Option 1: GrapheneOS Device

My clients each receive a new telephone with new anonymous activated service. Unless my clients absolutely insist on an iPhone, I issue new devices containing custom Android builds by default. This is going to get very technical, but the final product we create will possess more privacy, security, and anonymity than anything you can buy off a shelf. If you are not ready for this level of privacy, upcoming sections tackle other ways to possess an anonymous iPhone or Android device.

I believe **GrapheneOS** (grapheneos.org) is the optimal operating system for a mobile device. It eliminates all data collection by Google, and introduces "full verified boot" within a minimalistic custom operating system. Typically, uploading a custom ROM to an Android device requires you to unlock the bootloader. After the operating system is installed, the bootloader must remain unlocked in order to use this unofficial build. The unlocked bootloader could present a vulnerability. If I physically took your device; uploaded my own malicious version of your operating system to it; and then put the phone back, you may not be able to tell. Your data and apps would all look the same, but I could monitor your usage if I modified the OS to do so.

This is where GrapheneOS has an advantage. It detects modifications to any of the operating system partitions and prevents reading of any changed or corrupted data. If changes are detected, such as a malicious physical attempt to compromise the device, error correction is used to obtain the original data. This protects the device from many attacks. The authenticity and integrity of the operating system is verified upon each boot. Because of this, a Google Pixel device is required to install GrapheneOS.

Some may be surprised at that sentence. Yes, I recommend a Google Pixel device. This is because we will completely remove all software included with the device and replace it with better versions. Pixel devices offer superior hardware security capabilities than most Android devices. I purchased a Google Pixel 4a for $349, paid in cash at a local BestBuy store. Used devices can be found for under $300 on Swappa, but PayPal is required for payment. Fortunately, these devices are plentiful at many local retail establishments, and it is always best to pay cash for any mobile device. If you want to ensure longer support, you might consider purchasing a Pixel 5a. The instructions presented here are identical for the 4a, 4a (5G), 5, 5a, and 6, with the exception of the specific version of GrapheneOS required for each model. This should also work for Pixels released after publication. Always purchase the latest model supported. If I were starting over today, I would seek a Pixel 5a.

There are two options for installation of GrapheneOS onto your Pixel device. The web installer is the easiest for non tech-savvy users, while the Linux method is most stable. I will explain both. If you have a Linux computer as explained previously, I recommend using it for this purpose. If you do not have a Linux machine, the web installer should work fine for your needs.

Regardless of the installation path you choose, you must first prepare the phone itself. Turn on the Pixel device and dismiss any attempts to enter a Google account. Swipe the menu up to launch "Settings", and conduct the following.

- Tap "About phone".
- Tap "Build number" at the bottom several times until "Developer mode" is enabled.
- Tap the back arrow.
- Tap "System".
- Tap "Advanced".
- Tap "Developer Options".
- Enable "OEM Unlocking" and "USB debugging".

Your device may require internet access via Wi-Fi or cellular data to complete this process. We can now install GrapheneOS. I will begin with the easiest option.

GrapheneOS Installation Via Web Installer

From your Windows or Mac computer, navigate to https://grapheneos.org/install/web and read through the entire page. Once you understand the overall installation process, run through the steps, which are outlined here.

- Turn the device off.
- Hold the power and volume down buttons simultaneously.
- When you see the "Bootloader" menu, connect the device to computer via USB cable.
- Click the "Unlock Bootloader" button.
- Select your device from the popup menu.
- Click "Connect".
- Press the volume down button on the device to select "Unlock Bootloader".
- Press the power button to confirm the choice.
- Click the "Download Release" button on the GrapheneOS page.
- Allow the appropriate version of GrapheneOS to completely download.
- Click the "Flash Release" button.
- Allow the process to complete.
- Click "Lock Bootloader" on the GrapheneOS page.
- Press the volume button on the device to select "Lock Bootloader".
- Press the power button to confirm the choice.
- Make sure "Start" appears next to the power button and press it.
- Allow the phone to boot.

