

COMSEC

OFF-THE-GRID COMMUNICATIONS
STRATEGIES FOR PRIVACY ENTHUSIASTS,
JOURNALISTS, POLITICIANS, CROOKS,
AND THE AVERAGE JOE



JUSTIN CARROLL & DREW M.



INVESTIGADOR_Z

INVESTIGADOR_Z

COMSEC:
OFF-THE-GRID COMMUNICATIONS
STRATEGIES FOR PRIVACY
ENTHUSIASTS, JOURNALISTS,
POLITICIANS, CROOKS, AND THE
AVERAGE JOE

BY JUSTIN CARROLL AND DREW M.

COMSEC: Off-The-Grid Comm

Copyright © 2018 by Justin Carroll and Drew M.

All rights reserved. No part of this book may be reproduced in any form or by any electronic or mechanical means including information storage and retrieval systems without permission in writing from the authors.

First Published: July 2018

The information in this book is distributed on an “As-is” basis, without warranty. The authors have taken great care in preparation of this book but assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

Rather than use a trademark symbol with every occurrence of a trademarked name, this book uses the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

Due to the use of quotation marks to identify specific text to be used as search queries and data entry, the authors have chosen to display the British rule of punctuation outside the quotes. This ensures that the quoted content is accurate for replication. To maintain consistency, they continued this format throughout the entire book.

ISBN-13: 978-172224787

ISBN-10: 1722124784

INVESTIGADOR_Z

Table of Contents

[ABOUT THE AUTHORS](#)

[INTRODUCTION](#)

[CHAPTER 1: THE INSECURITIES OF PHONES](#)

[THE BASEBAND PROCESSOR](#)

[THE INSECURITY OF SMS AND STANDARD VOICE CALLING](#)

[THE APPLICATION PROCESSOR & APPLICATION PROCESSOR OS \(APOS\)](#)

[SUMMARY](#)

[CHAPTER 2: THE SMARTPHONE RE-IMAGINED](#)

[CHALLENGING THE STANDARD](#)

[PURCHASING PHONES ANONYMOUSLY](#)

[PURCHASING SERVICE ANONYMOUSLY](#)

[SUDO](#)

[GETTING RID OF OLD/UNUSED PHONES](#)

[SUMMARY](#)

[CHAPTER 3: SECURE YOUR SMARTPHONE APOS](#)

[OPERATING SYSTEM UPDATES](#)

[APPLICATION MANAGEMENT](#)

[DEVICE ENCRYPTION](#)

[PRIVACY SETTINGS](#)

[RESTRICTIONS \(iOS ONLY\)](#)

[SUMMARY](#)

[CHAPTER 4: SECURE YOUR COMMUNICATIONS](#)

[VIRTUAL PRIVATE NETWORKS](#)

[GENERAL-USE VPN RECOMMENDATIONS](#)

[IOS-SPECIFIC VPN RECOMMENDATIONS](#)

[SECURE MESSAGING APPLICATIONS](#)

[BEST PRACTICE: VERIFYING KEY FINGERPRINTS](#)

[CHAPTER 5: A SMARTPHONE WITHOUT A PHONE](#)

[WHY AN IPOD IS MORE PRIVATE AND SECURE THAN A PHONE](#)

[DREW'S IPOD SETUP](#)

[Device Setup](#)

[CUSTOM NUMERIC VS. CUSTOM ALPHANUMERIC PASSCODES](#)

[USE CASE SCENARIOS](#)

[UNINTENDED CONSEQUENCES OF THE IPOD TOUCH](#)

[CHAPTER 6: COMSEC BEST PRACTICES](#)

[PHYSICAL SECURITY](#)

[ENCRYPT APPS](#)

[PRIVACY SCREENS](#)

[CAMERA COVERS](#)

[MIC-LOC](#)

[FARADAY BAGS](#)

APPENDIX I: OUR COMSEC SUITES

[DREW'S MOBILE DEVICE STRATEGY](#)

[JUSTIN'S MOBILE DEVICE STRATEGY](#)

APPENDIX II: RECOMMENDED APPS

[MAIL CLIENT](#)

[NOTES](#)

[BROWSERS](#)

[AUTHENTICATION MEASURES](#)

APPENDIX III: FUTURE COMSEC SOLUTIONS

ABOUT THE AUTHORS

Justin Carroll is a former Marine, plank-owner in the elite Marine Special Operations Command (MARSOC) and has worked on a contractual basis with another government agency. After completing his last overseas deployment, Justin spent five years teaching digital security and identity management to hundreds of soldiers, sailors, and Marines of the United States Special Operations Command (USSOCOM) and was instrumental in the development of a highly technical surveillance program currently in use abroad by US Special Operations Forces. Justin resides just outside of Nashville, TN and is the author of *Your Ultimate Security Guide: Windows 7*, and *Your Ultimate Security Guide: iOS*. He co-authored *The Complete Privacy & Security Desk Reference* and is the co-host of *The Complete Privacy & Security Podcast*.

You can follow and contact Justin through his blog: [**https://operational-security.com**](https://operational-security.com)

M. Drew is a Detective in one of our Nation's largest cities assigned to high profile cases that often require covert investigative skills. He investigates crimes involving narcotics, gangs, adult & child sex crimes, human trafficking, and Internet crimes against children (ICAC Task Force). As an open source intelligence analyst and computer forensics and cyber-security specialist, he utilizes these skills to assist in criminal and private investigations of all types. He is a veteran investigator at his agency, and forever a proud United States Marine with overseas deployment experience. First and foremost, he is a privacy and security advocate with a passion for teaching digital operational security and identity management solutions. His classes are available nationwide to law enforcement, military organizations, and select groups in the private sector.

You can follow and contact Drew through his blog: [**https://hidingfromtheinternet.com**](https://hidingfromtheinternet.com)

INTRODUCTION

A Note from Justin

I have written several books dealing with end-user security prior to this one. As my experience and knowledge have expanded and matured, so too have some of my opinions and ideas on best practices. One such example is my exhortation to refer to a phone not as a phone, but as a computer. This is true, but it is not the whole story. What I was only dimly aware of at the time is that yes, the modern smartphone contains a computer, but it also contains a much more antiquated piece of hardware that is far more dangerous than the computer. This is the portion that actually makes it a “phone”. And the vulnerabilities that the “phone” adds to your iPhone or Samsung or even your Blackphone are difficult to fully grasp.

It amuses (and sometimes embarrasses) me to consider how I thought about mobile phones and mobile phone privacy just a couple of years ago. Or even just a few weeks ago. Penning Chapter One of this work has alarmed me afresh to the risks carrying a phone introduces. The one, most important takeaway that I hope each reader gains from this book is a firm understanding of the compromise we all make when we stuff a smartphone into our pockets and purses. As a society we should be far more aware of and concerned about this than we are. That is why the first chapter of this book is, to me, the most important. Read it, internalize it, and share it with others.

Writing the remainder of this book and working with Drew (on a project that was originally his idea) has been a pure joy. Very little of what we covered here is entirely new ground, but I do feel that we have both added new value to the topic. We hope you enjoy it, and more importantly, learn from it and put the techniques here into action.

Justin Carroll
Nashville, TN

A Note from Drew

Consistently, the most popular and discussed topics when I teach digital privacy & security courses are the communications strategies we use. In a digital age where technology connects everyone to each other, students learn that this convenience also comes with many real-world concerns. Collaborating with Justin on this project was truly a pleasure and we had a lot of fun compiling so much of what we have learned over the years about secure and private communications.

For me, privacy isn't about hiding something. It's about being able to control how we present ourselves to the world. It is the right to keep things to yourself. Technology allows us to challenge the traditional methods of using a cellular phone and leverage tools to enhance both the privacy and security of our devices. The protection of our personal information, online and in the physical world, has never been more important.

Law enforcement professionals, military personnel, whistle-blowers, and every citizen needs to understand the threats due to the relentless collection of personal data. This book explores many ways to take back control over the information our communication devices collect, share about us, and how to mitigate surveillance efforts that take place without our knowledge or permission. This guidebook is a collection of tactics and strategies that will help you make important changes in how you communicate in order to reclaim your right to privacy.

Lastly, thank you to my closest friends and colleagues who encouraged me to begin sharing my research into these topics over the years. To all of these amazing people in my life, thank you for the inspiration and your willingness to learn more.

Drew M.
Homestead, FL

CHAPTER 1: THE INSECURITIES OF PHONES

If you purchased this book, it is very likely that you already know why you need it. What you may not realize is the full extent to which you need it. All of us generally assume that no one is listening in on or recording our phone calls. If we assumed otherwise we wouldn't use the device. And mostly, we're right. But the risks of using a cell phone go much deeper than this. And it wouldn't feel right to open a book like this without exploring the breadth of what is possible.

What separates your iPhone X or Google Pixel from an old Nokia candy bar or Motorola RAZR from the very early 2000s? The main thing that most will point out is the large monitor (which we call a screen) and the addition of a computer. And you wouldn't necessarily be wrong; those things are different. It is useful to think of today's smartphones as consisting of two major components: the true "phone" and a computer. The computer is the portion with which we interact with on a daily basis. It consists of a processor, RAM, storage, operating system, and is made usable via the screen. It runs apps. It operates the camera. It works with the magnificent sensor array installed into the phone. It makes the phone "smart". There is no doubt that today's phones are more beautiful, powerful, and sleek than those basic candy bar and flip-phones of just a few years ago. But when it comes to how the device interacts with the cellular network, the real answer to the question with which we opened this paragraph is, "not much."

THE BASEBAND PROCESSOR

The cellular modem in your iPhone X or Samsung Galaxy S9 is almost indistinguishable in function from those found in the old bag- and car phones of yesteryear. The cellular modem (called the baseband processor or

baseband modem) that allows your phone to connect to the network hasn't evolved very much in a couple of decades. Consumers don't see this part of their "phone" and even if they did, probably wouldn't care much about it. But it is extremely problematic from a privacy standpoint and most of our readers probably care a great deal.

Your device's baseband processor is discrete from its Application Processor (AP) for a couple of reasons. First, your connection to the cellular network is largely dependent on a radio signal that must be extremely finely timed with the network's clock. Each tower can handle hundreds or thousands of users by separating them through time-based multiplexing. By separating the baseband processor and the AP, the baseband is freed to run a Real-Time OS (RTOS). The RTOS is capable of handling the exacting timing demands of the network. Additionally, the baseband hardware is optimized for radio transmission and reception. Neither of these are tasks at which the smartphone's "computer" (AP) would excel.

Secondly, many regulatory bodies (including the Federal Communications Commission [FCC] in the United States) require that all devices that interact directly with the cellular network be certified. Separating the baseband processor allows it to be certified separately, relieving the hardware manufacturer of certifying the entire application processor. This has some benefits to the end user. It allows manufacturers to update the Application Processor Operating System (APOS) much more frequently without having to go through lengthy certification processes, resulting in much faster updates to the APOS. This is far from a perfect model, however.

Privacy Problems with the Baseband Processor

The problems with baseband processors are widely known and have been for years. Cellular Service Providers (CSPs), governments, and hackers are all well aware of these issues. Unfortunately, the cellular providers and hardware manufacturers have made only token moves to correct them. The following is a list of concerns you should be aware of if you own a mobile device.

User Inability to Control the Baseband: The biggest danger represented by

the baseband is not the malicious actions it can be exploited to take. Instead it is your inability to control this processor. Because this processor is hidden from view, both physically and through any software settings, it is impossible to control. As long as the device has power the baseband processor may be on. Initiating the phone's "power down" sequence only has a guaranteed impact on your device's AP. In effect this means that all of the actions listed below may be taken whether or not the phone is visibly powered on.

The only way to fully defeat the baseband processor is to fully remove its power source. While once extremely easy, this is no longer a possibility to the vast majority of smartphone owners. Most hardware manufacturers have moved to cases that are not designed to let the user remove and replace the battery, leaving us all at the mercy of the baseband processor.

A note on terminology: because the baseband processor cannot, with any certainty, be turned off by the user, we will not reference "turning off" or "powering down" the device. Instead we will use some variation of "placing the phone in a dormant mode" to refer to this process. We feel this is an important distinction and we do not wish to perpetuate the myth that a smartphone can be fully turned off.

Since removing the battery in most modern smartphones is an impossibility, so is controlling the baseband processor. Even if your phone is in a dormant mode, the baseband may be manipulated to perform any of the actions described below.

Location Tracking: Because this processor may be constantly engaged it may be collecting your location at all times. We consider this to be one of the greatest threats to your privacy. All smartphones now offer the ability to somewhat control location services on the application processor level through software settings. It is impossible to control the baseband processor, however. One noteworthy example of this is the Android phone debacle that made news in late 2017.

The online magazine *Quart* broke a story in late December detailing Android's data collection. Even with location services fully disabled, it turns

out that Android phones were still reporting their location to Google (the maker of the Android AP operating system). This was all made possible thanks to the baseband processor. Even with location services completely disabled and no SIM card present, devices were able to record their locations in relation to cellular towers. Google admitted to this practice immediately and agreed to end it. This still does not protect you from the cellular carrier, however.

Each time a cellular phone “talks” to a cell tower it creates a record that will be maintained by the carrier who provides that tower for a minimum of five years. This creates a massive amount of historical data about your movements and activities. This should be especially alarming if you are an individual who works diligently to protect his or her personal privacy in communications and movement. All of your hard work may be undone one day. When it is and the phone’s IMEI is associated with your name, all of your historical data is, too. This unmask you not only into the future, but also into the past, and with anything you have done and anywhere you have been with that device.

It would be reasonable to assume that these records are only created and stored by the service provider that you have contracted to provide service. You would be wrong here, too, however. When your phone interacts with any cellular tower a record is created. The phone sends some basic subscriber information (including its IMSI, see definitions below) to the tower. The tower will determine whether or not that device is authorized to access its network. If it is allowed a process called an “IMSI Attach” will proceed, allowing your SIM card to connect to the tower and utilize the network for service. If your device is not authorized on that network it will be rejected. This will be stored in the tower’s rejection logs. Even cellular providers other than your own are tracking your location!

Where Does All This Data Go?

As we have seen, carrying a mobile device exposes you to constant location

tracking that you cannot disable and cannot opt-out of. Where does all this data go, and how is it used? Cellular service providers are not blind to the fact that they have amassed a treasure trove of marketable data.

Cellular service providers vary in the volume and types of data they are willing to share with advertisers. For example, Verizon's "Precision Market Insights" is one of the most aggressive collection and monetization policies we've ever seen. Verizon sells your location data, lists of apps you have installed, and the websites you visit. Supposedly this data is anonymized, but we don't place a lot of trust in anonymization. This data is also sold to third-parties that put it into mappable databases, which are sold to law enforcement agencies. Because the phone number or IMEI is obscured by an "anonymized" identifier, such behavior does not (at least theoretically) violate federal wiretapping or surveillance laws.

According to Verizon's Full Privacy Policy (<https://www.verizon.com/about/privacy/full-privacy-policy>), even selling all of your mobile data is not enough. Verizon even shares your "credit information for our marketing of new services to you." Combined with your location data, interests, apps and app usage, this is incredibly intrusive (and valuable) information. We feel that you ought to be troubled by this and should demand a service model that provides a straightforward service in exchange for your direct financial support.

Customers of most CSPs have at least some ability to opt-out of data collection and monetization. Verizon is now running a program called Verizon Selects that is even more intrusive but requires an opt-in (in exchange for "rewards"). Though we have picked on Verizon, AT&T, Sprint, T-Mobile, and others all participate in similar data collection and sharing programs. Conduct some research on your cellular service provider to find out how to opt-out of this information sharing.

NOTE: The IMEI and IMSI are numbers that are unique to your phone and its service provider/plan. It would be inappropriate to continue further into

this book without discussing these identifiers and what they mean.

- **International Mobile Equipment Identity (IMEI)** - This number is hard-coded onto your device and will never change. Even if you change your service provider, SIM card, and telephone number, the IMEI will link old and new together. Though the IMEI is not shared with the cellular towers your phone sees, this number is recorded when you purchase your device. Even if you switch service providers this number will follow you as long as you own the same device.
- **International Mobile Subscriber Identity** - The IMSI is not related to hardware on your device. This identifier is derived from the SIM (Subscriber Identity Module) card that is issued by your cellular service provider. This number is shared with the towers to which your phone sends connection requests. This number is associated with your service plan and the location where the IMSI was initially activated.

Electronic Eavesdropping: Your cellular service provider (and any government that can influence your cellular service provider) can access the baseband processor at will. This can be used to invade your privacy to a degree that most individuals would never imagine or consider feasible if they did. The phone's microphone can be accessed and activated at will. This can allow eavesdropping on not only telephone conversations, but anything that can be received by the device's internal microphone.

Many privacy enthusiasts take measures to prevent their communications from being intercepted in transit. This largely consists of using encrypted messaging and voice applications. There is certainly merit to this strategy as it protects your communications in transit. If the device's microphone is compromised these applications will do you little good. Your communications may be captured directly at microphone if your adversary has access to your baseband processor.

This access to the baseband can also potentially allow an attacker to activate the device's camera. This is alarming to consider, but it is generally less

problematic than the microphone being compromised. First, cameras can be fitted with “hack-proof” covers (see Chapter 6). Next, the compromising images the camera captures are few relative the vast number of images of the inside of your pocket or purse. Though it may catch some here and there, the microphone has the potential to capture every word you utter if you spend all waking hours within earshot of your phone or cellular-connected tablet or other device(s), and is much more dangerous as a result.

Firmware Vulnerabilities: The firmware that runs baseband processors is infrequently patched. This means that billions of phones all over the world are running baseband processors and RTOSs that have unpatched security vulnerabilities. Security researchers have warned of the dangers of these processors for years, but the industry has paid little mind. In the last year we have seen numerous reports of vulnerabilities discovered in baseband processors

Protecting yourself from the two sides of your smartphone (the Baseband/RTOS and the AP/APOS) require different strategies. The first chapter of this book will cover protecting yourself from your device’s computer. Successive chapters in this work will discuss protecting yourself from the vulnerabilities inherent in the existence of a baseband processor.

THE INSECURITY OF SMS AND STANDARD VOICE CALLING

Cellular telephone calls and SMS messages are both insecure and non-private. Your calls are accessible to the CSP. The content of all your SMS text messages is fully saved and recorded by your CSP. In addition to the content, all of the metadata about these transactions is recorded and stored, as well. This creates a privacy nightmare that is just waiting to happen.

