account — skip everything you can and just get to the home screen.

Step 2: Connect the phone to Wi-Fi and install all pending system updates. Go to **Settings → System → System Update** and keep checking and updating until the phone says no more updates are available. This step ensures your phone's firmware is current, which GrapheneOS requires. Don't skip it.

Step 3: Enable Developer Options. Go to **Settings → About Phone** and tap **Build Number** exactly seven times. You'll see a countdown and then a message confirming that Developer Options are now enabled.

Step 4: Enable OEM Unlocking. Go to **Settings → System → Developer Options** and find the toggle for **OEM Unlocking**. Turn it on and confirm. If this toggle is grayed out and you cannot enable it, your phone is almost

certainly carrier-locked. You will need to contact the carrier to request an unlock, or return the phone and purchase a confirmed unlocked model.

Run the Web Installer

Step 5: On your **computer**, open a supported browser and navigate to the official GrapheneOS website. Find the Install page and open the web installer.

Step 6: Power off your Pixel phone completely.

Step 7: Boot into Fastboot Mode by holding the **Power button** and **Volume Down button** simultaneously. Keep holding both buttons until you see the fastboot screen — it will show a small Android robot and some text. This is normal.

Step 8: Connect your phone to your computer using the USB-C data cable.

Step 9: In the web installer on your computer, click **"Unlock Bootloader."** Follow the on-screen prompts. On the phone, you'll need to use the volume keys to highlight "Unlock" and press the power button to confirm. The phone will factory reset itself — this is expected and normal.

Step 10: The web installer will now automatically download the latest GrapheneOS image for your specific device model. This may take several minutes depending on your internet speed. Be patient and don't disconnect anything.

Step 11: Click **"Flash Release"** to begin installing GrapheneOS onto your phone. The installer will flash all the necessary software components to your device. **Do not disconnect the phone or close the browser during this process.** Let it complete fully.

Step 12: Once flashing is finished, the installer will prompt you to lock the bootloader. This is a critical security step — **do not skip it**. Locking the bootloader re-enables verified boot, which means your phone will cryptographically verify its software integrity every time it powers on. Click "Lock Bootloader" in the installer and confirm on the phone using the volume and power buttons.

Step 13: The phone will reboot. When it starts up, you'll see the GrapheneOS setup screen. You now have GrapheneOS installed with a locked bootloader and full verified boot protection. Congratulations — you did it.

Quick Troubleshooting

If the web installer says "No device found," the most common cause is the USB cable. Try a different cable (make sure it's a data cable, not charge-only) or try a different USB port on your computer. Avoid USB hubs — plug directly into the computer.