This sounds simple, but a lot can go wrong. In my experience, only Google Chrome and Microsoft Edge browsers will complete the process. Attempts with Safari and Firefox failed for me. A poor quality USB cable can ruin the entire process, so use the cable included with the device when possible. Some Windows machines may not have the appropriate drivers for your device. If the phone is not recognized, plug it in and attempt a software update at "Windows Update" > "Check for updates" > "View Optional Updates". You should now have GrapheneOS installed. Skip past the next section about installation through Linux to continue.

GrapheneOS Installation Via Linux

The following steps were slightly modified from the GrapheneOS website at grapheneos.org/install. Always check that site before proceeding as things may have changed since this writing. I have included each step on my site at **inteltechniques.com/EP** for easy copy and paste. The following tutorial requires an Ubuntu Linux computer, and I used a laptop with Ubuntu 22.04 as the host. This is the cleanest and easiest option. While you can install from a Windows or Mac host, software requirements can vary and driver issues can be complicated. The Linux steps are more universal. Never use a virtual machine for this installation due to detection issues.

We must now configure software within our Linux computer. As stated previously, this can be completed within your new Linux machine or a live boot environment with a USB boot device. Full details can be found at https://ubuntu.com/tutorials/create-a-usb-stick-on-ubuntu. I will assume you already have a Linux laptop built from the previous chapter, but Windows and Mac options are explained at grapheneos.org/install. Conduct the following within an Ubuntu Terminal session. Note that the exact version presented here may have been updated. The tutorial steps offered at **inteltechniques.com/EP** will be updated as needed. Always rely on that version over any printed text here. **These steps also install ADB, which is required within other tutorials.**

- sudo apt install libarchive-tools
- curl -O https://dl.google.com/android/repository/platform-tools_r32.0.0-linux.zip
- bsdtar xvf platform-tools_r32.0.0-linux.zip
- export PATH="$PWD/platform-tools:$PATH"

- sudo apt install android-sdk-platform-tools-common
- sudo apt install signify-openbsd
- fastboot --version

The final command verifies that Fastboot is installed which should display the version number. We now need to boot our device into the bootloader interface. To do this, hold the power and volume down buttons simultaneously while the device is off. This should present a "Fastboot mode" menu. Connect the device to your Ubuntu computer via USB cable. Execute the following command within Terminal and verify it displays "OKAY".

- fastboot flashing unlock

Press the volume down button on the mobile device until "Unlock the bootloader" is displayed, then press the power button. We are now ready to download the new operating system files. First, you must navigate to grapheneos.org/releases and select your device within the "Stable Channels" section. Note that the 4a is code-named "sunfish", while other models are code-named "bramble" (4a 5G), "redfin" (5), and "barbet" (5a). **It is vital to choose the correct version for your device**. Next, identify the latest version number, such as "2021081411". You will need to replace each version within the following examples (2021081411) with the latest version displayed on the website during your installation. Execute the following within Terminal ONLY for the Pixel 4a.

- curl -O https://releases.grapheneos.org/factory.pub
- curl -O https://releases.grapheneos.org/sunfish-factory-2022030219.zip
- curl -O https://releases.grapheneos.org/sunfish-factory-2022030219.zip.sig
- signify-openbsd -Cqp factory.pub -x sunfish-factory-2022030219.zip.sig && echo verified

The last command should display a confirmation that the software is correct. This confirms that we have downloaded a secure file which has not been intercepted or maliciously replaced. The following Terminal steps extract the download and install it to the device.

- bsdtar xvf sunfish-factory-2022030219.zip
- cd sunfish-factory-2022030219
- ./flash-all.sh
- fastboot flashing lock

You should now see the option "Do not lock the bootloader" on the device. Press the volume down button until "Lock the bootloader" is displayed and press the power button. You can now reboot the device by pressing the power button labeled "Start" or holding down the power button to turn off, and then turning on as normal. You may see an error about booting into a different operating system, but this is normal. Allow the phone to boot without making any selection.

Upon first boot of GrapheneOS, press "Next" until the Wi-Fi connection screen is present. Connect to Wi-Fi and complete the following tasks, with considerations for each.

- Disable location services for now, this can be set up later if needed.
- Assign a secure PIN for the screen lock.
- If desired, add your fingerprint to the screen lock function.
- Skip any restore options.