All it takes to verify this is a quick look at your cellular phone bill. The bill will show a long list of incoming and outgoing calls, incoming or outgoing SMS messages, and in some cases even the city where your phone was

located at the time of the event. All of this metadata about your calls and texts, and the content of your texts, is stored for a minimum of five years. This information is consistently abused by CSPs who monetize it.

Verizon: On the counts of collecting and monetizing metadata and failing to provide meaningful protection to calls and messages, Verizon Wireless is perhaps the worst offender of the top-tier CSPs. Verizon sells your location data. While encrypting your calls is standard industry practice, Verizon fails to do so. We don't mean to imply that any of the major cellular providers are much better; we only mean to point out that Verizon is particularly notorious in this regard.

Government Access: Because your cellular calls are either encrypted poorly or not at all, their content is available to governments. Governments may access the content of your calls and SMS through the application of legal pressure. Governments may also access your calls without the complicity of the CSP through the use of a cell site simulator. A cell site simulator is an electronic device that puts out a very strong signal that your phone will recognize as a cell tower. If you are within its range and your phone assesses its signal to the strongest signal available, your phone will connect to the simulator.

Once your device is connected to the cell site simulator, all of your traffic will flow through the simulator where it is collected. Your only defense against this type of attack is to use strong encryption. Though we are not anti-law enforcement, we do recognize that these types of devices are frequently used without warrants, and they frequently capture the conversations of people other than the intended target. Neither of us are criminals, nor do we condone criminal activity, but neither of us want to be swept up as “incidental collection”.

SS7 Vulnerability: Modern cellular carriers utilize a routing protocol known as Signaling System 7 (SS7). This protocol was designed in the mid-1970s and allows carriers to exchange information between each other. This information is used to pass calls and messages between carriers, and to keep track of billing and usage. It is also used to verify roaming plans before

devices are allowed to access other networks. Unfortunately, this protocol has some major systemic vulnerabilities.

Hackers are sometimes able to break into the SS7 system. This provides capabilities similar to those of government actors. Hackers can forward calls and texts silently so that your device will give no indication of an incoming call. This could be used to deny you service, ascertain with whom you are communicating, or capture two-factor authentication tokens sent via phone call or text. Hackers can also view text messages sent via standard SMS between devices and track your location through the exact same protocols that CSPs and government actors do.

Unfortunately, there is very little you can do to correct the underlying vulnerability. However, you can take steps to mitigate some of the symptoms of this problem. We will discuss these throughout successive chapters of this book.

THE APPLICATION PROCESSOR & APPLICATION PROCESSOR OS (APOS)

Wi-Fi, Bluetooth, and NFC

If you own a modern smartphone it is almost certainly equipped with Wi-Fi, Bluetooth, and near-field communication (NFC) interfaces. Each of these presents more attack surface.

Wi-Fi: Accessing the internet wirelessly opens up a number of dangers. When you connect to a Wi-Fi network you should consider the following threats and threat actors:

- **Packet Sniffers:** Wi-Fi is nothing more than a radio that can transmit and receive data packets. Anyone within range of your radio (Wi-Fi) traffic to and from the router can potentially “listen in” on this traffic. All data packets that you transfer over Wi-Fi are vulnerable in the air-gap between

your device and the access point. Hackers with a simple program like Wireshark and a Wi-Fi antenna that can be placed in promiscuous mode may capture all of your packets and exploit them for personal or financial information.

Rogue APs/Evil Twins: Hackers can setup access points whose SSIDs are the same or similar to real APs in the local area. For instance, the legitimate Wi-Fi hotspot SSID at the San Diego Airport is #SANfreewifi while a malicious hotspot might be #SANfreewi-fi (notice the very subtle difference) in hopes of getting some uninformed or inattentive travelers to connect^[1]. Alternatively, a hacker may see your device's probe frame requests for networks it "knows" and will connect to automatically (probe frame requests are discussed in greater detail on page 14 in the section titled "SSID Broadcast"). He or she could then create an ad-hoc network using one of these names and your phone would connect to it, unbeknownst to you. The attacker now has the ability to receive and record every packet that is passed through his device.

Hardware Owners: Even if you manage to connect to the correct hotspot at the San Diego airport, your traffic is still routed through hardware you don't control. This means the network administrator at the airport will have access to all of your packets, as well. It is unlikely that most hardware owners are collecting all of your packets, but they do collect a substantial amount of metadata. This includes your device's MAC address, the times your connection was initiated and terminated, and the amount of bandwidth used. In many public Wi-Fi hotspots the websites you visit may be recorded, too.

Internet Service Providers: When your traffic reaches the local access point it will go through a process called network address translation (NAT) in preparation for being passed along to the Internet Service Provider (ISP). The ISP will shuttle your traffic to its intended destination and return that traffic back to you. Again, because you are choosing to put that traffic onto someone else's hardware, the ISP can retain your packets. If you are not using a Virtual Private Network (see Chapter 4) the ISP

potentially has access to everything you do online.

Governments: There are no countries in the world where the government does not exert some level of influence over internet service providers. Though some countries have stronger legal protections than others, you should assume that if the government wants to monitor your internet traffic, it can do so by applying legal pressure to the ISP. Additionally, governments have extremely robust offensive digital capabilities. It should be assumed that governments can, by default, inspect your traffic even without the ISP's consent or complicity.

Location Tracking: Wi-Fi is another mechanism through which your location may be tracked. Doing so requires access to the routers to which your device communicates in some way. This can be an explicit communication, like connecting to the router, or a subtler connection. Routers are capable of monitoring your device's probe frame requests - the requests that are transmitted when the device is searching for Wi-Fi. Because the set of networks that your device "remembers" is very likely unique to only you, this is a valuable identifier. When you walk around some large department stores Wi-Fi receivers are in place for this very reason - to track your habits in the store.

This model scales very efficiently and can be used to track your movements around a city, as well. This model also scales very efficiently the other way - Wi-Fi can be used to track your movements with extremely levels of accuracy and granularity by a single router. An individual router to which you are connected can measure your signal's round-trip-time (RTT) between the device and router. With enough data this can be used to map your entire house and tell exactly where you are within it at any given time.

Reverse Location Tracking: The previous paragraphs address Wi-Fi access points that can determine your location through probe frame requests, but this process also works in reverse. Apps that are installed on your device have the potential to see the networks that are within range of your device. By triangulating your position based on the observed networks

and their relative strength, your location can be determined with a good degree of accuracy. This data can then be shared with the app developer, hardware manufacturer, and parties that are able to intercept this data in transit^[2].

SSID Broadcast: When your device is not connected to Wi-Fi, it is broadcasting probe frame requests for all of the networks to which it has previously connected. This sets you up for an evil twin attack as described above, but it also reveals information about your day-to-day habits. Using open-source lookup tools like Wigle.net (<https://wisle.net>), a popular website that crowd-sources data about Wi-Fi hotspots, an attacker can map all the hotspots to which your device connects. This data can then be analyzed to reveal where you live, work, and frequent. You don't have to be followed around constantly, or even be the target of constant electronic surveillance for an attacker to know where you will be at predictable times.

Bluetooth and NFC: Both of these protocols present some common dangers. Because both emit a very small electronic signal around your device, both can be used for location tracking. This signal is associated with your device's MAC address, which can be used to identify you.

Bluetooth (or Bluetooth Low Energy, BLE) presents some unique challenges. Because of its versatility, Bluetooth is used for connecting all sorts of devices for all sorts of purposes. The Apple Watch pairs to one's iPhone via this protocol. Bluetooth is used to connect your phone to your car so music can be shared. It is used in the Airdrop file-sharing protocol, and for connecting hands-free communication devices.

Because such a potentially large volume and wide variety of data is transmitted through Bluetooth, hackers have been hacking it since the moment it was released. Generally, we recommend you avoid using this protocol altogether, or use it only for benign purposes. Connecting your device to a Bluetooth speaker inside your home is relatively low risk but using Bluetooth to carry out sensitive phone calls in public is not. We also strongly recommend you avoid using Bluetooth in conjunction with devices

like the Apple Watch. This device receives location data (from maps), text messages, and much more from your phone. Putting this data in transit (if only for a very short range) opens it up to a host of other attack vectors.

Like Wi-Fi, Bluetooth can also be co-opted to capture extremely granular levels of location tracking. Since the signal emitted by Bluetooth is so small, your proximity to a Bluetooth transceiver can be determined with accuracy down to a matter of inches. Tracking one across a larger area obviously requires the area be littered with many Bluetooth transceivers but they are fairly inexpensive and easy to implement. When location data is correlated with your device's MAC address this location data is correlated with you.

Defeating These Vulnerabilities

Most books, blogs, and lectures on mobile device security focus on protecting the computer portion of mobile devices. Because they are so deeply embedded into our devices, and because we have so little control over them, defeating the baseband modem is extremely difficult. But it is not impossible. The remainder of this book will focus on interventions designed to protect you from the phone's computer, its impressive sensor array, AND the baseband processor and its capabilities. Some of these techniques will seem drastic, but so are the capabilities of the modern mobile phone. Drastic measures are required, and in light of the slew of exploits against mobile devices, we feel they are completely justified. Ultimately it is up to you to choose your path and decide which of these techniques is right for you and your situation.

SUMMARY

By carrying a smartphone, you are making an enormous privacy compromise. You have chosen to carry a device that marries an incredible sensor array and several radio interfaces with a baseband processor. When combined, your device is capable of:

- Constantly monitoring and recording your location, even when you

- have disabled location services and believe the device to be turned off,
- refine your location through Wi-Fi and Bluetooth to a matter of a few feet, and determine your location within a building,
- monitoring your microphone, even when you believe the device to be turned off,
- remotely activating the camera(s),
- betraying your standard voice and text data to the cellular service provider, law enforcement and government agencies, and malicious hackers, and
- Mapping your home, and knowing when you sleep, wake, and your patterns of activity.

CHAPTER 2: THE SMARTPHONE RE-IMAGINED

CHALLENGING THE STANDARD

Traditionally, most people purchase a cellphone and service for that phone in the following manner: you choose the type of phone you would like to have, find a provider that carries that model, and then decide on a rate plan that fits your calling and data needs. The phone itself typically costs several hundred dollars, and the cost is subsidized and financed by the carrier in exchange for signing a one or two-year contract of service with them. Your new phone is then assigned a phone number from the carrier.

That business model enables a person to pay less (up front, but more overall) for the latest technology and choose a rate plan that suits his or her needs for the foreseeable future. Additional phones can be added to the account for additional savings and “family plans” can be set up to accommodate multiple phones under that same account. This method of obtaining cell phone service should sound very familiar and is likely the way you obtained your last cellphone.

When the cellular service provider subsidizes the cost of the phone and you sign a contract for service with them, your credit worthiness is checked as part of that process. Therein lies the first problem for those of us who desire to maintain privacy with our communications. By allowing a CSP to check your credit worthiness, details such as your SSN, true name, carrier assigned phone number, and service plan are forever tied to that particular device. Additionally, phones are frequently purchased using a credit card in the purchaser’s true name. However, you can also maintain your privacy and enhance the security of your communications.

Anyone concerned with their privacy will need to challenge the standard way of obtaining a cellphone and service. By purchasing your phone anonymously, obtaining service anonymously, and using your phone number in a non-traditional manner, you can still enjoy the convenience of cellphone service. However, you can also maintain your privacy and enhance the security of your communications. The location-tracking we discussed in Chapter 1 is much less frightening if the phone being tracked is not correlated with your identity. Let's take a closer look at how the privacy conscious individual achieves this goal.

PURCHASING PHONES ANONYMOUSLY

Purchasing a phone anonymously is similar to making any other type of purchase anonymously. There are several options and the most obvious is to make the purchase with cash. With a cash purchase you will pay full price for the phone up front. It will not be subsidized or financed by the carrier in any way. That is the first hurdle for most people who have a desire for private communications to overcome. Gone are the days when you walk in to a store and pay very little or nothing at all for your phone in exchange for a cell phone service contract – at least for those of us who desire private communications. Options for obtaining service will be discussed next, but for now let's focus on the phone itself.

When you pay cash for the phone you can obtain it anywhere. If you desire a new phone, choose a retailer that sells the model you want to buy and purchase it there. Simply walk into the store select the unlocked model of your choice and pay with cash. Something to be aware of though, is that you will most likely be asked to provide personal information about yourself during this process. Sales clerks will attempt to gather all sorts of information from you during the purchase. You may be asked for your name, for an email address to which to send the receipt, a phone number, or if you wish to participate in an extended warranty plan. These are routine questions a sales clerk will ask as a matter of standard operating procedure. When making a purchase of this type with cash you are not obligated to provide any personal information. We recommend always being kind and courteous, and to either

decline to provide the information or simply provide false information in the form of an alias name. Ask for a paper copy of the receipt^[3] and leave the store knowing you just made a purchase without giving up any personally identifiable information.

Some privacy advocates will take an anonymous purchase a step further out of necessity due to their threat model, or out of paranoia and enthusiasm for privacy. When making a purchase at a retailer, you have likely been captured on surveillance video making the purchase. The date and time stamp on the surveillance video could be matched up with the transaction record of your purchase which would reveal the serial number of the phone you purchased. Your name may not be attached to the purchase, but what about the surveillance video of you walking out of the store to your vehicle? Was your license plate also captured on video in the parking lot, an ATM or at a nearby license plate reader? You can see how the level of paranoia grows the more you think about the topic. Surveillance video is often kept for at least 30 days at retailers and oftentimes a person will wait until that time period has expired to activate their new phone. Only you can decide if that is important to your scenario. Another option is to have someone else make the purchase for you. The privacy pursuit affords a lot of opportunity to be creative so we encourage you to decide how far you want to take those efforts.

Purchasing a used phone from a third party may also be an option. A used phone's IMEI number would be tied to the previous owner(s) of the phone, which may or may not be a concern for you. A used phone would also mean you are purchasing older technology, which would save money compared to a new device. The decision on this ultimately lies with the end user (you), however we prefer to purchase a new device whenever possible.

Now that a new phone has been purchased without jeopardizing your personal information, the next step is to obtain service from one the major cellphone carriers in the same, anonymous, manner.

PURCHASING SERVICE ANONYMOUSLY

To maintain your anonymity with a cellphone service plan, you cannot undergo a credit check. Because you own the phone and are not receiving financing from the CSP, there is simply no need to verify your credit. The best option for providing service without associating a name and credit information is to use pre-paid service. All of the major U.S. wireless carriers offer pre-paid service options. Pre-paid wireless service is primarily intended for individuals with little or no credit who would otherwise be unable to obtain a traditional service plan where a credit check would be required. As a customer of pre-paid wireless service, you are responsible for paying your balance in advance each month in exchange for the service plan you chose when signing up.

Because the carrier is paid in advance for service you have not yet used, there is little to no risk from the carrier's perspective about you as a customer. If you do not pay for your monthly service, the carrier has not subsidized the phone for you and they are not left trying to collect from you on a service contract that you agreed to. The customer has already paid full price for the phone in this scenario, and in order to receive monthly service they need to pay in advance for that service. The pre-paid service is on a month-to-month basis and the customer can choose at any time to change their service options or change carriers entirely to take advantage of another pre-paid service that better suits their needs. Pre-paid wireless service offers a lot of flexibility and options to the privacy-conscious consumer.

The wireless service provider of your choice will likely have many different pre-paid options available when you visit their store. For our purposes we recommend choosing a rate plan that offers maximum data capacity. We do not care how many texts or voice minutes are allowed on the plan. The reasons for this will be explained later, but when looking through the various service options, keep an eye out for monthly plans that are heavy in data service and minimal in actual calling minutes. A plan such as this will allow you to take advantage of the data requirements of your new wireless service strategy.

If you choose to setup your new plan in-store, the sales clerks will attempt to gather all sorts of personal information about you. This is standard

procedure, but remember we are breaking away from the traditional way of doing things here. Where possible, we prefer to activate our service online. Major retail outlets like Best Buy, Target, and Wal-Mart allow you to walk in and pay cash for SIM cards from major carriers. You can also purchase a scratch-off voucher for a month of service on the plan of your choice. These can be paid for in cash and no personal information whatsoever is required. Later, you can install the SIM into your phone and activate it online, following the instructions enclosed with the SIM. When possible, we prefer to leave the name on the account at the default: “Registered User”, “Pre-paid Customer” or “Account Holder” are all options that we have encountered.

When you set up the new account, you will be asked to pay your first month of service in advance, along with an activation fee. By now you may have guessed that the best payment option is to pay with cash. The monthly service can also be paid for in cash by visiting the wireless carrier’s store each month. We dislike this option because if you have waited 30 days after purchasing your phone, you immediately associate it with your likeness when you walk into the store to pay your bill. Depending on your budget, it may be convenient to pay for several months in advance to reduce the number of times you have to visit the store to bring your account current.

There are two other ways you can choose to pay for your wireless service. We prefer these to paying in person. The first is to purchase prepaid wireless payment cards. Many major carriers including AT&T and T-Mobile sell these. They are typically available where gift cards and pre-paid credit cards are sold. We have seen them in grocery stores, pharmacies, gas stations, department stores, electronics stores, and home improvement stores. With these cards you simply scratch the back of the card and text the code to a payment number. Of course, you should pay for these with cash.

The other payment option is to use a service like Pay With Privacy (<https://privacy.com>). Privacy.com is a virtual credit-card service that allows you to create different credit card numbers for all of the merchants with which you deal. This strategy offers privacy as opposed to total anonymity as the charges to each Privacy card are debited to your bank account. This would be vulnerable to a warrant or other government requests and should be

a consideration if this is in your threat model. The benefit of this strategy is that your monthly payment may be slightly discounted (a discount of approximately \$5/month is typical). Only you can decide if this is worth it. We recommend you carefully consider your threat model because once your name is correlated with the device, so is all future activity. Unfortunately, so is all historical activity, so you have completely undone any privacy gained by purchasing the phone and its service anonymously.

By paying for monthly service with a credit card that is associated with your identity, you immediately pierce the layer of privacy we desire by metadata association. Details from the credit card such as name and billing address will now be tied to the phone. Our recommendation is to plan ahead, pay with cash, and maintain your privacy surrounding that phone and the service^[4].