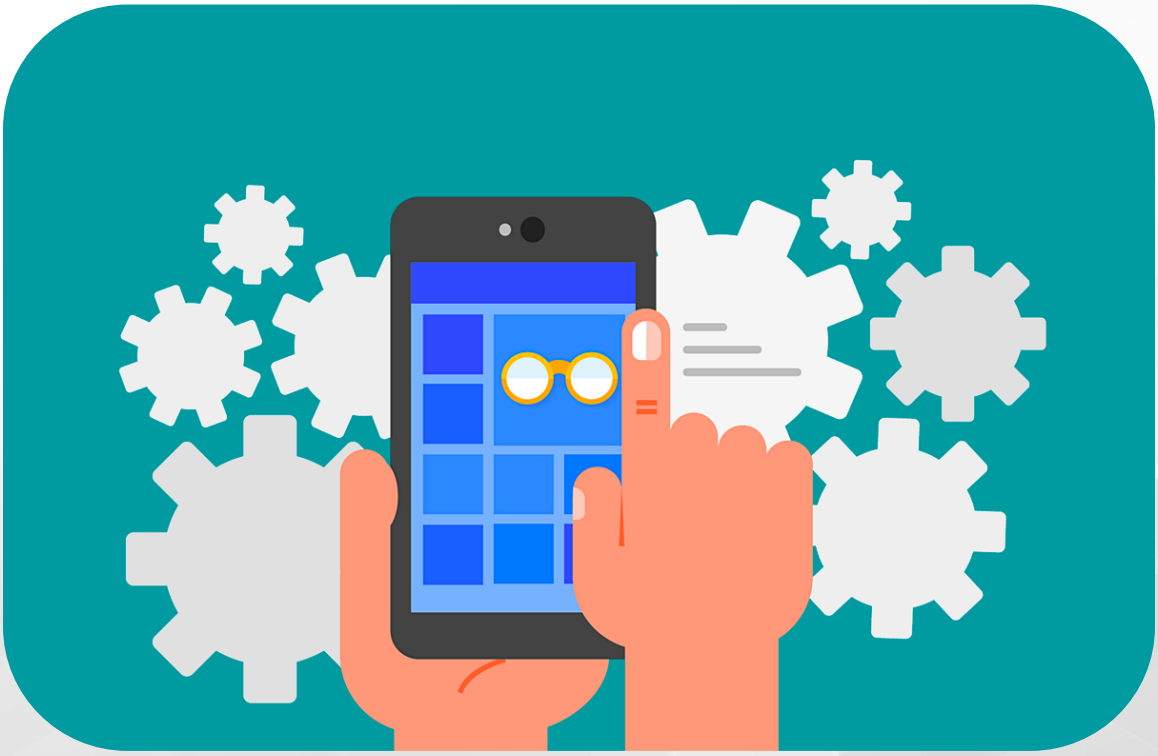
If OEM Unlocking is grayed out in Developer Options, the phone is likely carrier-locked. This must be resolved before you can proceed.

If the flashing process seems stuck or frozen, be patient. Large file transfers can take time, especially on slower connections. Only be concerned if there has been absolutely zero progress for more than 10 minutes.

For more detailed troubleshooting, refer to our full course materials and join our live training sessions where instructors can help you work through any issues in real time.

CHAPTER 8

Setting Up Your New Privacy Phone



Your phone has rebooted into GrapheneOS for the first time. Welcome to your new, private digital life. Let's set it up properly.

Initial Setup

Select your language and region. Connect to Wi-Fi — you'll need internet access to download apps. Skip any account sign-in prompts. GrapheneOS does not require any account to function, and you should not sign into anything during initial setup.

Set a strong PIN or password. We recommend a 6-digit PIN at minimum, or better yet, a longer alphanumeric passphrase. This isn't just a screen lock — it's the encryption key for your entire device. Every piece of data on your phone is encrypted with this code. Make it strong.

You can optionally set up fingerprint unlock for daily convenience. Your fingerprint data is stored locally on the Titan security chip inside the phone and never leaves the device — it is never uploaded anywhere.

Essential Settings to Configure

Network Permissions: This is one of GrapheneOS's most powerful features. In app settings, you can toggle internet access on or off for each app. Got a calculator app that doesn't need internet access? Turn it off. A notes app that works fine offline? Turn it off. This prevents apps from silently transmitting data in the background. No stock phone gives you this control.

Location Services: Keep location turned off by default. Enable it only when you specifically need it — for navigation, for example — and only grant location permission to the specific app that needs it. Turn it back off when you're done.

Scramble PIN Layout: In security settings, enable the scrambled PIN input. This randomizes the position of your PIN pad numbers every time you unlock your phone, preventing anyone from getting your PIN by watching your finger movements or by analyzing smudge patterns on your screen.

Auto-Reboot: GrapheneOS includes a powerful security feature that automatically reboots the phone if it hasn't been unlocked for a set period

of time. When the phone reboots, it enters a "Before First Unlock" state where all data on the device is fully encrypted and inaccessible — even to sophisticated forensic tools. This means that if your phone is ever lost, stolen, or seized, the data is protected as long as the auto-reboot has triggered. You can find and adjust this feature in your security settings. Check the current default when you set up your phone and decide what interval works best for your situation.

Exploit Protection: In security settings, toggles for advanced memory-related security features are set to sensible defaults. Leave them as-is unless specifically directed otherwise in the full course.

Note: GrapheneOS updates its interface between versions, so exact settings menu paths may shift over time. If you can't find a setting we've described, use the search function in Settings — it will locate any feature by keyword.

