Secondary Device Configuration

Your new private Android or iPhone may be all you need in regard to a mobile device. Most people carry it with them everywhere they go and leave it connected to the mobile network at all times. I believe this is risky behavior and a desire for extreme privacy will require you to take more extreme action. Many of my clients' primary mobile devices have never entered their homes and have never connected to a cellular tower within five miles of their houses. This prevents their phones from announcing their home locations. If someone did figure out a mobile number, and paid a bounty hunter or private investigator to locate a device, it would not lead anyone back to a home. The last known location should be a busy intersection with no connection to anyone. You can accomplish this and still possess a mobile device in your home with all of the communication apps you need with the following instructions. First, we should discuss whether you need a secondary home device.

I began presenting a secondary device option when I was still recommending Apple iOS devices. This was before GrapheneOS was available and I believed that Apple was our best option for privacy and security. This has changed. Apple is now collecting more information than ever before and continuously introducing new "features" which give us no control over their functionality. This presents a new dilemma for me. I had previously recommended Apple iPod Touch devices for use in the home while an iPhone could be used outside the home. While the Touch devices possess no cellular connectivity, they still collect and send data about you back to Apple every minute. Therefore, I am drastically changing my advice for secondary device usage. My current recommendation is as follows, in order of most private to least.

- Primary GrapheneOS device for use while traveling and a laptop within the home
- Primary GrapheneOS device outside the home and secondary GrapheneOS device within the home
- Single GrapheneOS device for use within the home and while traveling
- Primary GrapheneOS device outside the home and secondary iPod Touch device within the home

I will discuss all options, but we should first understand the reasons why any of this might matter to you. When you travel, your phone is always by your side and is your primary means of secure communications. When you return home, things might change. When you are about five miles away from home, at a very specific location, you might drop your device into a Faraday bag. This shielded pouch (amzn.to/3gmNJnZ) prevents any signals from reaching or leaving the phone. It stops all communications with cellular towers. The device might stay in this bag until you are at least five miles from home heading out on another trip. Since the phone is never connected to any network while near your home, it cannot reveal the overnight location of the device (or your home address). You might be surprised at the number of private and government organizations which have unlimited access to device location data.

While at home, you can still possess a secondary mobile device for secure communications. Many use an iPod Touch for this. The iPod Touch possesses the same iOS operating system as the iPhone. It connects to your wireless network in the home (behind a firewall with VPN as discussed later) and has internet access, but no cellular connectivity. It possesses a unique Apple ID never used on any other device. Most secure communication apps, such as Wire, work the same as on your primary phone and can share accounts. Neither Apple or Google will know this association. Many use this strategy in order to possess a small device within the home without the need to rely on a large laptop all day.

You can configure Linphone on your secondary device for all incoming and outgoing voice telephone calls using the same numbers as your travel device. This gives the best of both worlds while at home. Upon arriving home, connect the secondary device to your home Wi-Fi and it never leaves the house again. This secondary device replicates all communications options you may need. Aside from lack of a cellular-provided number and service, it appears identical to your "phone". MySudo can also possess the same telephone numbers for incoming and outgoing calls across all devices. In order to replicate an installation of MySudo, and share the same numbers across two mobile devices, both must be active at the same time during configuration. You must scan a barcode from the primary device within the secondary unit. Both devices need internet access during this process. Therefore, I set all of this up on public Wi-Fi behind a VPN before taking the secondary device to a client's

home. This is a one-time exception. First, I enable power on the secondary device at any library with free Wi-Fi and allow my cellular telephone to be connected to a cellular data connection. I configure everything on the secondary device as needed, which will require access to the primary device to allow these connections. I then "forget" the Wi-Fi network on the secondary device. An optional step here is to tell the device to forget all networks, if desired. I then turn it off completely.

An issue with this plan is the installation of Signal on the secondary device. Unlike username-based services such as Wire, Signal relies on a telephone number. Furthermore, it only allows usage on one mobile device at any given time. However, it provides a desktop application which can be used on multiple machines. Therefore, a secondary mobile device would not possess your primary Signal account, but your home laptop could. You can send and receive text, audio, and video over Signal while using a laptop.

I insist on preventing any devices from connecting to any cellular network while in my home. These connections can immediately identify someone's location. The iPod Touch has no cellular connectivity, but a secondary GrapheneOS device can also be fairly safe. Unlike Apple iPhones, GrapheneOS does not re-enable cellular and Bluetooth radios upon reboot after every software update. When you place the GrapheneOS device into airplane mode, the cellular connection sends absolutely no data to any cell towers. If your secondary GrapheneOS device does not possess a SIM card, this concern becomes even less.

The idea of a secondary device is that it never leaves the home and never connects to any other network. I think of it as a landline which only functions in the home. If you possess an anonymous telephone with prepaid service and an anonymous Wi-Fi only device, both of which have no connection to your identity or each other, you have an amazing layer of privacy protection. However, this could be overkill. Now that I have explained the reasons I have changed my view of the secondary device, let's revisit our options and expand on each. I begin with the most private and secure.