///// PROTECT YOUR “REAL” PHONE NUMBER /////

After you have activated service for your anonymously purchased phone, your prepaid account will be active and the carrier will have assigned a phone number to that phone. To maximize the privacy and security of your communications strategy, we highly recommend never using that carrier assigned phone number for anything. You will not place a single call from your new phone, receive a single call to it, or give that number to anyone. Please read that again because the importance of that concept cannot be overstated. **You will never use the carrier assigned phone number of that phone for anything.**

Literally the only purpose for which we could consider using the carrier assigned phone number is to pay the bill each month. If you pay in person or over the phone, the customer service representative will need to know that number to look up the pre-paid account in order to apply your payment. Aside from that scenario, the phone number to our phone remains unknown to anyone.

Many people frequently ask why we are so concerned with protecting our phone number. What we are really concerned with is avoiding correlating

this number with our true identities. Once entities capture the fact that 555-555-5555 belongs to Rachel Smith, Rachel's phone is no longer private. Her IMEI can now be correlated with that number to track her on the cellular network. The MAC address on her device is now known, and she can be tracked on Wi-Fi and Bluetooth networks. Rachel's historical data will also be retrieved and correlated with her, too, completely un-doing all of her hard work. One slip-up and all of the convenience that Rachel has sacrificed has been for nothing – her phone is now 100% correlated to her.

How would your name be associated with your private phone number? There are various ways. If you pay your phone bill with a credit card, that information is shared with the credit card issuer, the third-party processing that transaction, and the cellular service provider. If you share your phone number with a friend, he or she probably stores that information in contacts. This information is scooped up by any application that the friend allows to access "Contacts" and it is now associated with your name. If you give this number out to any merchant or service provider in conjunction with your name it will almost certainly be sold to a data aggregator.

If your carrier-assigned phone number is never used to validate online accounts that you set up, it cannot be tied to real information about you. That information cannot be released in the latest data breach and later reveal other details about your life. It has been said time and time again that our phone numbers are the digital equivalent to a social security number. When used in the traditional manner, phone numbers are tied to a tremendous amount of personal information and services that we use. A compromise in any one of those areas of our life that reveals our actual phone number could compromise many other aspects of our life and allow an attacker access to valuable personal details that we aim to protect.

You have now paid full price for a new phone, obtained pre-paid service, and were assigned a phone number that you will never use for anything. All of this was done without sharing any personal information that ties your identity to that device or the service you obtained. Let's take a look at what we believe is a better, more private and secure way to communicate, starting with

INVESTIGADOR_Z

how to use the phone to make outbound calls and receive incoming calls. In the connected world we live in with an abundance of state-sponsored surveillance, wide-ranging account breaches, and crafty telemarketers with endless supplies of throwaway phone numbers, achieving even a semblance of privacy is a daily struggle. Surveys show as much: according to the Pew Research Center, 86 percent of internet users have taken steps to remove or mask their digital activity, but many say they'd like to do more.

SUDO

Sudo (<https://sudoapp.com/>) can help solve the problem of giving out a working phone number. Sudo is currently available for iOS phones (a version for Android devices is coming soon). It is an application that operates on the concept of "avatars". When you first load Sudo, you are prompted to create one of the nine "virtual identities" allowed with options such as name, phone number, email address, credit card number, and profile picture. They are digital, fictional profiles you can use for services, websites, and apps to which you'd rather not supply your personal information. The app does not ask for your phone number as a verification method, and you do not create a login username/password combination to use any of the features it provides.

Each of Sudo's phone numbers is a Voice-over-IP (VoIP) line that accepts both text messages and phone calls, including those sent from landlines, mobile phones, and select international sources. Email addresses have an inbox with support for receiving and archiving up to one gigabyte of mail. Your Sudos (profiles) are live as long as you want. You can delete one after a week or devote a longer-lived profile to activities like online shopping, social networking, or dating. They allow you to compartmentalize your digital life, and pre-plan for scenarios where you need to provide a working phone number, or email address to businesses or individuals.

Using Sudo to Full Capability: The following is an example of how nine Sudo numbers could be compartmentalized. Doubtlessly there are dozens of other uses for Sudo numbers, and you are limited only by your imagination.

- **Personal:** this number is given to family and friends who are trusted but choose to communicate using their carrier assigned cell number. Though we would prefer to use a more secure communication option (see Chapter 4), these individuals have not graduated to that level of security.
- **Work:** this number is given to anyone who knows us through our jobs. Most of our work contacts (and probably yours) do not use a more secure form of communications.
- **Personal Business:** This number/email is reserved for businesses that know our real names. Such businesses may include our insurance companies, veterinarians, and other services that require we provide true name information.
- **Financial:** this number is only used for our banks, investment accounts, and other financial institutions. We do not believe you should give this number out to any other service for any reason. Anyone who spoofs this number can call the bank and impersonate you.
- **Travel:** We each keep a Sudo that is used solely for travel. This allows you to have a phone number and email account that is separated out for true-name use with rental car agencies and airlines.
- **Dating** – This number can be used to give out to potential romantic partners, for dating sites and applications, and other activities in that space. This allows you a strong layer of privacy against sharing your real phone number and all of the disparate sources of information that it connects with untrusted strangers.
- **Commerce/Online Activity** – You can have a Sudo dedicated to buying and selling items through online classifieds like Craigslist. You could also use a Sudo for other ecommerce sites, video streaming services, etc. You may also choose to have a Sudo that is used for brick-and-mortar retailers' loyalty, coupon, and discount programs.
- **Disinformation/Alias:** Sudos provide an excellent tool for creating disinformation about oneself. A dedicated Sudo gives you an email address and a phone number that can be used to setup online accounts, store loyalty cards, etc.
- **Reserved:** It is a good idea to keep a Sudo (or two) set up but reserved for unforeseen circumstances. This allows you to quickly give out a

number if put on the spot and forced to provide a number quickly.

If you assign a name to your Sudo profile, it will appear on your screen when you receive an incoming call. This lets you know what Sudo is being called, and how you should answer the phone. Additionally, each Sudo can have its own ring tone and text/email notification tones, and each can be silenced so you are not inundated with texts and emails.

Choosing Sudo Numbers: Since Sudo allows you to use any area code you wish when creating your phone numbers, we recommend you choose these carefully. If you look at the list of Sudo uses above, you will likely realize that some of these make more sense if you use your local area code, or one close to it. For example, if you bank with local banks or have a local insurance agent, it may make sense to have a local telephone number. For some of these numbers it doesn't matter what area code you choose and it may make sense to choose something radically different. For example, our Financial Sudos telephone numbers have area codes from cities that are hundreds of miles away from us. This makes it very difficult for an attacker to guess the phone number we use with our banks, and works because we do not use local banks. In the event the bank should spill our phone numbers, this makes it unlikely that an attacker would guess which numbers ours are.

Sudo allows you to digitally distance yourself from seedy merchants, home service providers like landscapers, babysitters, contractors, and real-estate agents, or even annoying strangers to whom you do not want to provide real information. You can organize the profiles into identities that you use to protect your real personal information. You no longer have to leave your real carrier assigned phone number or email address with untrusted people. It provides an additional layer of disinformation which you can control in any given scenario. Once the profiles are set up (which only takes a few minutes) you are ready to use them as you go about your life.

Problems with Sudo: Sudo is not a perfect product, and there are a couple of problems with it. The first is that Sudo does not support short-code SMS. This is the messaging protocol that is used by many services to send verification text messages. This means that you will not be able to get a text

message when setting up certain services. In some cases, you can work around this by choosing to accept a phone call instead, but not in all cases.

The second problem with Sudo is that your text messages and calls are plain-text. Sudo does encrypt emails that are sent between two Sudo accounts but calls and texts on Sudo offer no special protection. Finally, you may have some issues in receiving incoming calls to Sudo numbers because you have to unlock your device to answer them.

Finally, as with all mobile applications, Sudo is not perfect. It will not work if you do not have a data connection. The app will occasionally crash and calls are occasionally dropped. If you are using a VPN (a practice we strongly recommend) you may experience more dropped calls than normal when using cellular data. Sudo does come with a bit of frustration, and we would be dishonest if we did not acknowledge this. Overall, however, the product is a boon to privacy and we both use it daily.

Sudo Background: It should be noted that Sudo raises some privacy concerns because all emails, messages, and calls are routed through its parent company's (Anonyme Labs) dedicated servers. Sudo retains “zero knowledge” about the users, and employees couldn't pull up personal details even if they wanted to. The system is secured end-to-end — when you download the application for the first time, the encryption key stays on your device. Sudo was developed by Steve Shillingford, an entrepreneur and cyber-security expert. His blog (<https://medium.com/control-shift>) provides background information on his company and the reasons why he developed the app as a solution to growing privacy concerns. “We don't store anything that isn't encrypted,” Shillingford said. “Everything [Anonyme's servers] get[s] is encrypted gibberish.”

Sudo remains a privately funded project, but the company is considering different ways to monetize by offering premium services. In the future, it might charge a small in-app fee for additional Sudos, levee a larger fee for porting a number into Sudo, or give users the option to pay for larger inboxes. Custom-domain email addresses and phone number customization are other potential revenue generator. In the future you might be able to buy a

number by ZIP code or secure a premium 1-800 number. But Shillingford stressed that it won't stick any of Sudo's free features behind a paywall. "Privacy is important," he said. "[And] people should be able to control how much they have and how much they give away. We want to give people flexibility and freedom."

Sudo is an excellent and reliable tool that we encourage you to explore. We both use Sudo extensively and have found it is the best way to have several different phone numbers on your new private phone. It allows you to compartmentalize who and what entities get certain phone numbers from you and allows you to never give out your actual carrier assigned phone number to anyone. Since Sudo can use either Wi-Fi or cellular data, you have immense flexibility and are no longer stuck being tied to the cellular network.

All profiles except our Personal and Work Sudos are typically in silent mode so that we are not bothered with unwanted calls. The Work profile is also silenced when we do not want to be notified of calls or texts that are going to that number (days off). We do not like being included in group text messages. These text groups tend to inundate everyone with unwanted chatter, and we love the ability to silence these messages.

Sudo numbers are primarily used when we need to provide a phone number to someone and we do not want to give out our carrier assigned phone number. In the coming chapters we will explore dedicated encrypted calling applications and how they are used to further enhance the privacy and security of our communications.

The following is an example of the dangers of sharing your carrier assigned phone number with people and how an open source analyst or someone with bad intentions could use that valuable piece of information as an attach surface. Consider the following real-world example.

During a recent trip out of town, I met with a real estate broker to inquire about home prices in the area and also get a contact for a local attorney who may be able to help with purchasing property in a non-traditional, private manner. The broker I met worked for a well-known firm, one that caters to high end clients worldwide. For the purpose of this article, her name was “Megan”, and she proved to be very knowledgeable about the area I visited and her business in general.

During my conversations with Megan she shared some general details about her life, her history with her company, and some specific knowledge she had learned while living in the area. There was nothing unusual about her rapport building with a potential new client; she highlighted some areas of interest that we had in common and shared just enough about herself to keep the conversation professional while still making the interaction unique and genuine. Of course, as a student of social engineering I paid close attention to the details she chose to share. And as an OSINT investigator, I found the last part of our interaction quite interesting. She thanked me for stopping in and handed me her business card. Printed on the card was a cell phone number. I recognized the area code for that number as belonging to a state where she told me she had moved from prior to being hired at this real estate agency.

To be clear, she had not hand-written the cell phone number on her business card as if to only give it me. It was her official business card, and the only number printed on the card was a cell phone. Due to the area code, I guessed that it may be her actual personal cell number, probably one she had used for many years. This may be standard for some real estate brokers to do actually, so there’s nothing too unusual here. Until of course, that number falls into the hands of someone with a little knowledge about what a critical piece of information a cell phone number may be.

When I do privacy and security training, I always highlight the fact that a person's cell phone number is often the digital equivalent to a fingerprint. Most people only have one cell phone number and that number is likely tied to their real name, real address, and many other online and offline accounts that are also in their real name. For many people, the phone number they have on file with their bank is also the same number that is tied to their social media accounts, other online accounts, their utilities, their emergency contact number, or the phone number on their business card that is handed to strangers on a daily basis.

A recent New York Times [article](#) described a cell phone number as “A 10 Digit Key Code To Your Private Life”. It describes the many ways that a cell phone number can be the gateway to all sorts of other information about your life. As an investigator (or identity thief), if I had the choice of knowing either your Social Security Number or your personal cell phone number...I would always choose the cell phone number. Someone with the goal of obtaining information about you can compile a staggering amount of information based on that number alone. That personal information can be used to locate you and do a lot of damage. Plus, the information you give up by sharing your cell phone number is just down right creepy when you know that strangers have access to it.

I only spent about 10 minutes researching Megan's cell phone number just to confirm my suspicion that it was in fact linked to real information. I conducted a reverse-search of the number at <https://www.truepeoplesearch.com/> and immediately saw that it was her personal number. The information returned with her complete current address and 20 years of previous addresses and phone numbers. It listed the names of her family members and their addresses and phone numbers. Within a few seconds I had all of this information including personal email addresses, work history, information about her neighbors, and links to her social media accounts. This was all from just one online database.

Google searches revealed even more; other online accounts, street maps, and seven years' worth of personal photographs on her Instagram and

Facebook profiles, many of which were tagged with date/time/location information. During my conversation with Megan she mentioned that she owned a red Jeep, had a dog, and she showed me a video of local scenery that she had recently taken on her phone. She said the video was taken from her “bedroom window” within the past few days. The home address I researched on her (based on her phone number) combined with the street view of the area with a red Jeep in the driveway, confirmed which window she took the video from....and that same video had been posted to her social media account for reference (analysis) along with photos of her dog (good boy). My 10-minute exercise into her life quickly took me across several different online databases, connecting the dots and data points, and would have easily filled 30 pages of information and photos about her personal life. If I had spent another 10 minutes, or 10 days...imagine the amount of information that could be learned. Scary.

It should be noted that Megan did not own the property where she lived, and likely did not have utilities in her name. There was no public record of her being at her current address because she was a renter. Her current address *was* linked to her cell phone number across many databases though, which is one reason why that information was so easily found. Many renters falsely assume that their address is “hidden” because they are not a property owner. If their address is known to their cell phone provider or exists in other databases though, it is likely found online somewhere as a result.

Including a cell phone number on a business card is pretty common. Have a separate business number for that purpose, and don’t share your personal number. I know people who work in professions where their threat level is much higher than that of a real estate agent, who include their personal cell phone number on their business cards or in their email signatures. This is a terrible OPSEC if you are in a high-risk profession like law enforcement, or if you value your privacy and want to better protect your personal information. Remember, a cell phone number can be the digital equivalent to a fingerprint...the gateway to volumes of personal information about you.

Compartmentalize which companies and which individuals have your information. If you only have one cell phone number, then your options are severely limited when someone asks you for this critical piece of information. Have multiple options available. Utilize apps like Sudo (<https://sudoapp.com/>), which give you multiple phone numbers for use in your privacy strategy. I hope this information encourages you to think carefully about how and with whom you share your cell phone number, and also how you can change your approach to better protect your personal information.

GETTING RID OF OLD/UNUSED PHONES

Now that you have set up your new phone, what should you do with your old phone? We believe the best solution is to simply destroy it so that no data can be recovered from it. You could also sell it to a third party, donate it charity, or keep around as a reminder of how simple life was before you adopted a more private way of communicating. We choose to separate ourselves from the old equipment by either selling it to someone else who will likely activate it and create a whole new data trail in a different direction or destroy it and move on.

If you choose to rid yourself of an old/unused phone, ensure that you delete all information from the device. Even if you plan to physically destroy the device, we still recommend securely erasing all data from it. We recommend wiping the entire encrypted drive and re-encrypting it. Most modern smartphones have an ability to wipe all data on the device and reset it to factory defaults. If the device is encrypted, this will actually wipe the device's encryption header keys and restore factory defaults.

SUMMARY

Purchasing your phone anonymously has some major privacy benefits. Doing so and maintaining your privacy requires:

- Purchasing your phone outright, with cash, for full the purchase price,
- using a pre-paid cellular service plan,
- paying for your service plan in a way that does not link directly to you, and
- never giving out or using your real phone number to any person for any reason.

The Sudo application allows you to perform all of the normal functions of a smartphone, as well as giving you a raft of other functions. Some of the capabilities of Sudo are:

- The ability to receive incoming and place outgoing calls, texts, and emails,
- creation of nine separate profiles, each with its own email address and phone number,
- separate ring- and text tones for all of your identities, and
- the ability to conduct all of your normal communications on your cellular service provider's data plan or over Wi-Fi.

CHAPTER 3: SECURE YOUR SMARTPHONE APPLICATION OPERATING SYSTEM (APOS)

In addition to solving the problems of the “phone” half of the smartphone, we also have to solve the problems posed by the computer portion by locking down the Application OS’s settings. These are somewhat easier to fix than the baseband vulnerabilities. The Android and iOS operating systems are incredibly secure relative to Windows, MacOS, and yes, even many Linux distributions. Some basic best practices will keep these devices extremely secure. Because of the ever-changing nature of the mobile device landscape, we have attempted to provide principles rather than specifics. Though we both use iOS devices exclusively, the principles laid out in this chapter should apply to all operating systems.

This first chapter of best practices may seem boring, but it truly contains the most important advice in this book. Keeping your system up-to-date and free of superfluous software makes it much more resilient to malicious software. Malware is not the annoying nagware about which we were concerned years go. Modern, sophisticated malware is designed to install itself and to do everything possible to remain undetected. Once executed, malware can be used to systematically destroy your defenses by gaining a foothold inside your secure communication platform and allowing the attacker an inroad.

In fact, we occasionally see a shocking headline that some organization or hacker has broken this or that encrypted messaging protocol. While this may be possible in some situations, what we much more commonly find is that the app has not been broken at all. Rather, spies or hackers have found a way to gain direct access to the device’s microphone or keyboard. If the content of your communications can be accessed directly from the source there is no need to break the encryption on secure messaging applications. Regardless of

the other measures you have put into place, you no longer have even a hope of privacy or security if your device is infected with malware. Without further ado, let's begin.