User Profiles — Your Secret Weapon

One of GrapheneOS's most powerful and underutilized features is **multiple user profiles**. Each profile is completely isolated from every other profile — it's like carrying multiple separate phones in a single device. Each profile has its own apps, its own data, its own encryption keys, and its own storage. An app installed in one profile cannot see, access, or even detect data in another profile. This isolation is enforced at the hardware level.

Here's how we recommend using them:

Your **Owner Profile** is your main, everyday profile. Keep it clean and minimal. Install only the apps you trust most here.

Create a **secondary profile** for apps that require Google Play services. Install Sandboxed Google Play in this profile only. This keeps all of Google's services completely walled off from your primary profile — Google can't see your main contacts, photos, files, or any other data.

Optionally, create a **third profile** for anything especially sensitive or private. It has its own completely separate encryption and storage.

To create additional profiles, go to **Settings → System → Multiple Users → Add User**. You can switch between profiles from the lock screen.

Installing Sandboxed Google Play (Optional but Recommended)

Many popular apps depend on Google Play services to function — for push notifications, in-app purchases, maps functionality, and more. On a stock Android phone, Google Play services have deep, system-level access to your entire device. GrapheneOS solves this with **Sandboxed Google Play** — a version of Google's services that runs as a regular app with no special privileges. It can only access what you explicitly allow, like any other app.

To install it, look for the option within GrapheneOS to install Google Play Services, Google Play Store, and Google Services Framework. Install all three. The exact location of this option may vary between GrapheneOS versions — check the official GrapheneOS usage guide if you need help finding it, or refer to our full course video walkthroughs.

We strongly recommend installing these in a **secondary user profile** rather than your main profile. This keeps Google services completely contained and separated from your primary data. You get app compatibility where you need it, without sacrificing privacy where it matters most.

Once installed, you can open the Google Play Store, optionally sign in with a Google account, and download apps normally. The critical difference is that Google's access to your personal information is dramatically limited compared to any stock phone.

CHAPTER 9

App Stores – Getting the Apps You Need

One of the most common questions from new GrapheneOS users is: "How do I get my apps?" The good news is you have multiple excellent options — more options, in fact, than you had on your old phone. Each option comes with different tradeoffs between convenience, compatibility, and privacy. Let's walk through some of them.

Note: GrapheneOS administers its own option, simply called App Store, which ships with the OS. This has only a few basics and is mainly used to update system apps, or install the sandboxed Play store, or Accrescent app store.

Option 1: Sandboxed Google Play Store

As described in the previous chapter, you can install the Google Play Store in a sandboxed environment and download apps exactly the way you always have. This is the easiest option and gives you the widest app compatibility. It's also the most secure way to get apps from the Play Store catalog, because the apps come directly from Google's infrastructure with their original developer signatures intact. For most people, this is where you'll get the majority of your apps.

Option 2: Accrescent

Accrescent is a newer app store designed from the ground up with security as its top priority. It distributes apps with their original developer signatures (meaning the developer signs the app, not the store), which eliminates an entire category of supply-chain risk. Accrescent's security model aligns closely with GrapheneOS's own philosophy, and it's worth checking whether the apps you need are available there. The catalog is still growing, but it's an excellent choice for security-conscious users. Download it from the official GrapheneOS App Store or the Accrescent website (https://accrescent.app).

Option 3: F-Droid

F-Droid is a well-established alternative app store that exclusively hosts **free and open-source software (FOSS).** Every app available on F-Droid has its complete source code publicly available for anyone to inspect. F-Droid doesn't require any account to browse or download apps, and apps are

flagged with clear warnings if they contain any "anti-features" such as ads, tracking, or dependencies on non-free software.

A note on F-Droid's security model: In the interest of giving you the full picture, you should know that F-Droid builds apps from source code on its own servers and signs them with F-Droid's own keys, rather than distributing the developer's original signed build. This means you're placing trust in F-Droid's infrastructure in addition to the app developer. F-Droid has also historically been slower than other stores to push security updates for apps. For most users, F-Droid is still a valuable resource, and they have a proven track record — but if maximum security is your priority, prefer Accrescent or Sandboxed Google Play when the same app is available on multiple stores.