Your installation is now complete. The device itself is completely encrypted and sends no data to Google. Next, let's harden a few settings.

GrapheneOS Configuration

Once you are within the new operating system, confirm that OEM unlocking and developer options are disabled with the following steps. This may be redundant, but we want to make sure we are protected.

- Swipe the menu up to launch "Settings" and click "About phone".
- Tap "Build number" at the bottom several times until "Developer mode" is enabled.
- Click the "Back" arrow and click "System", "Advanced", then "Developer options".
- Disable "OEM Unlocking" and confirm the choice.
- Disable "Developer options" and reboot the device.

Your new GrapheneOS device is very private and secure, but there is always room for improvement. There are no Google services, and Google is not receiving any data about your usage. This presents a new problem. Without Google services, there is no Google Play store which is used to obtain apps. Since we will not compromise our integrity by adding the required Google software to activate the store, we will use better options instead.

- Launch the Vanadium browser within the apps menu and navigate to f-droid.org.
- Click the "Download F-Droid" button.
- Confirm the download and click "Open" at the bottom of the screen.
- If prompted, click "Settings" and enable "Allow from source".
- Click the back button and confirm the installation of F-Droid.
- Open the F-Droid application.
- Swipe down from the top and install any F-Droid updates available.
- If prompted, repeat enabling of "Allow from source" settings.
- Reopen the F-Droid application.

You now have a substitute app store which is not powered by Google. Many of the open-source applications we will use will come from this repository. This device is more private and secure than any stock unit which could be purchased from a retailer. Unlike a traditional iOS or Android phone, a user account is not required in order to use the device. If ever prompted to add a Google account, avoid or "skip" the option. This way, there is no single Google or Apple account which can be tracked, archived, and abused. Again, by default, GrapheneOS transmits no data to Google. Eliminating these privacy threats provides great benefits.

The installation effort can seem overwhelming, but is usually only a one-time event. Fortunately, updates are automatic by default and pushed to your device often. You will notice them within the notification menu, and you may be prompted to reboot to finish installation. Along with F-Droid, I recommend the application Aurora Store. Aurora Store is an unofficial client to Google's Play Store. You can search, download, and update apps. You can also spoof your device information, language, and region to gain access to the apps which are restricted in your country. Aurora Store does not require Google's proprietary framework. With Aurora Store, you can install all of the mobile apps mentioned throughout this book. Aurora Store can be installed through F-Droid. During installation, be sure to choose "Anonymous" mode, which prevents Google account requirements, and accept all other default options.

Always attempt any app installations through F-Droid before Aurora. If an app is missing from F-Droid, rely on Aurora Store. You can use the "Updates" menu of each app to make sure all of your installed applications stay updated. Make sure to keep Aurora updated through F-Droid in order to maintain functionality. I launch both F-Droid and Aurora weekly to fetch any pending application updates.

Let's pause and digest what we have accomplished. Our phone possesses the basic communications technology we need for daily use. It does not share any data to Google or Apple. An account is not required to download applications; therefore, an account does not exist to collect and analyze data about our usage. There are no

embedded cloud storage options which can accidentally be enabled. This is a huge feature for most clients. This minimal device encourages us to return to the original intention of a mobile phone: communications. In a moment, we will customize our device with communications options.

While your desired apps should install without issues, everyday function may be a problem. Since GrapheneOS does not contain any Google apps, you are likely missing some core Google software which provides services such as push notifications, location tracking, and mapping. This may sound like a huge benefit, but it also presents some limitations. You can typically still open apps and "fetch" data such as pending email or text messages at any time, but you might be missing instant notifications. With some apps, synching of content might simply be delayed. Some secure messaging apps, such as Signal, can deliver messages instantly through their own platform without the need for Google's push service. Traditional email applications, such as ProtonMail, may only fetch the data when the app is opened. This may be a desired feature to some. A true Google-free experience without constant incoming notifications is a nice change.