OPERATING SYSTEM UPDATES

The first and most important step you should take is to keep your operating system up-to-date. Unpatched operating systems have security vulnerabilities that have been publicly acknowledged. The risk posed by running n-day [\[5\]](#) vulnerabilities rather than 0-day vulnerabilities is much higher. You should download and install OS updates at your earliest possible opportunity.

iOS Devices: iOS devices will usually display a badge (the red circle in the upper-right corner on each app icon) on the Settings app when updates are available. Sometimes this does not occur so it is not a bad idea to check manually occasionally. To do so, open the device Settings, General, Software Update. On the Software Update screen pull down and release to check for an update.

///// THE PROBLEM WITH ANDROID UPDATES /////

On older Android devices your software may be months out of date, but your phone will still insist that you have the latest version and no updates are available. This is because hardware manufacturers have little incentive to rush to write updates for older models. Let's use Samsung as an example.

Samsung creates many versions of its operating system to run on the dozens of phones it produces. It further customizes each one of these operating systems for the various carriers it partners with. When Google pushes an update to Android, Samsung immediately modifies it and makes it available to its top-tier (read: most recent and most expensive) devices. If Samsung wanted to update every Samsung device in existence, it would have to write hundreds of slightly different versions of the OS.

This means that older phones that are still supported get updates much later

than newer, flagship models. To limit the amount of work they have to do, Samsung eventually just stops writing updates to accommodate older devices. If your phone is more than two years old, it is very likely that the hardware manufacturer no longer supports it. One exception is Google's own phones: The Nexus, Pixel, et. al, which are supported for three years from release. **If you are an Android user, we strongly recommend you upgrade your phone at least every two years. Otherwise you risk running an unsupported, outdated operating system.**

Android Devices: Open the device's settings. Scroll to the bottom of the menu and tap About Phone, About Device, or System. This will open a new screen of menus; look for System Updates or Software Updates. If updates are available, download and install them. Be warned that some models of Android manufacturers have been caught misleading users. These phones display messages that indicate they are fully updated when updates for the device have not even been written.

APPLICATION MANAGEMENT

Applications are both boon and bane to smartphone users. They enable us to protect our online accounts with password managers two-factor authentication. They allow us to use virtual private networks and to encrypt texts, calls, and emails. However, they also introduce a great deal of vulnerability. Because of the access they have to our devices, apps can gather a ton of information about us. Managing your applications required a multi-faceted approach. The techniques below are grouped into a "good, better, best" methodology. This does not mean you should skip the "good" techniques; they are still imperative. It simply means that if you wish to go above and beyond, we have provided a pathway for that.

Good - Application Updates: Like your operating system, your applications should stay updated. And, like your OS, running outdated versions of apps means that you have unpatched n-day vulnerabilities on your mobile device.

- **iOS Devices:** The App Store icon will display a badge when updates to installed applications are available. You can also instruct your device to download and install updates automatically. We recommend this unless you have a compelling reason for not doing so. Open Settings, navigate to iTunes and App Store, and look for a section called Automatic Downloads. Ensure that Updates is toggle ON.
- **Android Devices:** Open the Play Store and tap the overflow button (the three stacked dots on the top of the screen). When the drop-down menu opens, tap My Apps and Games to open a list of installed apps. If updates are available tap the Update All button and allow your applications to update.

Good - App Permissions: Both the Android and iOS APOSs allow you to control your app's permissions individually. You can control the ability of your apps to access your location, camera, microphone, contacts, calendar, and more. It is important to go through each one of these settings for each application on your device. Remember that restricting app permissions is not a guarantee of privacy or security. Though Apple (and to some extent Android) goes to great lengths to enforce app permissions, this is still a software solution to hardware problem.

While keeping your applications up-to-date and restricting their permissions is extremely important, we feel this is secondary to limiting the applications that you install onto your device. Every single app that you install is granted persistent access to a great deal of sensitive information. Many of these applications are allowed to access your contacts, your camera and microphone, and location information. Even if you restrict these permissions, these applications can certainly see your SIM card phone number, your MAC address, and the Wi-Fi hotspots to which you are connected. This information may be used to positively identify you, as well as the locations you frequent based on the Wi-Fi networks to which you connect. In addition to keeping applications updated, we have two further techniques that you should consider.

Better - App Audit: After updating all of your applications and restricting

their permissions, you should conduct an application audit. You should go through every single app on your phone and consider the last time you used it. If it has been more than a week since you've opened it, it is very likely that you don't need it. Look at each app critically. Is there a default app on your device that will perform a similar function in a satisfactory manner? If so, consider getting rid of the app in question. Some people are hesitant to do this, but keep in mind that if you need the application later you can always reinstall it.

Before you delete an application, you should consider what information it contains. First, you should record any account data like usernames and email addresses (if any). Next, you should remove any personal information, especially sensitive information like credit card numbers and phone numbers. If it is possible to delete history about your usage of the app, do so. After you have removed all data that is possible to remove, delete the application from your device.

There may be apps that you use only on rare occasions but for which you do have a recurring need. If this is the case, consider installing that application each time you need it. Perform its function, and then delete it from your device. This allows you to use the app when needed without providing it an extraordinary amount of access into your daily life.

Better – Remove Bloatware: Both iOS and Android devices come with a number of applications pre-installed. This number of apps seems to climb each year, and many of these apps are unused by the majority of mobile users. Where possible, we recommend removing these applications and their attendant data collection capabilities.

iOS: On iOS devices you can “remove” a large number (but not all) of the OEM apps. Most apps that can be deleted are actually removed from the device rather than simply hidden. We recommend removing every application that you are not going to actually use.

Android: If you have an Android device you may not have such flexibility. If you follow our recommendation in the next chapter and

purchase a phone outright, we recommend purchasing directly through a hardware retailer rather than from a wireless carrier. Many manufacturers partner with cell carriers who install a huge number of bloatware programs on devices, for which they all receive subsidies. While this may help you get a slightly less expensive phone, it creates the potential for major privacy violations since most of these apps cannot be removed. If you purchase your Android device for full purchase price directly from the manufacturer you are much more likely to get a phone without dozens of bloatware applications. If there are applications on your Android device that you cannot delete, we still recommend you disable them. This will perhaps limit some of their data collection capability and security risk.

Best - App Vetting: We hope that after having read this chapter you will be hesitant to install applications in the future. Your best bet with all apps is to vet them thoroughly before installing them on your device. This seems like a surprising concept to many people who think nothing of downloading a free app. Conversely, we may seem surprising to them when we insist on taking the following measures before downloading an application. These are the minimum steps you should take.

1. **Download from Trusted Sources:** If you use an iOS device, this is not a decision you can make - the only source for apps is the App Store. If you are an Android owner, you have many more options for downloading apps. There is the Google Play store, the F-Droid repository, and you can side-load APKs from various sources. We recommend that you stick with the Google Play store. Though this isn't perfect (a lot of malware gets through) it is not quite the Wild West that other sources for applications are.
2. **Privacy Policies:** Read the application's privacy policy and understand what data is being shared. Most privacy policies are lengthy, but you should pay special attention to certain sections. You should look carefully at how your data is collected, how it is shared, and with whom it is shared. The most important of these is what data is collected. Even if the current owner of the app has no intention of sharing your data, the app may be

sold at some point in the future, along with all the information it has collected. Also, don't buy into vague language such as, "we collect some data to improve our services..." You should demand to know exactly what this data is before you give the application access to your device.

3. **Contact the Developer:** If you have read the privacy policy and still have unanswered questions (or if you can't find the privacy policy), don't be afraid to reach out directly to the developer. We have contacted numerous app developers, most of whom were happy to answer our questions.

Why? You may be wondering why we are so rigid about keeping the apps on your mobile device to a minimum. First, every single application on your device represents additional attack surface. Each application has discovered or undiscovered vulnerabilities. Each has access to certain permissions on the device. However, these permissions and vulnerabilities don't matter if you never install the application on your device. There is also a privacy aspect to our concern. In a 2015 study entitled *Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps*, researchers revealed some shocking statistics:

- 73% of Android apps and 47% of iOS apps share personally identifiable information with third-parties like Google Analytics, Facebook, and Crashlytics,
- 47% of iOS apps and 33% of Android apps shared geolocation data including GPS coordinates,
- The average Android app shares personal data with 3.1 third-parties and the average iOS app shares personal data with 2.7 third-parties

To read the full study visit <https://techscience.org/a/2015103001/>

DEVICE ENCRYPTION

Your mobile device should be encrypted. Full disk encryption protects the data that is stored on the device when it is out of your physical control. This means that a thief could not simply pick up the device and access the data on

the device. If the encryption (and passcode) is good it also means that government and law enforcement agencies will have to spend serious resources to access this data. Because you carry your mobile device literally everywhere, its likelihood of being lost or stolen is significantly high.

iOS Devices: If you are running iOS device it is encrypted by default by the manufacturer. This encryption is non-user configurable, meaning you cannot accidentally turn it off. All you have to do is apply a strong passcode to the device. We also recommend that you enable the “Erase Data” setting. This causes the phone to erase all the data it contains after 10 incorrect passcode attempts.

Android Devices: If you are running a recent-model, flagship Android phone from a major manufacturer, your phone is *probably* encrypted by default. Google still struggles to get Android manufacturers to encrypt all devices by default. The current mandate from Google is that Android phones meeting certain performance benchmarks must be encrypted by default. This leaves a huge majority of users unprotected. The good news is that you can still encrypt your phone, but at the penalty of some performance degradation.

To encrypt your Android device, first ensure your battery is charged to at least 80% and the device is plugged in. Next, open the Settings menu and find “Encrypt Phone”. If you are running a newer device and this setting is missing, it likely means your device is encrypted already. You will be prompted to enter a passcode or passphrase, and then met with several warnings. Click through these and your phone will begin encrypting. Do not use the phone until the encryption process is complete. It may take as long as an hour.

PRIVACY SETTINGS

The next major focus area is managing the privacy settings of each application. You should give your applications reasonable access to the settings they need to perform their desired task, but nothing more. All of these settings are merely software settings and rely on the APOS for

enforcement. They are not a replacement for best practices or physical security measures.

iOS: There are two ways to access these settings on an iOS device. The first is to open Settings and navigate to privacy. This will give you a list of all the privacy settings available. Opening any of these will display a list of apps that have accessed or attempted to access the particular setting's data. We recommend you begin here. The second way to access these settings is by opening Settings and scrolling all the way to the bottom of the page. This will display a list of all your applications. Tapping each will open the list of permissions the app has requested. We recommend you check your app permissions here after you have done a thorough scrub through the technique described above.

- **Location Services:** We like to protect our location information for obvious reasons. This is to protect us from both near-real-time (NRT) and historical location tracking.
- **Camera:** This should be limited only to the applications that truly need access to the camera to perform their intended function. You may wish to enable this for applications through which you send photographs natively, like Wire or Signal (see Chapter ____). Some applications will require this access for less obvious reasons. Various two-factor authentication apps require access to the camera to scan a QC code to generate the correct token for the account. We still believe you have some element of control here. You probably don't add a new account on a daily or even monthly basis. This means that you could allow camera access **ONLY** when adding a new account, and keep it disabled the rest of the time. Remember, even though an application may have the best privacy policy in the world and be extremely trusted, it may still be infected with malware.
- **Microphone:** From an intelligence collection standpoint, access to your microphone is arguably much better than access to a camera. If your microphone is compromised your device will be a listening device that captures everything that happens within earshot. We recommend an

extremely judicious eye when considering this setting.

- **Contacts:** This may not seem incredibly important to you. However, an article released during the writing of this book revealed details about Facebook's use of this permission. If users allowed Facebook to record their contacts, it also gave the company the ability to collect all call and messaging metadata. Some users discovered this when they requested their information from Facebook and it is almost a certainty that other applications are doing the same thing. Not only is this information stored on a remote server with a company that does not respect your privacy, it also puts this information at risk in transit.
- **Photos:** Settings allowed to access your device's camera roll can peruse all your historical photographs and transmit them off the device. Use extreme care in selecting which apps can access this information. Your camera roll very likely contains not only pictures of you, but also pictures of your friends and loved ones and we believe protecting their likeness is just as important as protecting our own. This is out of a sense of privacy and respect, but also a sense of self-preservation. If an app is able to see likenesses of all our friends and family, it can probably leverage Facebook to find out why they are. This would go a long way toward piercing our own privacy.
- **Other Settings:** There are various other settings in both iOS and Android that should be carefully controlled. These include your calendar, reminders, Health, Homekit, access to device storage, and others. At this point it is probably safe to assume that most readers understand the risks of sharing this information, and we will not cover each one in detail.

RESTRICTIONS (iOS ONLY)

The iOS operating system offers the ability to set Restrictions. This is a greatly underutilized setting for privacy and security enthusiasts. Restrictions

is intended to give parents the ability to lock down mobile devices that are primarily utilized by their children. To use restrictions requires that you set a four-digit passcode. Once the passcode is set you can prevent anyone without the passcode from changing certain settings, including Camera, Safari, Siri, AirDrop, and CarPlay. Installing and Deleting Apps, and In-App Purchases. Restrictions also allows you to specify which privacy settings can be modified once set, including Location Services, Contacts, Calendar, Photos, Share My Location, Microphone, and many more. Finally, Restrictions lets you disallow changes for Accounts, Cellular Data, Background App Refresh, and more.

We believe this is one of the most important settings in an iOS device. Locking down Restrictions ensures that if you OS is updated, key privacy settings won't be changed or disabled. Of course, this means that every time you install a new app that needs access to your microphone you have to unlock Restrictions, make the change, then go re-enable the restriction. Because we use so few apps and change permissions so infrequently, we do not believe this to be too great of an inconvenience.

SUMMARY

Locking down the APOS is not all that difficult but it requires some discipline and attention. The most important settings are:

- Ensuring the operating system is up-to-date,
- Keeping all applications up-to-date,
- Tightly controlling application permissions, and controlling them in the longer-term using Restrictions (in iOS),
- Removing any unused or superfluous applications and any bloatware, and

- Thoroughly vetting applications before installing them.

CHAPTER 4: SECURE YOUR COMMUNICATIONS

VIRTUAL PRIVATE NETWORKS

In the constant search for redundant, overlapping layers of encryption, a Virtual Private Network (VPN) is a critical component of a secure communication system. Virtual private networks provide two things: security, and privacy. We will address each and explain the basics of what a VPN is and how it works.

VPN Basics: A virtual private network allows you to shift trust from your Internet Service Provider (ISP) or CSP to a third-party. Under typical conditions, the packets that are sent between your computer and the sites you visit may be partially encrypted through the HTTPS protocol. This only protects the packet contents but does not prevent these parties from seeing the sites you visit. This also makes you more vulnerable to attacks that can undermine your HTTPS connection by serving your browser a self-signed certificate. This would make the content of each packet visible to the attacker, not merely the header information.

Subscribing to a VPN service allows you to connect to a remote VPN server before you begin passing traffic. Your traffic is then encrypted between your device and the VPN server to which you are connected. This means that you are making your packets cryptographically inaccessible to hackers on the local network, owners of hardware to which you connect, and your ISP/CSP. These parties will only see that the traffic originated at your device and terminated at the VPN server, and vice-versa. This is how a VPN provides security.

On the other side of the transaction are the websites and services that you

visit. Under typical conditions (that is, not using a VPN) these sites are able to see your Internet Protocol (IP) address. Your IP address is assigned by your ISP and is unique to your home's internet connection. This allows these sites to track you over time by your IP address. When using a VPN, this traffic appears to originate from the VPN server. This gives you two privacy advantages. First, if you connect to the VPN server before every single session, you will give the sites you visit a huge range of IP addresses rather than a single, trackable IP. Secondly, because your IP address is correlated to a geographic location, you deprive the sites you visit from knowing your exact location. This is the privacy afforded by a VPN.

For the purposes of this book we will focus primarily on the security that using an VPN offers. Adding additional layers of security on top of your encrypted messaging gives you a solid defense-in-depth. For example, if you are connected to a Wi-Fi hotspot or cellular tower, the VPN prevents these parties from seeing that you are using a secure communication application. The HTTPS connection protects these packets from the VPN itself, and once they exit the VPN's server. The individually encrypted messages protect your content from all of the above, and from exploitation by the encrypted messenger's own servers.

It is probably safe to assume that all of these three protocols (the VPN, HTTPS connection, and individual message encryption) all have as-of-yet undiscovered vulnerabilities. By using a layered approach, we maximize our chances of successfully communicating securely. We also minimize the chances that an attacker, armed with an exploit for one of these protocols, will be able to get all the way down to the content of the message that we are ultimately attempting to secure.

The other reason you need the protection of a VPN on your mobile device is the data that it constantly transmits. Your mobile device is potentially connected to dozens or scores of servers at any time. These connections are constant and share a great deal of data about you and your device. Much of this data is protected by HTTPS, but far from all of it is. You should take it upon yourself to protect as much of this data as possible by using a VPN at all times - not just when conducting some sensitive activity.

Selecting a VPN: When you select a VPN, you are paying a subscription service to be able to access the provider's servers and bandwidth. Your VPN provider sees both sides of your internet usage. The service will see both your IP address, all of the sites that you visit, and at least some of your activity on many of these sites. This is an extraordinary level of access to give to a third-party and necessitates choosing your VPN provider very carefully.

Though it may seem counterintuitive, many VPN providers abuse their customers. There have been VPN and proxy providers that have sold customers' unused bandwidth to malicious hackers. On a somewhat more benign level, some providers simply don't provide the security they claim to. A VPN called Onavo is owned by Facebook and even though it encrypts your traffic, it allows all of it to be inspected and collected by Facebook. Many so-called VPNs don't encrypt any traffic at all, completely robbing you of any security benefit. Most "free" VPN services are abusing you by collecting your data for monetization, or in some other way. It is imperative that you choose your VPN provider carefully!

The first set of criteria to which you should pay the most careful attention are the security factors. These factors are as follows:

Encryption Protocols: The strength of your VPN against attackers is directly related to the strength of the encryption algorithms used to protect it. This is one of the first things you should consider. There are two specific factors that you should investigate:

- **Handshake Protocol:** This is the strength of the keys that are exchanged to establish your secure connection to the VPN. The handshake protocol strength should be **RSA-4096**. Weaker keys (RSA-2048) are often used; we recommend always using RSA-4096.
- **Encryption Strength:** This is the level to which your browsing traffic will be encrypted. The encryption strength should be **AES-256**. Some VPNs only offer up to AES-128, and some VPNs may offer AES-256

but enable 128 by default.