Popular F-Droid apps include: NewPipe, a YouTube client that lets you watch videos without ads, tracking, or a Google account. Organic Maps, a full-featured offline maps and navigation app. Aegis Authenticator, an excellent two-factor authentication app. KeePassDX, a local password manager. DAVx^5 for syncing calendars and contacts with privacy-respecting servers. HeliBoard, a privacy-respecting keyboard. And many more.

To install F-Droid, open the Vanadium browser on your GrapheneOS phone, navigate to the official F-Droid website (https://f-droid.org), and download the F-Droid APK. When you open the downloaded file, your phone will ask you to allow installation from this source — grant it, and F-Droid will install.

Option 4: Aurora Store

Aurora Store is an alternative front-end to the Google Play Store catalog. It lets you browse and download the same apps available on the Play Store — but **without needing a Google account**. Aurora Store works by using shared anonymous session tokens, so you can download apps without signing in with personal credentials. It also shows you detailed information about

what trackers are embedded in each app before you install it, which is a useful transparency feature.

A note on Aurora Store's security model: Because Aurora Store acts as a middleman to the Play Store, you're adding an additional layer of trust to the app delivery process. Aurora store can also have their accounts restricted by Google at times, making it less reliable. For the highest security assurance, getting apps directly through Sandboxed Google Play is preferable when possible. Aurora Store is best used when you specifically want to avoid having any Google account, even in a sandbox.

You can install Aurora Store from F-Droid, or download the APK directly from the official Aurora Store website (https://auroraoss.com).

Option 5: Direct APK Downloads

Some app developers offer direct downloads from their own websites. This can be an excellent option since you're downloading directly from the source. For example, Signal is available from signal.org, Brave Browser from brave.com, and Mullvad VPN from mullvad.net.

When downloading APKs directly, **always download from the official developer website** — never from third-party APK mirror sites, which may distribute modified or malicious versions of apps. Keep in mind that this is a manual option, meaning updates may or may not be automatic. Only do this if you want some extra control.

Our Recommended Privacy App Stack

- For **web browsing**, use Brave or the built-in Vanadium browser.
- For **email**, ProtonMail.
- For **private messaging**, Signal is the gold standard.

- For **maps** and navigation, use Organic Maps. It works offline and it doesn't collect any data.
- For **VPN**, Mullvad or ProtonVPN are both excellent, privacy-respecting choices.
- For **password management** Bitwarden (cloud-synced) is a strong option.
- For **two-factor authentication** (2FA), Ente Authenticator is outstanding.
- For your **keyboard**, use the included Graphene option or replace the default with HeliBoard or OpenBoard from F-Droid — these are open-source keyboards that never transmit your keystrokes.
- For **notes**, you can choose Standard Notes or Joplin provide encrypted, private note-taking.
- And for a **camera** app, the built-in GrapheneOS camera app works well for everyday photography. If you want the full suite of Google's computational photography features, you can install Google Camera through Sandboxed Google Play in a secondary profile.

CHAPTER 10

Living With Graphene OS – Tips for Daily Use

Your First Week

Days 1 through 2: Focus on installing your essential apps. Get your messaging, email, browser, and daily-use apps set up. Take your time configuring permissions as each app requests them — think about whether each app truly needs the access it's asking for.

Days 3 through 5: Explore the settings more deeply. Set up user profiles if you plan to use Sandboxed Google Play. Familiarize yourself with network permission controls. Experiment with toggling off internet access for apps that don't need it.

Days 6 through 7: Refine your setup. Remove any apps you installed but don't actually need. Tighten permissions further. Set up encrypted backups — GrapheneOS includes a built-in backup solution that encrypts your data so only you can restore it. Check the current GrapheneOS documentation for the latest recommended backup approach.

Battery Life

GrapheneOS generally provides **noticeably better battery life** than stock Android. Without Google services constantly running in the background, pinging servers, collecting data, and processing analytics, your phone has significantly less work to do. Users commonly report 15 to 30 percent better battery life compared to the same phone running stock Android. Fewer background processes results in longer battery for you.