Personally, I prefer to intentionally fetch desired content when needed in order to keep Google or Apple out of my business. My phone never lights up during meetings and never dings audible tones throughout the day. There is never a looming notification reminding me that my inbox is growing with unread messages. I check for any communications on my own time. I am never tempted while driving to check the latest email which just arrived. When appropriate throughout my daily schedule, I check my email and other communications apps by opening each. The content is fetched from the various servers and I can tackle anything which needs a response. Emergencies through Signal messages and calls continue to present a notification as designed. It took a while to lose the anxiety of potential missed messages. Today, it reminds me of the way email was checked when I first started using it. Back then, you logged into your computer; opened your email client; fetched any incoming messages; responded to those desired; and closed the software after the messages had been sent. You then might even turn off the computer and go about the rest of your day. Today, I check my phone often for email and other communications, but it no longer controls my life.

Many readers may think this is an unattainable luxury. I respect that you may have children in school which need to get in touch with you at all times; an employer who insists you respond to anything within minutes; or a sick family member which needs direct access to you. If you need immediate notification of incoming email and SMS text messages without launching applications, then GrapheneOS may not be for you. Many people discuss installing an open-source version of Google's Push services through software called microG, but that will not work with GrapheneOS. This operating system is hardened very well, and does not allow weakened security through the use of these privacy-leaking options.

Before I scare you away from GrapheneOS, let's discuss some actual experiences. If you use ProtonMail as your secure email provider, as recommended in the next chapter, you will not receive any notifications of incoming messages. You will need to open the app occasionally and check your email. If you use Signal as your secure messenger service, as recommended in the next chapter, you can receive immediate notifications of incoming text messages without the need to open the app. If you use Linphone for telephone calls, as explained later in this chapter, you will receive notifications of incoming calls. Your device will ring as normal. Most other communication applications will not send notifications, and you will need to open those apps in order to see any pending messages. For most people, I believe the ability to receive incoming calls and secure message notifications through Signal is sufficient for daily use without the need for any Google services.

Remember that mobile device privacy is a series of decisions which produce an environment most appropriate for you, and will be unique for everyone. I have a few clients who use GrapheneOS every day and love it. I have others who hated it. It really depends on your personality and need to be notified of everything at all times. For me, switching was therapeutic. It reminded me that I do not need to see everything in real time, and there was life outside of my various networks. I believe GrapheneOS is not only the most private and secure mobile device option we have, but it is the most elegant and minimalistic. It has no bloatware or undesired apps. I must admit that most of my clients do not use GrapheneOS. Only those with extreme situations have successfully made the

switch. Today, the majority of my clients insist on iPhones. Therefore, I make them as private and secure as possible, as explained in a moment. First, we should discuss some GrapheneOS limitations.

I am thrilled with using GrapheneOS as my daily mobile device. However, it is not perfect. Since we have eliminated Google and Apple from collecting our data, we have also removed their helpful features. By default, the settings within GrapheneOS are hardened with privacy and security in mind. However, there are several modifications I make for myself and clients. The following outlines multiple considerations for your own GrapheneOS installation.

Missing Applications within Aurora: You may search for an app within Aurora and be unable to find it. At the time of this writing, both MySudo and Privacy.com are not indexed within the native search feature. However, that does not mean we cannot install these applications from Aurora. They are actually present if we know the exact URL, but that is unlikely. There are two options for installing applications which are missing form Aurora's search. The first is to visit the company's website, such as Privacy.com, from the mobile device and long-press the button to install the app via Google Play. Select "Open link in external app" from the popup menu. This should navigate you to the installation option for this app within Aurora. If that does not work, you may be missing an important setting.

- Open "Settings" and select "Apps" > "Default apps" > "Opening links".
- Enable "Instant apps" and tap "Aurora Store".
- Enable "Open supported links" and click "Add links".
- Enable all options and repeat the previous link opening process.

If you encounter a desired application which does not possess a link on their home page, search through the Google Play website. When you find the desired link, long-press and open through Aurora. If this all fails, go to "Settings" > "Networking" within Aurora and enable "Insecure Anonymous Session". Log out of Aurora, close the app, open it, and log back in. If desperate, download the desired application's APK file from apkmirror.com or apkpure.com and install it manually. This should populate the app within Aurora for all future updates.