- **Implementation:** There are several VPN protocols that are used to route your traffic. The only two you are likely to encounter currently are some variation of the IPSec and OpenVPN protocols. OpenVPN is the strongest protocol currently available and should always be your preferred protocol. IPSec (Internet Protocol Security) has some weaknesses and should not be inherently trusted against state actors. There are some situations in which we may to rely on IPSec if you use an iOS device. These situations will be discussed on Page ____.

Logging: The next thing you should want to know about your virtual private network is what logs about your usage (if any) are kept. Since VPN providers have full access to your traffic they also have the ability to log a high amount of information. This may include the true IP addresses from which you access the service, the amount of bandwidth you use, and the times you connect and disconnect from the service. Some VPNs may even log your DNS requests which would reveal the sites you browse to, or your actual traffic. Logging is extremely problematic because it creates a massive single point-of-failure. If the VPN is subpoenaed, hacked, or sold, all of your browsing data would then be no safer than it was in the hands of the ISP/CSP.

An excellent resource for vetting virtual private networks is That One Privacy Site. The site is run by the aptly named That One Privacy Guy, who accepts no affiliates or other incentives from any VPN providers. TOPG's methodology is extremely transparent. Currently he reviews over 180 VPN services, and his spreadsheet covers over 50 different criteria, broken in the following categories: Jurisdiction, Logging, Activism, Server Configuration, Security, Availability, Website (whether or not it serves cookies and third-party trackers), Pricing, and Ethics. That One Privacy Guy's unrivaled spreadsheet is available at: <https://thatoneprivacysite.net/vpn-comparison-chart/>

GENERAL-USE VPN RECOMMENDATIONS

We recommend and stand behind the following virtual private network services. These are not the only worthwhile VPNs but we have personally used these and speak from experience. The first two VPNs we will cover (Private Internet Access and Mullvad VPN) are somewhat general-use in nature. One features a native client for almost every imaginable platform; the other runs (almost) strictly through OpenVPN. Both of these are outstanding VPNs for general use and will perform just as well on your mobile device as your desktop computer. We like this because it does not necessitate the need for a special VPN just for your mobile device. The second pair of VPN recommendations are those we feel confident recommending for dedicated iOS use because of the performance of their native clients. The reason behind this will be addressed at the beginning of that section.

Private Internet Access: This is our default VPN recommendation for users at every skill level. Private Internet Access (PIA) offers native applications for Windows, Mac, Linux, Android, and iOS. It also offers the ability to download OpenVPN config files. Users are permitted to use either TCP or UDP network protocols, and use small packets, making this usable on slow networks or networks that attempt to prohibit VPN traffic.

Users can choose their level of encryption on all platforms except iOS. The default security levels are AES-128 (data encryption), RSA-4096 (handshake protocol), and SHA-1 (data authentication protocol). These defaults are defaulted to these settings to balance security and network performance. However, they can and should be changed to AES-256, RSA-4096, and SHA-256, respectively. The OpenVPN protocol is used by default in all instances of PIA except on iOS.

Private Internet Access offers access to over 3,000 servers in 28 countries (over 1,500 of these are in the United States). The cost for PIA is a very reasonable \$39.95/year. This averages out to just \$3.30/month. You are allowed to connect five devices simultaneously with your PIA credentials, and there are no bandwidth limitations. Payment can be done anonymously through Bitcoin or by redeeming prepaid gift cards from a number of mainstream retailers.

For more information and to sign up with PIA visit <https://www.privateinternetaccess.com/>

Mullvad VPN: This is the most private VPN we have encountered and Mullvad receives extremely high praise from every VPN review we have seen, including That One Privacy Guy. With around 60 servers worldwide Mullvad is not the biggest VPN service but they take privacy extremely seriously.

Mullvad allows you setup and fund an account completely anonymously. Though many of our readers will not need this level of anonymity for setting up their VPN, some will and it is nice to have the option. When creating a Mullvad account, zero information is required for signup. One simply solves a CAPTCHA and is given an account number. This account comes with three hours of service, after which it will need to be funded.

Mullvad allows you to pay through a number of methods including credit card, PayPal, Bitcoin, and bank wire. Our favorite, however, is with cash. Simply put any amount of any currency into an envelope, along with your account number. Mail the envelope to Mullvad (address available on their website). Within fourteen days the appropriate amount of time will be added to your account. We have never before encountered a VPN company that allows you to pay for your service with cash and we greatly appreciate this.

We do have one complaint about Mullvad VPN, in regards to their native applications. In a word, they are terrible. In all of our trials with Mullvad's native applications they have leaked some information like DNS requests, or in one case, IPv4 addresses. This is unacceptable, and Mullvad should ONLY be used through OpenVPN or an OpenVPN application like Tunnelblick for Mac, OpenVPN Connect for iOS, or OpenVPN which is native to Linux.

For more information and to sign up with Mullvad VPN visit <https://mullvad.net/en/>

IOS-SPECIFIC VPN RECOMMENDATIONS

iOS/VPN Weirdness: If you use an iOS device, you will be forced to make some decisions regarding your virtual private network(s). iOS devices do not have a native ability to run the OpenVPN protocol and require a third-party app to do so^[6]. Unfortunately, this application does a poor job of staying connected when the device is idle. Also, once the connection with the server is broken, the app will sometimes not automatically re-establish a connection. This means that if you rely solely on OpenVPN through this application, there is a significant opportunity for unencrypted data to be transmitted from your device.

Even when your device is idle (screen is dark and locked) a flurry of activity is happening in the background. Apps are making connections with their respective servers, event logs are being transmitted, and other your geolocation is being updated to keep your maps, weather, and other applications apprised of your location. Unfortunately this risks passing a great deal of personally identifiable information in plain text, and all of this information is correlated with your true IP address and potentially your device's MAC address, correlating it permanently to your device.

The other alternative is to use a VPN with a native application, but a weaker encryption protocol. Many good VPN providers offer apps for iOS, but they are all limited to the IPSec protocol or a variant thereof (like IKEv2/IPSec). This creates something of a conundrum for the privacy enthusiast - use a VPN that doesn't protect you at all much of the time, or a VPN that is always on but that offers a lower level of security?

Each reader will have to answer this question for him or herself and consider his or her own threat model realistically. If you are attempting to opt-out of mass surveillance by commercial actors like ISPs and CSPs, and relatively unsophisticated hackers, an IPSec VPN will be sufficient for your needs. If you are concerned with taking your privacy to the maximum possible extent, or if government actors are your biggest realistic threat, a more complicated approach is appropriate for your situation.

There are a couple of strategies you could implement if you are in an extremely high-threat situation. The first is to limit network connectivity

except when you are actually communicating. This necessitates keeping your device in a Faraday bag except when being used (see Chapter 5) but makes it easy to toggle the OpenVPN on as soon as the device is removed from the bag. The second strategy would be to run both a native iOS app-based VPN, and OpenVPN connect. You could rely on the IPSec VPN to protect your background traffic, and switch to OpenVPN before initiating a communication session. This requires a great deal of discipline to carry out in practice, but it may be worth it to you. You can even set this up without purchasing two VPNs. Most VPNs that offer an iOS application also offer OpenVPN configuration files that can be imported into the OpenVPN application.

IKEv2 Protocol: Both of the VPNs listed below are recommended for iOS and both utilize the IPSec/IKEv2 protocol. This protocol is well-known for its ability to re-establish a dropped connection automatically. It is also extremely stable, especially when bouncing back and forth between cellular connections and Wi-Fi hotspots. Finally, IKEv2 is extremely fast, while still offering the best possible security with the IPSec protocol. These VPNs are not our favorites for general use, as their native applications do not, in our opinion, work to an acceptable standard on desktop computers.

NordVPN: NordVPN offers an excellent iOS application. It is simple and user friendly, and NordVPN has an excellent reputation. NordVPN costs \$69.99/year or \$79.99 for two years. You are allowed to connect up to six devices simultaneously.

Windscribe: We have only been using this VPN for a few months now, but its performance is simply outstanding on iOS devices. The only downside we have noticed is that Windscribe uses batteries significantly faster than other options. Windscribe does collect bandwidth logs but these are cleared every 30 days. Windscribe VPN costs \$49.99/year.

SECURE MESSAGING APPLICATIONS

Wire Secure Messenger

Wire Secure Messenger (which we will refer to simply as “Wire” hereafter) is our favorite messaging application. Wire offers the same basic features that many encrypted applications offer: end-to-end encrypted messages with zero provider knowledge. Fortunately, it offers a lot of features that most messaging systems are lacking.

Features and Platforms: First, Wire provides native applications for all major operating systems including Windows, Mac, Linux, Android, and iOS. Wire also has a web login for those who cannot install the native application, such as individuals working on government computers. All instances of Wire (including the web version) allow you to send text messages, voice calls, video calls, and file-sharing. Wire supports group calling (up to 10 participants) and group messaging (up to 128 participants).

Getting your friends to switch to Wire should be fairly painless. The application is intuitive and user-friendly. It has an extremely pleasing look, feel, and notification sounds. One of the most attractive features of Wire is its call quality. Many of the employees of Wire are former senior employees at Skype, so the company has deep institutional knowledge of VoIP systems. Wire stands head and shoulders above many other messengers (even some mainstream messengers) in regards to call quality.

Wire also offers message ephemerality or expiring messages. This means that you can set messages to expire after a pre-defined period of time. Currently Wire’s periods of expiry are a little restricting. You have the option to have messages expire with the following periodicity: 5, 15, or 30 seconds, 1 minute, 5 minutes, or 1 day. We would prefer to see these be spaced out a bit more (perhaps along the lines of 5 seconds, 5 minutes, 5 hours, 1 day, 5 days). For almost all contacts we set messages to expire after 1 day. Keeping in mind that message ephemerality is designed to limit the historical communications stored on the device, we feel this is a good compromise between usability and security.

To download all Wire versions, visit <https://wire.com/en/download/>. Wire is available for Android as an APK at the above website, or in the Google

Play Store. Wire is available for MacOS through the Mac App Store, and iOS through the App Store. To access Wire for Web from your Chrome, Edge, Firefox, or Opera browser visit <https://app.wire.com/>.

Security: Wire's security is excellent. Wire utilizes the "Proteus" message encryption protocol. This protocol is based in the highly-regarded Signal Protocol and utilizes a form of perfect forward secrecy (PFS). Perfect forward secrecy means that if each message exchanged transmits additional encryption instructions, and if an attacker is able to break some historical messaging, this does not compromise future messages. All messages are encrypted on the sender's device and decrypted only on the recipient's device, and unavailable on Wire servers. In addition to each message being encrypted with zero provider knowledge, connections to and from Wire servers are protected with TLS 1.2 (HTTPS) encryption.

Wire's code has been extraordinarily well-reviewed. First, it was reviewed by a security researcher at the University of Waterloo in 2016. The researcher in question identified several major problems in Wire's crypto system that were promptly fixed. The next step was to launch an independent security audit, which Wire did. The audit looked at all of Wire's implementations including Wire for Web and was completed in February of 2017. It found some non-critical security issues which Wire claims to have fixed. A second round of auditing on the iOS and Android apps was completed in March of 2018 with more planned. In talking to Wire during the writing of this work, the company reiterated a desire to make security audits a consistent, ongoing process rather than a one-and-done. All of Wire's code is open source, including its server code. All of Wire's security audits may be downloaded at: <https://wire.com/en/security/#audits>

Account Setup: Wire allows you to setup accounts while providing only minimal information. When you create an account on a mobile device you will be required to provide a phone number. If you set up your account on a desktop device you are only required to provide an email address. While we would prefer to provide no information whatsoever, an email address is the least intrusive and, quite frankly, easiest means.

There is one other consideration if using a telephone number for setup. Using a telephone number allows account discovery by others. Let's assume you set up your Wire account with your primary phone number. When anyone with that number installs Wire on their phone and allows it to access their contacts, you may be automatically added as a contact in their instance of Wire. This happens because Wire stores a hashed (read: not plain text) copy of your phone number to facilitate account discovery. This is not the case with email addresses, which are not used for account discovery.

We recommend setting up your Wire accounts through the organic Wire application on a desktop computer. You will be asked to provide an email address and password. Our preference is to choose an email address that has not been used elsewhere for any purpose. A Blur email address works extremely well for this. Next, you will be prompted to retrieve a six-digit code from your email that you will enter into the application to verify ownership of the email address. Finally, you will be asked to choose an @handle (Wire's version of a username) and screen name.

Screen Names and Handles: Of course, there are multiple approaches you can take here depending on your aims. Wire contacts are added by their screen name and/or @handle. The screen name is how you appear in others' contact lists, and the @handle is your actual Wire username. If you are shooting for maximum anonymity, choose a handle and screen name that is exceedingly common; anything with the base name "john" will blend nicely into the herd. Another option is to choose a pseudorandomly-generated username. Remember that other users can search by both your @handle and your screen name. Creating an @handle that is designed to hide in the noise does no good if you make your screen name your first and last name.

If you are not shooting for anonymity and want others to be able to find your account, use something that approximates your name or other information for which people would search. Examples of this would be your first initial and last name or full first and last name. Even if people are able to locate your account you still have some protections in place from receiving unwanted messages from them. We will discuss these in the next section.

Multiple Wire Accounts: Wire will allow you to have three accounts open in any instance of the application. For example, if you have the app installed on your phone you can have three active accounts open in the device. We like this feature because like Sudo, it allows us to segregate contacts into certain groups. There are many ways you could choose to segregate these accounts, but several ideas for specific account uses are laid out below:

Public Account: This is an account with an easily pronounceable username that you can give out to casual contacts. The username may align closely with your true name or a username that you use on other messaging accounts. If you are a public figure who lists your contact information online, this might be the appropriate account for such usage.

Family & Friends Personal Account: Since this account is used to communicate with trusted parties you may wish to protect it a little more closely. You may eventually wish to “upgrade” some people from your Public Account to this account after they are deemed trustworthy.

Work Account: This is an account that can be used to segregate your work contacts from your personal contacts. All of your co-workers, partners, vendors, etc. with whom you need to stay in contact but with whom you don’t communicate on a personal level can go in this list.

You are limited only by your own imagination in how you use these accounts, but you should take advantage of this capability. Wire also allows you to choose a theme color for each account. To make it clear to yourself which account you are in at any given time, we recommend color coding these along the lines of the US Government classification system. Our Public accounts are green (least private), our work/semi-public accounts are red (somewhat private), and our Personal accounts are orange (most private).

Wire Contacts: Wire only allows you to communicate with people in your contacts who have also accepted you as contact. To initiate a new contact you will have to find that person’s @handle and send them a connection request. When that person has received and approved the request, he or she will be

added to your list of contacts. If at any time you decide you no longer wish to receive messages from a contact you have two options.

First, you can “mute” that conversation. You will still receive all of his or her messages, but you will not receive notifications for them. We find this especially helpful for noisy group conversations. The next option is to block the contact. This does not remove the individual from your contact list but prevents him or her from being able to send you a message. If you decide later that you no longer wish to block that individual, you can undo this action.

Wire Negatives: The first strike against Wire, and one that we would be remiss for not mentioning is that some of your metadata is accessible to system administrators at Wire. They are able to see your contact list. Having this information available is necessary to sync your conversations across all devices. Be advised that this is simply a list of contacts; it does not record how or how often you communicate with these contacts. If they have been diligent about setting up their accounts privately as well, this should reveal minimal information about either party.

Another slightly annoying aspect of Wire is how disappearing messages work. While we understand the limitations of message ephemerality, the implementation seems somewhat clunky. Currently Wire offers no ability to set a global message expiration period. This means that you have to enable expiring messages for every single conversation. It further means that you have to do this across all your devices; if you have expiring messages enabled on your desktop, you have not enabled it on your mobile device and will have to remember to do so.

Signal Private Messenger

Though Wire meets most of our needs, we find it necessary to maintain two completely separate methods of secure communications. This is for two reasons. First, there may be an undiscovered security problem with Wire. It so, we want another trusted option immediately available. Secondly, we sometimes need to pass out-of-band traffic. That is, traffic passed through

another means of communication. The reasons we would need to do this are varied but could include verifying key fingerprints as discussed in the next section. If your security needs are high enough, you may even wish to break messages up over different messaging systems to reduce the likelihood of interception over one particular messenger. Our preferred “backup” encrypted messaging application is Signal Private Messenger.

Signal is one of the most trusted messaging applications around. It has been around for several years, even though it was originally introduced as multiple apps under multiple names (TextSecure and RedPhone for messaging and calling, respectively).

Signal Negatives: As with Wire, we have a couple of issues with Signal. The first is Signal’s contact discovery methodology. In order to setup a Signal account you must provide a phone number. This phone number is sent a text message and is forever associated with your Signal account. In the future when someone installs Signal and has your number in their contact list, they will be able to see that you are a Signal user. This method of account setup and contact discovery makes Signal easy to use and eliminates the need to setup usernames and passwords, but it also creates several complications.

We carefully segregate our Sudo numbers over our many contacts. When we give someone a phone number only to later discover they have Signal, we then have to give them another phone number. This begins to create linkage between our Sudo numbers. Next, if you use a burner number to create your Signal account, you will have to create a brand-new Signal account if you re-install the app on a new (or newly wiped) device. If you are setting up Signal for the first time, we recommend that you set it up using a Sudo that you will have for the foreseeable future. If you have already setup Signal using your SIM-card phone number, we recommend you transition over to a Sudo number and migrate your contacts over.

Another complaint with Signal is the lack of the ability to passcode protect the application on iOS devices.

Our final complaint with this messaging system is the inability to conduct

audio and video calls from the desktop. These features are only available on the iOS and Android version of the app, while the desktop versions are limited to text messaging. This is the one feature above all others that prompted us to move to Wire Secure Messenger. Though it might sound like a small thing, this allows us to communicate from our desktop computers while at home, and it helps to sell the product to others.

BEST PRACTICE: VERIFYING KEY FINGERPRINTS

Both Wire and Signal give you the ability to verify your contacts' key fingerprints. Though often overlooked, this is an important step for any contacts with whom you desire to actually communicate securely (if you are reading this book we assume you wish to communicate with everyone securely). If you are not verifying key fingerprints you are simply trusting in the ideas that your connection has not being tampered with by a man in the middle or your keys have become corrupted in some non-malicious way.