Camera Quality

The Pixel is famous for its camera, and that capability is fully available on GrapheneOS. The included GrapheneOS camera app is clean, fast, and functional for everyday photography. If you want the full suite of Google's computational photography features — Night Sight, Portrait Mode, and other advanced processing — you can install the Google Camera app through Sandboxed Google Play in a secondary profile. Most users find the stock GrapheneOS camera more than adequate for daily use.

Banking and Payment Apps

This is one of the most common concerns people have before switching. The good news: many banking apps work well on GrapheneOS, especially with Sandboxed Google Play installed. GrapheneOS is designed to pass the Play Integrity checks that banking apps use to verify they're running on a legitimate device.

That said, Google periodically tightens **Play Integrity** requirements, and individual banking apps vary in how strictly they enforce these checks. If a specific banking app doesn't work for you, check the GrapheneOS community forums and discussion channels — chances are very high that someone has already encountered and solved the exact same issue. Some users also report success with contactless payments, though your mileage may vary as this is an area that can change with updates from both Google and your bank.

Staying Updated

GrapheneOS receives **frequent over-the-air updates**, often more frequently than stock Android. Security patches are typically integrated and pushed out within days of Google releasing them. Updates download and install automatically in the background — you'll simply see a notification to reboot when an update is ready. Always reboot promptly. These updates include critical security fixes and you want them applied as quickly as possible.

VPN — Use One Always

We strongly recommend running a trustworthy VPN at all times on your GrapheneOS phone. This encrypts your internet traffic and prevents your

internet service provider, Wi-Fi network operators, and other intermediaries from monitoring your online activity.

GrapheneOS supports the Android "Always-On VPN" feature, which ensures that every single network connection from your phone goes through the VPN — no leaks, no exceptions. To enable it, go to **Settings → Network & Internet → VPN**, select your VPN app, and toggle on both **"Always-on VPN"** and **"Block connections without VPN."** The second toggle is critically important — it acts as a kill switch, preventing any data from leaking if the VPN connection momentarily drops.

Encrypted DNS

By default, your DNS queries — the requests your phone makes to translate website names into IP addresses — are visible to your internet provider, telling them every website you visit. GrapheneOS supports **Private DNS** (DNS over TLS), which encrypts these queries so your provider can't see them.

Go to **Settings → Network & Internet → Private DNS** and enter a trusted provider. This is a quick, simple change that meaningfully improves your privacy. Verify that your chosen DNS provider is still actively operating and recommended by the privacy community at the time you set this up.

CHAPTER 11

Your Next Steps With Privacy Academy

Congratulations. By reading this guidebook and following through on what it teaches, you've taken a monumental step toward reclaiming your digital privacy. You now have — or will soon have — a phone that actually works for you. A phone that doesn't spy on you, doesn't report your location to corporate servers, and doesn't sell your personal life to advertisers.

But this guidebook is just the beginning.

The Full GrapheneOS Course

This eBook is your companion to the **Privacy Academy GrapheneOS Course,** which goes significantly deeper into every topic covered here. The course includes detailed video walkthroughs of every installation and configuration step so you can follow along in real time. It covers advanced setup strategies including detailed profile management, app hardening techniques, and network security configuration that go well beyond what a guidebook can cover. It includes troubleshooting guidance for common issues and edge cases. And it's continuously updated as GrapheneOS evolves and new features are released, so your knowledge stays current.

Live Training Classes — This Is Where It All Comes Together

Reading a guidebook is valuable. Watching course videos is even better. But nothing compares to **live, interactive training** where you can get real-time help from expert instructors.

Privacy Academy offers **live training classes** where you can set up your phone with an instructor guiding you step by step. You can ask questions and get answers tailored to your specific situation, your specific device, and your specific needs. You'll learn advanced techniques that go beyond what any written material can fully convey. You'll stay current with the latest privacy threats and how to defend against them. And you'll connect with a community of privacy-conscious people who are on the same journey you are — people who understand why this matters and who can share their own experiences and solutions.