Battery Drain: If you install GrapheneOS, and a suite of communication applications such as Signal, Wire, and others, expect fast battery drain. Since the device does not possess Google's push services, some apps will try to constantly listen for new incoming communications. This forces those apps to be ready at all times and prevents them from becoming dormant within the background. In my experience, this can change battery length with normal usage from two days to nine hours. Fortunately, there is a fix. Since we do not receive notifications on the device through push services, there is no reason to ask apps to listen for new communications. The following is my process to regain proper battery life.

- Open each third-party app, such as messaging, email, and web browsers, and then close them.
- Navigate to "Settings" > "Apps".
- Open each of these apps under the recent screen; select "Notifications"; and disable all options.
- Navigate back one screen; Select "Battery"; and change to "Restricted".
- Repeat for all desired apps.
- Check these settings on occasion until you have modified each app as desired.

This instructs the operating system to prevent applications from constantly accessing the network when minimized or closed. It prevents apps such as Signal from maintaining a constant connection to various servers. It prevents your email from fetching new messages when you are not using the app. It also prevents unnecessary attempts for notifications on your screen. This all saves precious battery life but also adds privacy. These applications are not constantly connecting to servers and sending your IP address until you take intentional action to check your messages. Manually launching each app synchronizes the account and your messages are populated in the screen.

If you rely heavily on Linphone for voice calls or Signal for secure communications, and you want to be notified of incoming communications, you should leave the default notification and battery settings enabled for those apps. If you child messages or calls you through Signal, you might want to always be notified when a communication arrives. This may impact your battery life, but it may be a priority feature for you in order to stay in immediate contact with others. I explain more about these services later. I have every third-party application on my device in restricted mode without notifications. My phone never prompts me to answer a call or check a message, but I check for messages often. With this minimal usage, my device only needs charged every other day.

Permissions: Navigate to "Settings" > "Privacy" > "Permission Manager" and consider these options. By default, some apps may already have permission to access your camera, microphone, or other hardware features. Communication apps obviously need access to your microphone, but a calendar does not. Consider modifying everything in this menu to your specifications. As an example, I disabled all "Body Sensors" access and severely limited my location, microphone, and camera access. I also disabled all "Nearby Devices" associations, which allows the use of wearable devices, such as a smart watch.

DNS: GrapheneOS does support firewall applications, but they cannot run along with VPNs in the way iOS can. The most appropriate option for most users who want to restrict ads and trackers within applications and browsers is to enable a private DNS option. You can do this by opening "Settings" > "Network & Internet" > "Advanced" > "Private DNS", selecting "Private DNS provider hostname", and entering "dns.adguard.com". This will route all of your internet traffic through AdGuard, and AdGuard will block many trackers, ads, and other unwanted connections. This is not perfect, but it is helpful. It is also applied at the operating system level which should globally block much unwanted data. Later, I present much more details about DNS options.

Update Modifications: On multiple occasions, I have updated the GrapheneOS operating system and reboot to find modifications to my settings. I have witnessed my mobile data connection become disabled, resulting in no internet access. If this happens, open "Settings" > "Network & Internet" > "Mobile Network", and enable "Mobile Data".

Home Menu Shortcuts: The labels for applications within your home menu and the applications menu are often truncated. Instead of displaying "Standard Notes" below the app icon, it may appear as "Standa...". This drives me crazy. I use a program called "Shortcut Creator" to generate custom icons and labels on my home screen. I only recommend this if you are bothered by the truncated names.

Display: I mentioned on my podcast that I restrict my screen to monochrome colors. This helps me focus. I no longer want to use my device to stream video or browse websites. The monochrome display forces me to use the device for communications as it was intended. If you want to test this for your own use, navigate to "Settings" > "Accessibility" > "Text and display" > "Color correction". Enable "Use color correction" and select "Grayscale". I believe this makes my text communication crisper and discourages "playing" on the phone.