How Fingerprinting Works: For this example, let's assume that to users, Alice and Bob, each have a phone. They have established a connection (by accepting each other as a contact), and in the process a public key is exchanged. This public key is used to encrypt their communications and has a completely unique fingerprint (a very long code). This means that Bob's key should produce the same fingerprint on Alice's device that it does on his own device. If it does not there is a problem in the cryptosystem, and they may be the victim of a Man-in-the-Middle (MitM) attack.

A man-in-the-middle would attempt to get between Alice and Bob's communications. He or she would establish an intermediary relay. To be able to read their messages, however, the hacker would have to have a way to decrypt them. Rather than let Alice and Bob share their keys directly with each other, the hacker would capture both keys, then issue his own keys to Alice and Bob. This means that Alice and Bob would both display a fingerprint for a different key. When Alice attempts to verify Bob's key

fingerprint she would see the hacker's and this would not match the number on Bob's phone. Verifying key fingerprints gives us a very strong assurance that our communications are not being tampered with in-transit, and our communication system is truly secure.

If you take the time to do this (in either Signal or Wire) you can be confident that your communications are encrypted all the way to the recipient's devices. You can also mark each contact as verified, which gives you a quick, visual indicator of which contacts are verified and which are not. This process takes a bit of time because you must verify keys with each of your contacts but is well worth it for the peace of mind it provides.

It is strongly recommended that you exchange keys through an out-of-band communication methodology. "Out-of-band" means you are exchanging that information outside of the app that you are verifying (i.e. if you are verifying a Wire contact, do not rely on key fingerprints sent via Wire). The reason is that if you are exchanging key fingerprints you have not yet done so and the communication system is not yet fully trusted. Because it is not yet fully trusted, you also cannot fully trust key fingerprints transmitted through it.

To verify fingerprints from these applications, we recommend using a completely different system such as ProtonMail. All it would take is capturing a screenshot of each of the other person's fingerprints and emailing the screenshots to him or her. If they match on his or her end, you can fully verify that communicant. Another, perhaps better method would be to verify these via voice or video call. This is perhaps the most secure method because tampering with a text message or email is trivially easy compared to tampering with a person's voice and face in real time during a conversation.

Signal: In Signal, open a conversation. Tap the contact's username or phone number. In the settings menu tap "Show Safety Number". This will present you with the number itself, a 60-digit numeric code. This can be exchanged remotely using the methods described above. Signal will also provide you with a QR code which is useful if you are face-to-face with the other party. You can simply scan his or her safety number and Signal will mark the contact as verified. In the future a small check mark will appear beneath the

user's username or telephone number when you open that conversation.

Wire: Before verifying your contacts, you should verify your own devices across all your other devices. For this explanation, assume that you have three devices: an iPhone, an iPod Touch, and a desktop computer. First, open Wire on all three devices. Next, beginning with your iPhone, open your Wire account. Access the settings by tapping your avatar at the top of the screen, then click "Devices". This should display a list of all devices that are logged into this account. Find the device you are currently on (the iPhone); it should be at the top of the list. Now repeat this process on your iPod and desktop computer, but on these devices, select the iPhone. Ensure that the key fingerprint displayed on the iPhone itself is the fingerprint that the iPod and desktop display. If they are, toggle the "Verified" button.

Repeat this process on your iPod and desktop. This takes some time and can be slightly confusing, but it is worthwhile. It ensures that your connections between devices are not being tampered with. It also ensures that in the future all of your devices reflect all of your correct fingerprints and you can verify these with contacts without opening all of your devices. Once you have verified all of your devices you can begin verifying contacts' devices.

To do so, tap or click your contact's avatar at the top of the screen. On the next screen (mobile) or the flyout menu (desktop) click "Devices". This will list the devices from which the person has logged into the account. He or she will have to provide you with the key fingerprint, an 84-digit alphanumeric string. Our strategy is generally to provide the other party with the first 4 pairs and last four pairs in the string. If these match, it is safe to assume the codes are good. After verifying that your numbers match those of the other party, toggle the "Verified" switch. In the future when you tap that contact's screen name, a blue shield will be displayed by the contact's name, indicating he or she is trusted.

CHAPTER 5: A SMARTPHONE WITHOUT A PHONE

Privacy enthusiasts know that the pursuit of protecting their personal information and overcoming obstacles to our privacy and security often require us to adapt and to be creative with technology. It is also a matter of degrees, where a person needs to find an acceptable balance between convenience and their privacy goals that fit their lifestyle and capabilities. This chapter explores a communications solution on one end of the spectrum that some may consider to be extreme. Having already laid out the challenges that traditional cellular communications present to our privacy, we feel that many readers may benefit from learning new techniques to overcome some of those vulnerabilities.

One option to overcome the privacy challenges of the baseband process is to use an iPod Touch as your mobile device. We have both incorporated this approach in our communications strategies. This helps to limit the amount of information we disseminate as we communicate, and still maintain (most of) the options and functionality of what a smartphone provides.

WHY AN IPOD IS MORE PRIVATE AND SECURE THAN A PHONE

Why would you go to all this trouble to setup a device that is far less capable than an iPhone, even an iPhone that is two or three generations old? It is the very lack of capability that makes an iPod desirable. First it does not have cellular connectivity. Mobile phones are tracking devices at their very core. They must “know” where they are in relation to towers to provide you with service, which means they can be easily tracked. Secondly, mobile phones – even when powered off – can be remotely controlled by sophisticated

adversaries (see Chapter 1). The iPod Touch is a far less complicated device. It has neither an IMEI, the unchangeable number associated with a mobile phone, or SIM card (or MEID, ICCID, SEID, etc.). It cannot attach itself to a cellular network or be tracked by one. It does have a MAC address that will be associated with the Wi-Fi networks you use, but you can carefully manage those, and we will discuss this later.

ADVANTAGES

The iPod Touch fills a much-needed space. Wi-Fi only, with no baseband processor or GPS chip.

- **Network:** the iPod does not have inherent baseband or SIM card insecurities.
- **Network:** you can control which Wi-Fi networks your device is exposed to.
- **Data at Rest:** The iPod employs default device encryption.
- **Data at Rest:** Our messaging applications of choice (Wire & Signal) employ database encryption and isolation.
- **Data in Motion:** Wire & Signal use modern protocols and state-of-the-art encryption.
- **OS Security:** Apple pushes security patches relatively quickly and the iPod is a more challenging device to infect with malware when used correctly.
- **Verifiability:** Wire & Signal allow users to compare and verify encryption key fingerprints.
- **Verifiability:** Wire & Signal are a free and open source software projects that are publicly audited.
- **Scalability:** other people with an iPod, iPhone or Android can freely install and use Wire & Signal encrypted messaging applications.
- **Liability:** when employed in a work place with supportive policy, work-oriented communications are separated from personal devices.

DREW'S IPOD SETUP

I am no longer paying a cell phone bill. The monthly savings is significant and I no longer have to visit my carrier's retail store to make a payment on the pre-paid account.

As we have discussed, we use our phones in a very non-traditional manner. We have never used the carrier assigned phone number for anything, and instead use VoIP apps to handle all of our texting and calling needs. Encrypted communication apps like Wire and Signal handle the bulk of our communications with the majority of people we keep in touch with daily. The rest of our contacts have a compartmentalized Sudo number to reach us.

I could continue paying for cell service, but why? At home I use a properly configured firewall which acts as a high-powered router that is capable protecting my network 24 hours a day. The router and firewall are configured to utilize a VPN with an absolute kill switch. Every device on my network is protected by a VPN, and it blocks all incoming connections and forces a VPN on all outgoing Internet traffic. Because all of my communication apps only need Wi-Fi to work, my phone is in airplane mode while at home and is never connected to a cellular network.

Away from home, I have other "trusted" Wi-Fi networks that I can connect to throughout the day. Again, the phone remains in airplane mode and never needs a cellular network to connect to. With Wi-Fi availability so common nowadays, I decided to stop paying a cell phone bill entirely and also change to a device that did not even have the capability to access a cellular network. This device that now handles 100% of my communications is the iPod Touch. An iPod Touch is remarkably similar to an iPhone, but potentially far more private and secure.

Purchasing an iPod Touch Anonymously

A Note to the Reader: Because we both "geek out" on privacy and security, we took the step of purchasing our iPods anonymously to the extreme. In most cases expending such thought-energy on this step is unnecessary.

Unless you are in the very highest threat models, you will be fine strolling into Target, picking out your device, and paying in cash.

The first step is to find an iPod Touch and purchase the device anonymously. We recommend purchasing the latest model (currently the 6th Generation) to (attempt to) keep pace with technology. To do things as anonymously as possible, we initially considered the purchase of a used model. Though this might create linkage with the original owner, we thought this was preferable to purchasing in-store. There would be no security cameras, or at least not ones that are directly correlated to purchase date/time stamps. We could also easily find one for sale in the major cities an hour from our homes and meet the seller at a big shopping center to prevent our vehicles from being seen. To minimize any data associated with us, we would also thirty days after the purchase before setting up the device. This would ensure that the owner's memory of us would have faded sufficiently.

Finding and contacting a seller without creating linkage proved to be a challenge. Obviously, we couldn't call from our "real" numbers. Even calling from a Sudo would create a permanent record with their cellular service providers. We considered the purchase of a "burner" phone for this use, but it would have been extremely difficult to purchase such a phone without creating linkage with our real devices. A burner phone would also increase our investment by \$30-50. Even searching for the device online was problematic. Even using a VPN there was some level of concern that worried us about creating a trail. Despite our anti-forensics efforts, our computers would be littered with records of Craigslist searches. We could have asked a surrogate to make the purchase, but this created additional complications and linkage to us personally.

With all of this considered, we decided to buy a new one from Wal-Mart, even though it would cost a bit more up front. We would still pay in cash and let the iPod "cook" for 30-60 days. This would let us be reasonably certain any security footage would be gone by the first time we turned the device on, so this is what we did. Even this presented its own challenges. Before making the purchase, we debated heavily on two strategies. The first strategy would involve stopping at a Wal-Mart somewhere between two points (i.e. while

driving from Cleveland to Columbus). The other strategy involved driving an hour (or more) from a fixed point. The fixed point would be either our home or a hotel at which one of us was staying for a short period. We both chose the latter (fixed point) option because it allowed us to leave our phones at the fixed point. This prevented cellular location data from placing us in the same location, and at the same date and time, as the purchase.

While on (separate) business trips we found a Wal-Mart about 45 minutes from where we were staying. We purposely chose a Wal-Mart that was not the closest to our hotel. We left our phones at the hotel and drove out to the store. We paid cash for a 6th Generation iPod Touch with 32 GB of storage, which we felt would be more than sufficient for the amount of storage we would need with limited applications and other data. We also purchased a \$20 iTunes gift card, the smallest denomination we could find. To download any apps we would need to fund the iTunes account for the device. Unlike Google Play, iTunes allows you to fund your account without providing a credit card – an important feature. Like the device, the gift card would also “cook” for 30-60 days because it, too, could be linked back to the purchase. Two months later we pulled these devices out and began setting them up.

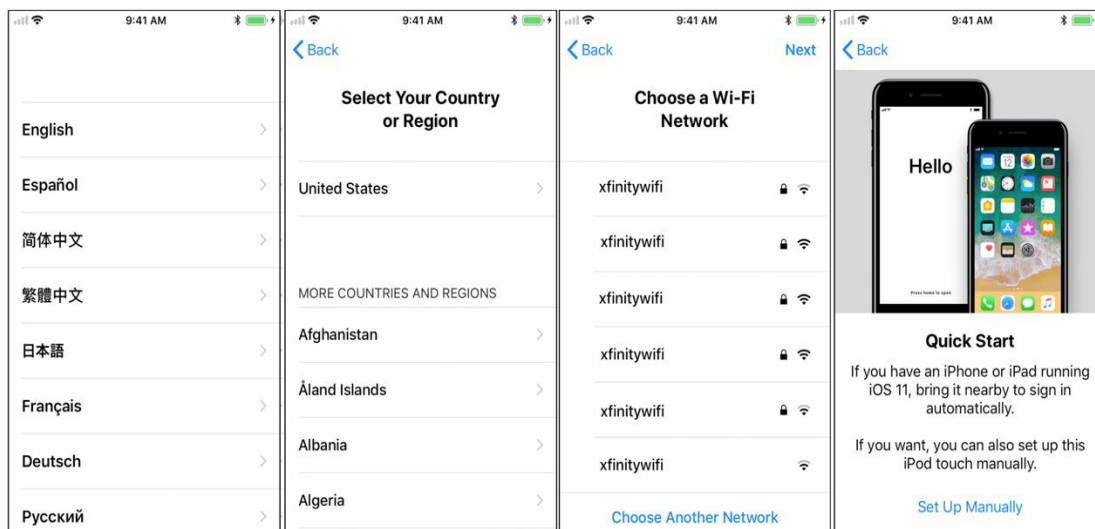
Device Setup

Upon initially powering on the device, you will be met with a welcome screen. Notice that **Wi-Fi and Bluetooth are already on!** If you are attempting to set up the iPod completely anonymously, DO NOT power the device on within range of your home network (or any other network/device that could be tied to you). After you begin the setup you will be asked to select a language and country/region. Finally, you will be asked to select a Wi-Fi network. Be extremely careful about here; if you are attempting anonymity use only public Wi-Fi that you have never associated your other personal devices with.

The setup process will begin with some very basic questions. You will be asked to provide your language and country. You will also be asked to sign

into the Wi-Fi network of your choice, and this is a necessity. Without Wi-Fi connectivity you will not be able to complete some of the next steps. When you have signed into Wi-Fi you will be asked whether you prefer a “Quick Start” or to set the device up manually. Of course, we recommend a manual setup.

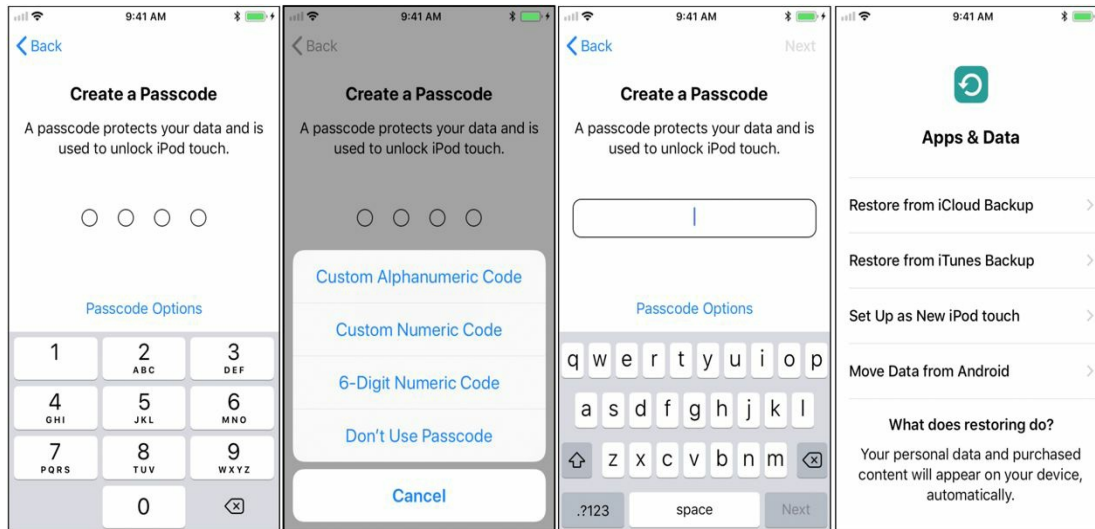
The next screen will guide you through setting up a passcode. The iPod Touch still defaults to an insecure four-digit passcode. Tapping “Passcode Options” will give you the full suite of choices. We recommend choosing a Custom Length Numeric Code. Enter the code twice to set it. Finally, you will be asked about restoring from another iOS device; for this option choose “Set Up as New iPod Touch”.



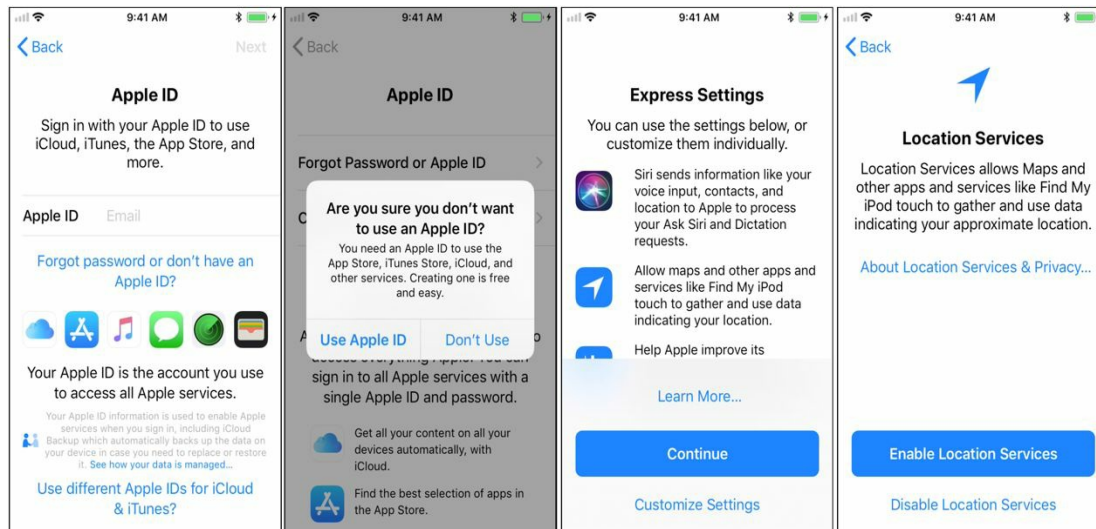
CUSTOM NUMERIC VS. CUSTOM ALPHANUMERIC PASSCODES

Your choice here will depend on your threat model and use-case. We generally recommend using a Custom Numeric Code on iOS device (more than six numerical characters) because they can be very long. We have successfully tested passcodes as long as 40 characters. Additionally, with Apple’s enforced 80-millisecond delay between passcode attempts, coupled

with the Erase Data function, a 12-16-character passcode will probably not be broken. If, however, you are operating in an exceptionally high-risk environment or plan to leave the device unattended, we recommend a Custom Alphanumeric Code.