Primary GrapheneOS device for use while traveling and a laptop within the home: Your travel device possesses an anonymous prepaid account, but all cellular usage is logged forever. The location of this device can be tracked any time the cellular radio is enabled. Dropping it into a Faraday bag before going home truly protects you. While at home, you may only need a laptop computer for all communications. This option has become much more popular lately with clients. They realize that they can conduct almost all of their typical mobile device usage within a laptop. In some cases, the laptop is more stable than a mobile device. Email, Signal, Wire, Linphone, voice calls, and SMS texting can all be accomplished on a laptop without any mobile device requirement. There is no option for cellular connectivity. The only limitation is the absence of MySudo, but calls can be made through Linphone. Some clients say they appreciate the lack of "playing" on their mobile device all night, and simply check their laptop on occasion throughout the day. Traditional VOIP and secure Signal calls audibly ring on the device.

Primary GrapheneOS device outside the home and secondary GrapheneOS device within the home: Your primary travel device stays in a Faraday bag while near the home. Upon arrival at home, the secondary GrapheneOS is practically identical to the travel device. It is in airplane mode and only connects via Wi-Fi. All of your apps work the same way, with the Signal exception. If airplane mode is accidentally disabled, there is no SIM which would associate the device to a specific account. A connection to a cell tower would be made, but this would not expose any phone number or account.

Single GrapheneOS device for use within the home and while traveling: This option eliminates the secondary device completely, but would require some serious discipline. You could place the device into airplane mode while traveling and connect to Wi-Fi while at home. For extra credit (and comfort), you could remove the SIM before placing the device into airplane mode. Since there is no Google or Apple account associated with the device, there is no central repository collecting data about the device's location and usage. If you were to accidentally disable airplane mode, a connection would be made to a nearby cellular tower which could expose your location. However, who would know it is you? Your prepaid account is in an alias name and you never use that number for anything. The risk here is low, but there is still risk. I would never encourage a high-risk client

to use their primary device in the home, but the majority of GrapheneOS users might have no issue with this. The pressure would be on you to enter airplane mode any time you are near your home. Only you can decide if this is feasible.

Primary GrapheneOS device outside the home and secondary iPod Touch device within the home: Finally, you have the traditional option of a GrapheneOS device while you travel and a Wi-Fi-only iPod Touch for the home. This was my method for many years, and I have no regrets. My current distrust of Apple and their data collection has eliminated this possibility for me and my high-risk clients. Apple requires an Apple ID which will be used to assimilate all collected data into your profile. Apple will know a lot about you, but there will be no evidence of your true location, as long as you are connected to a home network VPN (explained later). It may surprise some readers that I recommend a single GrapheneOS device for travel and home usage over this option. I believe that you have the discipline to stay in airplane mode while near your home, but consider all of these options carefully.

I followed the secondary iPod Touch strategy until 2021. Today, I do not use any iOS devices due to their requirement to possess a valid Apple ID, constant data collection, and increasing privacy invasions. What do I do now? I have two GrapheneOS devices, but I rarely use the "home" device. One is my "travel" device which is dropped into a Faraday bag at a specific place before going home. The other is my "home" unit which has never possessed a cellular SIM card and never leaves the house. It only uses Wi-Fi in my home and is almost a clone of the travel device. I find myself relying on my laptop for the majority of my communications from home. There are days when I never turn on the secondary device. This may be extreme and paranoid, but remember why you are reading this book.

Since my "home" GrapheneOS operating system does not share any device information to third-party servers, and a Google or Apple account is not required to use the device, my fears of data collection from my VPN-protected home network are minimal. This also applies to my laptop. Since there is no cellular connection enabled and a SIM is missing, I do not worry about cellular network connections associating my usage to my travel device or a cellular account. GrapheneOS updates and reboots do not reset the radio connections similar to Apple, so accidental disabling of airplane mode is also minimal. Is this perfect? No. The worst-case scenario is that I accidentally enable the cellular data connection; the home device connects to a cellular tower without a SIM card; and that cellular company now has a record of that specific hardware's location. The device was purchased with cash and it has never registered to any cellular account. The damage would be extremely minimal. The cellular tower company would have no information to offer. Is it best for you? Only you can determine that. I present this here to simply disclose my own modifications as my privacy plan changes.

Reality Check: Do you need two mobile devices? If your prepaid service is in an alias name; you have never used the number assigned to the account; and your device was purchased with cash, it might not matter. I know many people who place their GrapheneOS device into airplane mode before they approach their homes and do not have issues of being tracked. Stock Apple and Android devices present greater risk. Ultimately, this all depends on your level of discipline and overall privacy and security threats.

If you go through the troubles of obtaining an anonymous home as discussed later, these steps may be vital so that you do not expose yourself. Airplane mode is not always enough, especially with iOS. Apple system updates disable airplane mode on reboot. It only takes one accidental connection to create a permanent record of the location of a device. These steps prevent unintentional exposure that could ruin all of your hard work.

Some readers of the previous edition expressed concerns of Apple eliminating the iPod Touch from its lineup of mobile devices. Fortunately, they released a 7th edition in 2019. This device supports the current version of iOS (15). Based on previous support models, I expect the latest iPod Touch to receive support updates through 2023. You should note that all iPod Touch models lack Touch ID, Face ID, 3D Touch, NFC, GPS, an earpiece speaker and a noise-canceling microphone. However, all communication functions work well with a set of earbuds which contain an in-line microphone (such as those included with most older iPhones).