Mapping Applications: There are no map applications included with GrapheneOS. You could install Google Maps from Aurora and possess the standard functions. However, you are now sharing data with Google again. I recommend a combination of Magic Earth (Aurora) and OSMAND+ (F-Droid). Magic Earth is better with navigation and identification of businesses, but it does collect some telemetry which may be outside of your comfort zone. OSMAND+ is completely open-source and relies on the OpenStreetMap project. Neither are great with navigation or display traffic congestion from Apple or Google. That is the biggest weakness for most users. However, we can download full maps for offline usage. While both applications allow download of offline maps, I prefer OSMAND+ due to their privacy policy. The F-Droid version allows unlimited download and update of maps of the entire world. These can then be used offline without any cellular or Wi-Fi connection. I download all street maps of the United States to my device (>16GB). When I need to find a location or navigate to a specific address, I do so within OSMAND+. No data is shared about my trip, and I can disable connectivity if the route is extremely sensitive. The application and maps have helped me tremendously when cellular service was unavailable in remote areas.

Individual Profiles: GrapheneOS supports multiple profiles within a single device. This allows you to create unique configurations for multiple users, or your own alias profiles. I played with this for a few weeks, and found it very intriguing, but ultimately decided not to use this feature as part of my communications strategy. Since GrapheneOS is not "calling home" and sending our data out to Google or Apple, I found little reason to isolate my app usage. The one benefit I enjoyed was the ability to possess multiple instances of Signal within a single device, but switching profiles to take advantage of this became tiresome. If you believe you could benefit from isolated instances, please research this option within the GrapheneOS website. It could be quite valuable for segmenting business, alias, and covert usage. In a moment, I explain usage of secondary profiles after sanitizing a stock Android environment.

Sandboxed Google Play Services: GrapheneOS now supports installation of core Google services, which are "sandboxed" and available only on an application level. This additional Google software does not have full access to your operating system as it would with stock Android. Many GrapheneOS enthusiasts believe the installation and execution of this software is acceptable. I do not. While Google will not receive a unique hardware identifier, such as a serial number, it will receive your make, model, and IP address constantly. We simply never know what other tracking metrics are embedded, or will be embedded, into the software. The purpose of an un-Googled device is just that. I do not want Google receiving any data about my usage whatsoever. If you need Google services installed in order to receive push notifications and use Google applications, then I believe GrapheneOS is not appropriate for you. Consider one of the next options. Many will disagree with my harsh resistance to adding Google frameworks into my devices, but I strive for extreme privacy. That means no Google. Period.

Wi-Fi Disabling: GrapheneOS, and other custom ROMS, have the ability to disable Wi-Fi after it has been disconnected from a network. I like this feature. If you leave your home while Wi-Fi is enabled, it will shut itself off to prevent accidental connection to public networks or public beacons from tracking you via Wi-Fi. Navigate to "Settings" > "Network & internet" > "Internet" > "Network preferences" > "Turn off Wi-Fi automatically". I set mine to "1 minute".

Backup: Once you have your GrapheneOS device configured, I encourage you to create a backup. This will preserve all of your settings and customizations. Open "Settings" > "System" > "Backup". Allow the backup to save to the internal location and tap "Recovery code". Document the words presented to you, as these will be required if you want to restore to this version. I recommend that you enable all backup options. However, I tapped "Backup status"; the three dots in the upper right; enabled "Exclude apps"; and de-selected the offline maps. I did not want to take the chance of wasted storage on gigabytes of maps which could be re-downloaded later. On the main "Backup" screen, select the three dots and choose "Backup now". This will create a new folder titled ".SeedVaultAndroidBackup" at the root of your device's storage.

Once complete, I connect my device via USB to my computer; select the option to transfer data within the device's drop-down menu; and copy this new folder onto the computer. I then delete the backup from the device. This allows me to restore a backup to a new device if required. You will likely never need this backup, but it might save you hours of work if you lose your device. If you have the VOIP options presented in a moment configured, this backup may become even more vital. I create a new backup after configuration of everything mentioned in this chapter.

My GrapheneOS experience has been wonderful. I no longer check my phone every minute to respond to incoming messages. I check them on my time. I no longer worry about the data collection about my usage. I do not feel the constant need to request and scrutinize my data from Apple. I am never prompted to enter my long password in order to download a free application. I never need to confirm a code via text or email in order to complete an update or make a change within my settings. I am never forced to log in to an account to verify that I am the proper user of the device. My phone no longer feels "dirty" a few weeks after using it. There is a great sense of freedom when you leave that world behind.