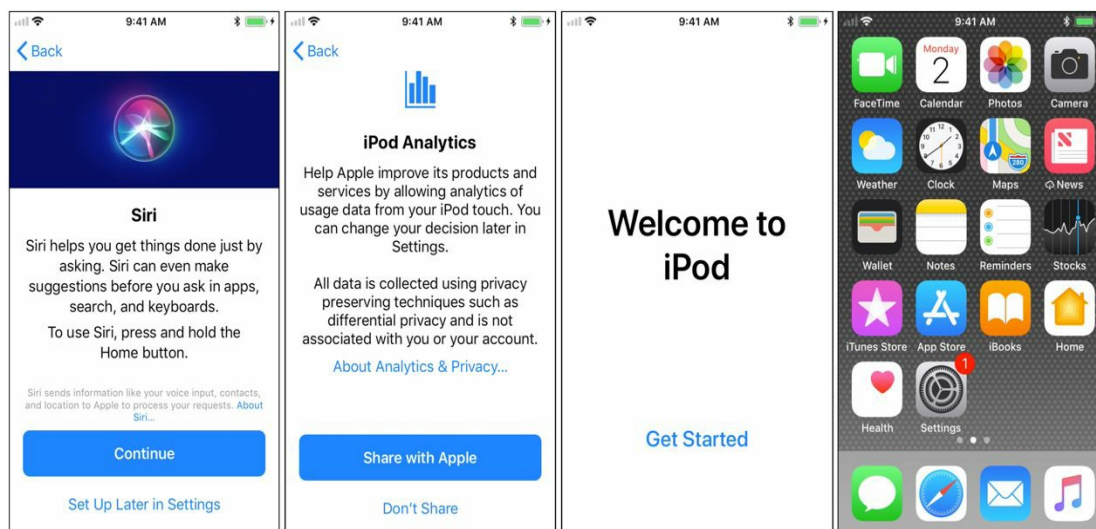


The next series of screens will attempt to get you to setup an Apple ID account. We recommend skipping this step for now. We went through the process of setting up a brand-new iPod Touch for this book and we are glad we did. Though we have both set up multiple iPods, the process has changed significantly in the last few months and much more information is required. You will be asked to confirm that you want to skip this step.



After you have skipped the Apple ID setup, you will be asked if you want to use Express Settings or opt for a manual setup. Where possible, we always prefer a manual setup as it allows us more control over what permissions are offered. The next screen will ask you about Location Services. Again, we recommend setting this feature up later in the process when you have more control of what apps and services are allowed to access this sensitive data.

On the next screen you will be asked if you would like to enable Siri (by tapping Continue) or “Setup Later In Settings”. Siri is very intrusive, and we recommend leaving this feature turned off. Select the option to Setup Later. Finally, you will be asked if you would like to share Analytics data with Apple. Obviously, our answer is a very firm “no”. After you have made this selection you will be welcomed to your new iPod.



This is just the initial device setup. Next, we will cover going through the iPod's settings to ensure the device is as secure and private as possible before continuing.

The goal of these settings is to make the device as inherently hardened as possible. These changes are designed to lower the footprint of the iPod by limiting the amount of information it transmits, making it less trackable, and generally less “noisy”. Many of these settings can also be applied to your iPhone.

General Settings

The remainder of the settings we will deal with are within the Settings menu. The first is perhaps one of the most important settings on the device: Software Update. Keeping the OS updated is incredibly important to security. Navigate to **Settings >> General >> Software Update**. The iPod will automatically check for an update. If an update is available, allow it to download and install before you proceed further. Next, go to Spotlight Search and turn off all options. Next, go back to General and scroll down to Siri. Ensure that Siri is turned off. Finally, go to Handoff and Installed Apps and turn both off.

Passcode Lock and Privacy

Go back into Settings and scroll down to Passcode Lock. Since you have already applied a passcode to the device you will be prompted to enter it before being allowed to proceed. If you did not initially setup a good, strong passcode you can do so here. Next, scroll down to Require Passcode and ensure it is set to “Immediately”. This will ensure that your iPod is locked as soon as the screen goes to sleep, giving you positive confirmation that the data on the device is protected. Next, turn off access to all settings when the device is locked including Voice Dial, Today, Notifications View, Reply with Message, and Wallet. Even though we will not use any of these settings with this device, I would like to limit, to the maximum extent possible, what is available on the lock screen. Finally, enable Erase Data. This will cause the device to be completely overwritten and erased upon the entry of 10 incorrect passcode attempts.

Next, go back to Settings and tap Privacy. Tap the first setting, Location Services. Location Services should already be disabled (from setup), but if it is not, disable it here. Also tap Share My Location and disable this setting, as well. Next, scroll through each Privacy setting (Contacts, Calendars, etc.) and turn off any app that is requesting access to this data. In the future we will have to manipulate some of these settings for some apps that we will install, but for now disable everything. Finally, scroll down to Diagnostics & Usage and Advertising.

Privacy >> Diagnostics and Usage: Tap Diagnostics & Usage. Select “Don’t Send”. This will limit information transmitted back to Apple about usage of the device.

Privacy >> Advertising: Toggle the “Limit Ad Tracking” slider to ON. Though I won’t use this device for much (if any) browsing, I still want to limit the information that can be collected about me. Tapping “Reset Advertising Identifier” allows you to reset the advertising code that is unique to your device. Again, this is probably not a major concern for our purposes but resetting this occasionally can help limit tracking through iAds.

iCloud

iCloud is Apple's cloud storage solution. By default your iOS device will be setup to send information to iCloud. We recommend you disable all of this sharing. Navigate to Settings >> iCloud. Toggle iCloud Drive and Photos to OFF. Confirm these decisions. Next, toggle all other settings to OFF. This will ensure that your data is not being transmitted to iCloud. Finally, tap "Share My Location" and ensure that it, too is turned off.

Background App Refresh

Finally, navigate to Settings >> General >> Background App Refresh. Toggle each application to off, then turn the Global Setting to OFF. Background App Refresh allows applications to check for updates and new content. Turning this off will help preserve your battery, and limit the information being transmitted to and from the device.

The initial setup of the ultra-private iPod phone and system settings applied here have the device almost ready to go. Before communicating on it we first need to add applications that will permit us to talk securely. We will cover iTunes setup and adding applications in the next part of this series. Stay tuned!

At this point in the process, the iPod has been initially setup, and the settings modified to make it as organically secure as possible. At this point it is necessary to fund the iTunes account. Even if you only plan to use free applications, the account must be funded before you can download apps.

We are very disappointed to report that Apple now requires much more information to create a fully funded iTunes account than it did just a few months ago. To set up and fund your iTunes account you will need to provide the following:

- **Name**
- **Address:** This cannot be a fictitious address, but it is not verified.
- **Telephone Number:** We have had limited success using an application

called Burner for this purpose. Apple will not accept Sudo numbers. As a last resort, you may have to purchase a very inexpensive “burner” telephone to at which you receive this verification message.

- **Credit Card Number:** We have had success using credit card numbers from services like Blur (<https://dnt.abine.com/#/register>) and Privacy.com (<https://privacy.com/>), as well as prepaid credit cards.

You will be required to provide all of this information before you will be permitted to download apps from the App Store. After you have access to the App Store, you can begin downloading and installing applications.

Applications on the iPod Touch

Since the iPod is designed as a secure messenger, we want to keep applications to an absolute minimum. We recommend the following applications, all of which have been discussed previously discussed:

- Private Internet Access VPN
- Wire Secure Messenger for use as our primary messenger
- Sudo, for plaintext phone calls and SMS messages
- ProtonMail for sending and receiving encrypted email

Additionally, we both use a password manager to keep track of the passwords for these applications. We both use and recommend MiniKeePass. MiniKeePass is a fork of KeePass, and will open any database built with the .kdbx file format.

USE CASE SCENARIOS

Use Case 1: Total Anonymity. Total anonymity is a very hard act to pull off. Users in this category have immediate concerns falling into the “life or liberty” category. They are operating against an adversary and would use this device to protect both their identity and the content of their

communications. I have previously mentioned that Signal (or any other encrypted messenger, really) cannot hide your metadata. Using an iPod, rather than an iPhone, takes a lot of players out of the loop, but metadata is still being created somewhere. If you start calling your usual Signal contacts on your new device, the metadata will very quickly reveal the owner of the device.

For this tool to be a truly effective tool for anonymity requires two-party participation. This means that those with whom you communicate will have to take similar measures. This will very likely be cost prohibitive, and you will probably find others unwilling to take such extreme measures. You should also be aware of other factors that may pierce your anonymity. Public Wi-Fi hotspots without attending security cameras may be difficult to locate. If your life depends on anonymity, you should scout these locations well in advance of connecting your iPod phone.

OPSEC for this threat model: There are a couple of operational security measures you may wish to take with a similar device:

- Do not connect to your home, office, or other network to which you have associated your true-name devices.
- Do not turn Wi-Fi or other interfaces on within range of your other devices. A sufficiently sophisticated adversary could access this which would reveal your true identity. Even if your other devices are not in your true name they could be turned into eavesdropping devices by certain adversaries.
- Be wary of security cameras at public Wi-Fi hotspots.
- Leave Wi-Fi off when the device is not in use. It can – and already is – used to track your location.
- Don't forget to "forget" Wi-Fi networks you have used prior to turning Wi-Fi off. If you consistently use the same networks I recommend storing their SSIDs and password managers elsewhere, like in a password manager or encrypted notes application, like Standard Notes.

Use Case 2: Enhanced Privacy. This is a much more realistic goal

for most. Our iPod phones, while not completely anonymous, offer an outstanding privacy layer – even though we have written about them. We can now give out a phone number that is not tied to our names, or cellular accounts and that can be reached only through Wire, Signal, or Sudo. We can also communicate using Wire to trusted contacts or use Sudo for other scenarios that require a VoIP number. We have a lot of options. We can also turn the device off and have high confidence that it cannot be tracked by cell towers or remotely activated.

Use Case 3: Blended Approach: Using an iPod Touch doesn't have to be a 100% solution. There are numerous ways it can be rolled into a blended approach to allow you the convenience of a cell phone while still preserving much of your privacy. One excellent use-case is to use the iPod Touch while at home and at work (where you likely have Wi-Fi). This means that 90% of the time you don't need your actual phone and can lean on the iPod, while still keeping your phone handy for weekend excursions, family outings, or navigating to unfamiliar places.

Other Use-Cases For the iPod Touch

Even if you choose not to be a “privacy extremist” and replace your phone with an iPod touch, there are numerous other reasons you may consider getting one.

Backup Phone: These devices are an excellent backup to your regular smartphone. If your phone is lost or damaged you can transition immediately to the iPod. Of course, this assumes that you primarily use Sudo, Wire, and other VoIP technology for your communication needs. It also assumes you have access to Wi-Fi throughout most of your day.

Special Purpose Communications: If you are a person who has special communications needs, an iPod Touch may be right for you. If you have an extremely active dating life and wish to keep those numbers and applications on their own mobile device, the Touch gives you the ability to do so. If you participate heavily in a business that requires a great deal of interaction with customers, this gives you the ability to completely turn your “work” phone

off for the day while still not completely cutting yourself off from the world. And of course, if you have special security concerns but aren't willing to give up a cellular-enabled smartphone, the iPod at least gives you the ability to compartmentalize your sensitive communications. The circumstances for this need may vary widely and your threat model will dictate your needs.

Preparedness: If you are preparedness-minded and keep a bag packed and ready to go, an iPod Touch would be a more affordable alternative to a second phone. Though it would do you little good while departing your immediate area, it would provide you with a communication capability once you are out of the affected area and are able to access Wi-Fi. If you choose to use an iPod for this purpose, we strongly recommend you exercise the battery by using the device and recharging it^[7] at least once per month. And of course, you should sync it frequently to keep the phone numbers, password manager databases, and other critical information up-to-date.

UNINTENDED CONSEQUENCES OF THE IPOD TOUCH

Using an iPod Touch as a communication device offers some amazing advantages for privacy-seekers. It also has some disadvantages. Some of these are obvious, such as the lack of a constant data connection. Some of these are less obvious, and we do not mean to imply that the iPod is an iPhone minus the baseband processor. Some of these factors are far more serious than others. The two major disadvantages that we see are the lack of the ability to call 911 and the lack of a Secure Enclave. These are discussed more fully below, as are the smaller, convenience-related downsides.

MAJOR DISADVANTAGE - 911: Perhaps the single biggest practical downside of the iPod phone replacement solution is the inability to call 911. Even if the device has a Wi-Fi connection, you will still be unable to call 911 through voice-over-IP systems. This presents a hazard to you by restricting your ability to call emergency services. This also potentially endangers others; if you witness a crime, accident, or other emergency, you have to way

to reach help. Finally, if you carry a concealed handgun and are forced to use it, you will want to call 911 immediately. If you only have an iPod Touch you may not be able to do so. We do offer a couple of possible solutions below, but realize neither is perfect:

- Save the standard phone numbers for your local police department, sheriff's office, and state police in your contacts in Sudo. The downside to this solution is that it requires you to use many fine motor skills to find the number. You will also likely have to explain to the person answering the phone that you do not have the ability to call 911. And of course, if you don't have Wi-Fi, this technique offers no help at all.

- Carry an inexpensive mobile phone in a Faraday bag. You will not need to keep a SIM card active to call 911 on the device. All mobile phones (in the US) must be allowed to place 911 calls even if no service is active on the device. This would still require that you retrieve the device from storage (in your car, a backpack, etc) prior to use. If you choose this strategy ensure that you charge the phone regularly and exercise the battery occasionally.

MAJOR DISADVANTAGE - Secure Enclave: The current (6th-gen) iPod Touch does not have Apples famous (or infamous) Secure Enclave hardware encryption module. Though the device does offer full disk encryption, we have very little confidence that this is unbreakable to sophisticated, well-funded adversaries. This should inform several decisions you make about how to use your device, including:

- **Limit Data Stored:** Though there are several "technology solutions" offered here, your best line of defense is to modify your behavior. You should limit the information stored on and accounts accessible through the device to the absolute minimum. If you use the iPod's camera, you should be disciplined about downloading these photos to another platform and clearing them from your device as often as is feasible. The same should go for other information stored on the device.

Encrypted apps. Because it should be assumed that your device can be accessed by sophisticated actors, you should attempt to encrypt everything on the device with another form of encryption. We mentioned this in Chapter 4 and offered several alternatives to native applications including Wire Secure Messenger and Standard Notes.

In addition to encrypting local content, many encrypted messengers also offer ephemeral messaging. This means that your messages expire and are after a pre-determined interval. Though many uninformed individuals believe this to be a way to prevent others from saving copies of their images, this is truly designed for another purpose. If you set all of your messages to expire after 24 hours, the most message content that can be captured from your device is the last 24 hours' worth. Contrast this to the average person's text message history, which is plaintext and likely stores many months of conversations, both on the device and with the provider. This expands both the threat model and the attack surface greatly.

Passcode/Passphrase Protect: Each application that can be individually locked and protected with its own passcode, should be. Many applications offer this ability, though not all of them operate the same. Some passcode-protect but do not encrypt content. Some do not allow you to choose a custom passphrase and only allow you to use the device's existing passcode (which, in our opinion offers very little additional security from sophisticated actors). Some applications only allow you to assign a four-digit passcode, which again, provides very little security.

Reachability: The iPod Touch makes it difficult to remain reachable. If you are not on Wi-Fi or a mobile cellular hotspot, you cannot be contacted. Sometimes we like this, and doubtlessly you will, too. But there are also times when others need to get in touch with us. For this situation we recommend you consider an old-school solution: the pager.

Pagers are passive radio receivers. They do not emit any signal and cannot transmit. As such, they cannot be used to track your movements. Because they contain very little information, hacking one would not be particularly

valuable, and the loss of one would not be a big deal. A pager allows you to receive a short, alphanumeric message (typically a phone number). Pagers are inexpensive and coverage plans are available for as little as a few dollars per month.

Aftermarket Support: The iPod Touch isn't nearly as popular as the various versions of the iPhone. Because of this there are far fewer options for protective cases, screen covers, and the various other accessories that make mobile devices more convenient.

Battery Life: The battery life of the iPod Touch is much shorter than that of the iPhone. This is the cost of the thin, small size of the device. We have found that charging the device several times per day is necessary. There are a couple of extended battery iPod cases on the market, but as the previous paragraph mentioned, aftermarket support for the iPod Touch isn't great. We have yet to find a battery case that we are really happy with.

Size: The size of the iPod Touch will be a blessing or a curse depending on how you feel about the size of the current crop of iPhones and the trend toward larger models. It is substantially smaller than the flagship iOS device. This decrease in size is boon in the pocket and bane in the hand. Even though both of us can appreciate smaller devices, the decrease in size from even an iPhone 6s is dramatic. This requires an acclimatization period to get used to the position of the smaller keyboard and other controls that you are familiar with. Within a week of daily use this will become a non-issue.

Speed: The speed of the iPod Touch is much slower than that of newer iPhones. The 6th Generation iPod Touch has an A8 processor, the same processor found in the iPhone 6, but the iPod Touch version is slightly underclocked (meaning speed-limited) at 1.1 Ghz versus the full 1.4 Ghz the processor is capable of^[8]. Additionally, this chip is at least three generations old at the time of this writing. In the meantime, apps have been developed to utilize the power of newer, faster processors. This all adds up to a device that is noticeably slower than a newer iPhone. There is lag when opening apps or accessing certain functions in apps (including Sudo, Wire, etc.)

TouchID: Though we do not recommend TouchID to unlock your iOS device, we do find it useful for unlocking applications and approving purchases on the device. The iPod Touch does not have a TouchID feature, and TouchID is completely unavailable. The obvious solution to this is to use a passcode on all applications that offer this ability. Protecting these apps individually is much more important on the iPod than the iPhone because of the iPod's lack of the Secure Enclave encryption module.

Missing Settings: Not all of the settings of the iPhone are available for the iPod Touch. Some of these are understandable, and some are completely inexplicable. Some of the settings and capabilities that you may miss when transitioning from an iPhone to an iPod are:

- **Battery:** Two of our most-missed settings pertain to battery life. The first is Low Battery Mode. Found on the iPhone, this mode allows you to put your phone into a battery-preserving mode. Because the battery life on the iPod is so limited, we would really like to see this feature added to the iPod. The other missing battery setting is the ability to display a percentage of remaining battery life in the status bar. To determine your battery's remaining life you are left making a rough judgment from the visual battery indicator.