Live training classes are available exclusively to monthly members of Privacy Academy*. If you haven't already joined, we strongly encourage you to sign up. Having access to live expert guidance makes the difference between a good privacy setup and a truly bulletproof one. When you're configuring something unfamiliar and you hit a wall, there's nothing more valuable than being able to ask an expert and get an immediate, personalized answer.

**Note: A purchase of any stand-alone course may also include a free 60-day trial of the membership that gives you access to live classes during the trial.*

The Bigger Privacy Journey

Switching to GrapheneOS is one of the single most impactful actions you can take for your personal privacy. But it's one piece of a larger picture. True, comprehensive digital privacy encompasses how you communicate — encrypted messaging, secure email. How you browse the internet — VPNs, Tor, browser hardening. How you handle your finances. How you manage your identity online through compartmentalization and careful information control. And how you think about data — understanding threat models, practicing data minimization, and building habits that protect you by default.

Privacy Academy covers all of this and much more. Your GrapheneOS phone is the foundation — the single most important piece. Now let's build on it together.

CHAPTER 12

Further Reading

If you want to verify the claims in this book or dive into the research behind our advice, the following topics and sources are worth exploring:

On Android data collection: Research by Professor Douglas Schmidt at Vanderbilt University examined Google's data collection practices on Android devices in detail. The Trinity College Dublin study by Professor Doug

Leith compared telemetry from iOS and Android devices and found significant data transmission from both platforms even when idle and when users had opted out.

Apple data collection: Tommy Mysk and Talal Haj Bakry documented iOS analytics transmission behavior even with disabled sharing settings.

App tracking: Exodus Privacy project maintains a database of trackers embedded in Android apps, which is a useful resource for evaluating apps before you install them.

GrapheneOS: The official GrapheneOS website contains comprehensive documentation on features, the security model, FAQ, and installation guides. This should be your primary reference for current information.

On privacy-focused tools: The Privacy Guides website provides regularly updated recommendations for privacy tools across categories including VPNs, email, browsers, and more.

We encourage you to verify, question, and research. An informed user is a safer user.

FINAL WORDS

Every time you use a stock phone, your data that is collected, analyzed, sold, and used to build a detailed profile of who you are, where you go, what you think, and what you do. That data is permanent. It doesn't expire. It doesn't get deleted. Once it's collected, you cannot take it back.

But starting today — right now — you can stop the bleeding.

Your GrapheneOS phone is more than a device. It's a declaration. It says: **my data is mine, my conversations are mine, my location is mine, and my life is mine.**

Welcome to the privacy revolution. We're glad you're here.

For the latest updates, live training schedules, and membership information, visit Privacy Academy. Sign up as a monthly member to get access to live training classes and ongoing expert support.

This eBook was prepared by the Privacy Academy Expert Team: GrapheneOS Specialist, Technical Writer, Marketing Editor, and Fact-Check Auditor. All technical instructions were verified against official GrapheneOS documentation and current research at time of publication (April 2026). Always refer to the official GrapheneOS website for the most current installation instructions and device compatibility information.

AFFILIATE DISCLOSURE: Privacy Academy has an affiliate relationship with Proton (proton.me). However, none of the links in this ebook are affiliate links, and we receive no commission from any action you take through this guide. We recommend Proton because we genuinely believe it is the best privacy-focused alternative to Google's services. We also recommend several products in this guide (Brave, FreeTubeApp.io, Magic Earth) with which we have no financial relationship.

PRIVACY IS FREEDOM.

Protect Your Assets & Stop Surveillance

Join the only community designed to help overwhelmed, non-techy people learn how to get private and secure online.

Get Private Today.

GET LIVE TRAINING WEEKLY AND ACCESS TO OUR LARGE LIBRARY OF PAST WEEKLY TRAINING RECORDINGS.

👉 **Join Privacy Academy Today.** https://privacyacademy.com/

Join over 75,000 people who are taking control of their digital lives. Whether you're 18 or 87, tech-savvy or a complete beginner, Privacy Academy will meet you where you are and walk you to where you need to be.

Your privacy is your freedom. Protect it.