- **Control Center:** The iPod is also missing the ability to open the control center from the lock screen or open the camera from the lock screen. This is an inconvenience as it requires that you unlock the device to access the flashlight, the camera, the alarm/timer, Do Not Disturb mode and several other nice features.

- **Reachability:** Enabling this little-known setting on newer iPhones wakes the phone when you pick it up. Because this is not available on the iPod you have to press the Home button twice before entering your passcode.

- **Vibrate/Silent Mode:** The iPod Touch lacks the familiar ringer/silent switch used on the iPhone. Not only does it lack the switch, it also lacks the ability

to vibrate at all. This means that to fully mute the phone's notifications, you have to place it in Do Not Disturb mode.

All of these disadvantages may not paint an appealing picture of the iPod Touch as a full replacement for your iPhone. Other than the two major disadvantages listed above, all of these problems are possible to live with. In fact, there are some unintended positive consequences of the iPod Touch as well.

Forced Disconnection: Because you do not have constant data access there are times you are forced to “disconnect”. This is a two-edged sword and the thing that most people struggle to adapt with this model but over time it becomes something of a boon. It makes you realize that just a of couple decades ago we all survived without cellular phones, and we can do so again.

Voluntary Disconnection: We have discovered that some forced disconnection makes us both much less dependent on our mobile devices and promotes more voluntary disconnection. We no longer automatically resort to them any time we have an unoccupied minute. We no longer jump at the sound of an incoming message. This makes us far more observant and aware of our surroundings, and much less likely to retreat into a digital shell. This also promotes more and more meaningful social interaction with others in a wide range of circumstances.

You can promote “voluntary disconnection” through a couple more steps. The screens of cell phones have amazing color depth and resolution and app developers have exploited this to make us more susceptible to their apps. But using bright colors for notifications and badges, we check our phones more often and spend more time on them^[9]. By turning off some notifications and setting your device's screen to grayscale (black and white) you can reduce your use of the device in a way that doesn't require a lot of discipline or conscious effort on your part.

Texting and Driving: Because you do not have a data connection while on the road, there is zero temptation to text and drive.

Justin's Experience With the iPod Touch

During the writing of this book, I set up a brand-new iPod Touch from scratch. There were several reasons for this, including wanting clean screenshots without personal information, and to relearn the process. During the setup of the device I chose to give it all false information. I created a brand new Sudo account with nine new numbers and email addresses. I created three new Wire accounts and set up a new Signal account. Getting these apps onto the phone required setting up an Apple ID and funding my iTunes account. This created some hurdles that I had not anticipated.

A couple major things have changed since my original blog posts on this topic back in 2016. The first is that a working phone number is absolutely required by Apple when setting up an Apple ID. I tried using various VoIP services, but none was successful. I finally resorted to purchasing a burner phone and was successful. The other major change is the requirement to fund the account with a credit card. Previously I was able to fund my iPod's iTunes account with a gift card. I do not believe this is still an option, though there is the possibility I missed some workaround. If you require total anonymity, I recommend using a prepaid card that was purchased with cash. If not, a Privacy.com card will suffice.

CHAPTER 6: COMSEC BEST PRACTICES

PHYSICAL SECURITY

We are huge advocates of encryption. Encryption is one of the surest and best defenses against attacks to capture the data stored on your device. However, encryption should be considered a last line of defense – NOT the first.

In order for encryption to come into play, we have to fail elsewhere. We have to let an attacker gain physical control of our device(s). There are times when this is impossible to prevent. When crossing customs into another country you are at the mercy of the customs agency and they may demand to inspect your device as a condition for entry. You may be detained by police and forced to give up your device. Military personnel may be killed or incapacitated and lose their digital devices as a result. These are all extreme cases.

Most devices are lost under far more mundane circumstances. Most devices that are lost are the result of carelessness. Phones are forgotten sitting on bars or restaurant tables. Phones fall out of pockets onto the seats of buses and taxis. Unfortunately, there is no technical solution to this human problem. The solution is to be more mindful of where you leave your phone or iPod. You should be extremely careful about leaving it lying around in public. Physical security truly is the first line of defense against forensic attacks against your data-at-rest.

ENCRYPT APPS

Many applications offer passcode protection. This means that you must unlock the app, even after you have unlocked

the device. It also means that if anyone else should gain access to your device, they still have limited access to the information on it. We strongly recommend enabling individual device encryption anywhere it is possible.

PRIVACY SCREENS

Privacy screens are glass covers that protect your screen from scratches and from prying eyes. These screens make the content displayed on the screen difficult to see by someone peering at an angle. Privacy screens are inexpensive and available for most recent smartphones.

CAMERA COVERS

Because your device's camera is accessible via malicious software, you should protect it. We believe that the priority should go to the device's rear-facing camera. This is the one with the most consistent view of your face. The forward-facing camera will primarily only be able to see the inside of your pocket and things facing away from you. This still presents a threat of exposing your loved ones, the layout of your home, the type of car you drive, and other sensitive information.

For protecting the rear camera, we recommend simply covering it with a sticker. There are a number of stickers on Amazon.com that are designed to cover webcams. These stickers are typically covered with a very dark color, preventing light transfer. Against a bright background enough light may otherwise get through to allow the camera to "see" items of high contrast and silhouettes. These stickers also feature a non-marring adhesive that is easy to remove if you need the camera or wish to sell the device.

If you use your rear-facing camera a lot, you may choose a sliding camera cover. These covers attach directly to the screen and feature a moveable

element that can be slid over the camera when it is not in use, and easily slid out of the way when you wish to take a selfie. All of these solutions are inexpensive, costing just a few dollars for a sliding cover or a sheet of stickers.

MIC-LOC

One massive danger when using a traditional cell phone is that of the microphone being accessed remotely. Though we are emotionally much more concerned about the camera being accessed, accessing the mic would gain much more information than accessing the camera. This risk is so great that this is why the US Government does not allow cell phones inside Sensitive Compartmented Information Facilities (SCIFs) or within earshot of classified conversations.

A product on Amazon.com known as the Mic-Lock is a simply 3.5mm audio jack. It has a small resistor installed in it to mimic the line-load of a set of earbuds with inline mic. This tricks the phone into switching to an external mic instead. This is not a guarantee that your phone can't be tampered with because this still relies on iOS or Android software to determine which mic to use. We believe this is worth considering but we would still not rely on it to protect extraordinarily sensitive conversations.

FARADAY BAGS

Faraday bags are designed to block radio wave transmissions, to act as an insulator to protect against electronic currents, and to block tracking and hacking. Federal agencies and local law enforcement officers use them to protect information and evidence (cell phones or laptops) from being hacked and tampered with. Preppers use them as a precaution against an electromagnetic pulse (EMP) from a bomb or astrological event called a coronal mass ejection (CME). Simply put, the Faraday bag is an enclosure that prevents outside signals from communicating with your device. It is made with materials that block wireless signals from entering the bag, thus

protecting the integrity the contents from outside influences.

Silent Pocket offers Faraday sleeves in a variety of styles and sizes. Some are large enough to accommodate laptops while some are perfectly sized for a cell phone. When your device is placed inside, it instantly blocks all wireless signals to your device including cellular, GPS, Wi-Fi, Bluetooth, RFID, and NFC.

We have been using the Faraday sleeve at times when we want to be sure there is no digital trace of our movements or location...you know, when it's time to be off the grid for a while. A Faraday bag also ensures that our phone cannot be turned into a listening device by activating the microphone. As we have discussed, our strategy for cell phone use offers many enhancements to privacy and security already. Using a Faraday sleeve gives you even more control and peace of mind.

Oftentimes, people will put their phone into "Airplane Mode", which is a pretty reliable way to turn off wireless signals from reaching your phone. Two things to consider when using that practice. One, when you put your phone into Airplane Mode, your phone sends a signal to the network (technically referred to as an "IMSI Detach" that you have manually enabled this mode and the service from your phone drops off. When you turn off Airplane Mode, your phone again sends a signal that it is now reachable again, an "IMSI Attach". Also, even when your phone is in Airplane Mode it still receives GPS signals, which means applications can communicate with your phone and report your location. I have tested this, in Airplane Mode, while walking around the neighborhood. GPS signals report the route I take very accurately. Something to be aware of.

When you slide your phone into a faraday bag it drops all communication with the outside world but may take at least 30 seconds to do so. The nearest cell tower simply shows that your phone dropped service. Your phone is invisible while safely inside the Faraday bag, but it should be mentioned that the phone will continue to use battery life searching for a signal.

Many privacy enthusiasts (ourselves included) make a habit of putting their

phone inside a Faraday bag before we reach our residence. We rely on an iPod Touch (discussed in Chapter 5) for communications at home. With the cell phone inside a Faraday bag at home, it cannot be located or associated with our home address. Once we are a distance away from the house, the phone can be retrieved from the bag. This scenario may seem extreme to some. We believe it is extremely practical and should be employed by anyone seeking a high degree of privacy at home.

APPENDIX I: OUR COMSEC SUITES

DREW'S MOBILE DEVICE STRATEGY

Primary Device

Hardware: iPod Touch 6th Generation, 32 GB, iOS (latest)

Carrier: None (Wi-Fi Only)

Service Plan: None

Primary Secure Calling/Text: Wire

Secondary Secure Calling/Text: Signal

Miscellaneous Calls/Text: Sudo

Secure Personal Email: ProtonMail

Browsers: SnowHaze, Brave

VPN: PIA using OpenVPN

Password Manager: Mini KeePass

Connection Strategy: The anonymously purchased iPod is my primary communications device and only connects to trusted Wi-Fi networks through a VPN. It remains in airplane mode at all times with only Wi-Fi enabled.

Notes: The majority of people I communicate with also use Wire and their preferred encrypted method. Signal is used as a back-up secure channel to communicate, and also for out of band Wire contact verifications when needed. Anyone who has a traditional phone number for me (people and businesses) each have one of my nine Sudo numbers designated for that purpose. Occasionally, I carry an anonymously purchased Verizon MiFi device with pre-paid data service with me for times when I want to check messages between trusted Wi-Fi networks. That device remains powered off and inside of a faraday bag when not in use.

I do very little internet browsing on this device. Applications have been carefully scrutinized and removed to eliminate all but the essentials. All settings and permissions are maximized for their effect on privacy and

security, and carefully reviewed after each iOS update.

Secondary Device

Hardware: iPhone 7 128 GB **Operating System:** iOS 11.3
Carrier: None (SIM card removed) **Plan:** None (Wi-Fi only)
Primary Secure Calling/Text: Wire
Secondary Secure Calling/Text: None
Miscellaneous Calls/Text: Sudo
Secure Personal Email: ProtonMail
Browsers: SnowHaze, Brave
VPN: PIA using OpenVPN
Password Manager: Mini KeePass

Connection Strategy: This phone was purchased anonymously, remains powered off and inside of a faraday bag at all times. The only time this phone is for calling 911 in an emergency and during periodic charging of the battery.

Notes: A less expensive flip style phone would be ideal for this specific purpose. Again, all application permissions and privacy / security settings were carefully scrutinized during the device setup.

JUSTIN'S MOBILE DEVICE STRATEGY

Primary Device

Hardware: iPhone 6S, 64 GB, iOS (latest)
Carrier: AT&T
Service Plan: AT&T Prepaid, \$65 Unlimited Data (up to

22 GB unthrottled)

Primary Secure Calling/Text: Wire

Secondary Secure Calling/Text: Signal

Miscellaneous Calls/Text: Sudo

Secure Personal Email: ProtonMail

Browsers: SnowHaze, Brave

VPN (Primary): Windscribe

VPN (Secondary): Mullvad Using OpenVPN Connect

Password Manager: Mini KeePass

Secondary Device

Hardware: iPod Touch 6th Generation, 32 GB, iOS (latest)

Carrier: None

Service Plan: N/A

Primary Secure Calling/Text: Wire

Secondary Secure Calling/Text: Signal

Miscellaneous Calls/Text: Sudo

Secure Personal Email: ProtonMail

Browsers: SnowHaze, Brave

VPN (Primary): Windscribe

VPN (Secondary): Mullvad Using OpenVPN Connect

Password Manager: MiniKeePass

Connection Strategy/Notes: My strategy is based on my situation, and both of these devices are “primary” devices

depending on where I am located. If I am home, the iPod Touch takes the primary role. This device is the one I use in my house and around my city where I typically don't need mapping applications or a constant connection.

When traveling for work the iPhone takes over as the primary device.

APPENDIX II: RECOMMENDED APPS

Unless a third-party app offers some tangible benefit or capability, we generally recommend sticking with the native solution. Apps designed by Apple and Google are much more likely to be free of large vulnerabilities than third-party applications. For example, aftermarket podcast applications don't offer an appreciable privacy or security benefit over the native iOS Podcast app, and very possibly have the downside of sharing additional analytics data. For this reason, we prefer to stick with the native version.

In many cases there are applications that offer a major benefit over the stock apps on a phone. Below are some of our recommendations for replacements.

MAIL CLIENT

The native Apple Mail client does a great job and it allows you to connect multiple accounts at any given time. The bad news is that it also attempts to share information with a lot of other apps to more thoroughly “integrate” your email. We recommend two potential alternatives, or a combination of both depending on your needs. Each will require that you change your primary email provider, but both are much more private than mainstream email providers.

- **ProtonMail:** ProtonMail is our favorite email provider. All emails sent between ProtonMail users are end-to-end encrypted. All your mail is stored in a format that only you can decrypt, yet ProtonMail is still as user-friendly as the mainstream providers. Basic ProtonMail accounts are free, but their functionality is somewhat limited; a user is limited to

500 MB of inbox space. Premium accounts start at \$4/month and allow you to increase your mailbox size, use alternate email addresses, import custom domains, etc.

The ProtonMail mobile app (from iOS and Android) is an excellent replacement for the standard Apple Mail or Gmail apps. Data is encrypted on the device, and you can protect it with a PIN or passphrase. ProtonMail does not run any additional analytics software on the app. For more information and to sign up for a free account, visit <https://protonmail.com/>.

- **Fastmail:** Our second-best alternative is Fastmail. Fastmail is much more private than mainstream providers because they monetize directly. Fastmail does not scrape users' email or any other data for marketing purposes, offers unlimited email aliases, and custom domain support. Fastmail offers a suite of features including calendaring that is comparable to Gmail. Unfortunately, Fastmail does not offer default end-to-end encryption, but it is much more private. All Fastmail accounts are paid but they are very inexpensive, beginning at just \$3/month.

Like the ProtonMail app, the Fastmail mobile app is much more private than the default from Apple and Google.

NOTES

We both love the ability to take notes on our mobile devices. They have almost (but not quite) replaced the myriad notepads, journals, and stickie notes in our lives. Unfortunately, when you create a note on most applications, including Apple's built-in Notes app, much of what you write is shared or uploaded to the cloud. We do not like this.

- **Standard Notes:** Our preferred note-taking application is called Standard Notes. By default, Standard Notes encrypts all of your data. You can use the product in one of two ways. You can install the application on your device without setting up an account. This will

allow you to store your notes locally. If you set up an account, you can sync your notes across all your devices. Standard Notes offers native applications for Windows, Mac, Linux, iOS, and Android devices, as well as offering a web login. Standard Notes is completely free. For more information visit <https://standardnotes.org/>.

BROWSERS

The default browsers on iOS and Android devices leave much to be desired. Both are designed for user experience rather than privacy and security. We recommend you select an alternative browser to replace the stock Safari or Chrome on your device. There are numerous browsers that claim to be privacy- and security-oriented. In reality we have only found a select few that live up to most of the hype.

- **Brave:** Brave is an excellent browser that offers excellent privacy and security options. Brave allows you to block scripts, stop third-party tracking, block fingerprinting attempts, and block ads, all from a convenient drop-down menu. Currently we have serious concerns about using Brave on the iOS operating system. The WebRTC protocol can be used to leak your true IP address, even when using a VPN. We hope that Brave works to resolve this issue soon.
- **Snowhaze (iOS only):** Snowhaze is our favorite browser. Like Brave it offers the ability to block scripts, block ads, and browse in an “always private” mode that forgets history.

AUTHENTICATION MEASURES

Though it is somewhat counterintuitive, smartphones can be used to increase the security of your online accounts. Two-factor authentication applications can be used to store software tokens.

- **FreeOTP:** This is a completely free and open source implementation of

the Time-based One Time Password (TOTP) authentication system.

- **Authy:** Authy is a commercial alternative to FreeOTP. We like this option for several reasons. First, it is much more user-friendly than FreeOTP. It also allows the user the ability to passcode protect the application.

Your smartphone can also be used to store passwords in an encrypted state through password managers. Because we always recommend very long, very strong passwords for all online accounts, services, and local applications, a password manager is a necessity. Both of the password managers recommended here are compatible with the popular “.kdbx” database format used by KeePassXC, and other KeePass forks.

- **iOS:** MiniKeePass
- **Android:** KeePassDroid

APPENDIX III: FUTURE COMSEC SOLUTIONS

Purism Librem 5

Purism is a hardware manufacturer built on the ideology of “open source.” Purism began by manufacturing computers in the United States, with all proprietary code removed completely. Purism made a name for itself by leading the way in disabling Intel Management Engine, a software component included in all recent Intel processors. Intel Management Engine is an enterprise tool that allows Intel, the hardware owner, and potentially governments and hackers to access your computer below the operating system. Purism went a step further, adding hardware power switches to the camera and microphone and Bluetooth and Wi-Fi radios. After developing several highly secure computers, Purism turned its attention to smartphones.

The Purism phone, dubbed the Librem 5, is a completely open-source phone that runs PureOS, a Linux distribution. It is compatible with desktop Linux applications. Most importantly the Librem 5 will offer the ability to separate the phone’s baseband processor from its computer via a “baseband kill switch”. This switch puts the user back in control, allowing her to disable the baseband while still leaving the device completely functional on Wi-Fi. Like Purism’s computers, the Librem 5 phone will also offer kill switches for the Wi-Fi and Bluetooth radios and the camera and microphone.

There are a number of other benefits to the Purism phone. It offers a much-needed alternative to the current industry duopoly. Users are given control of what features, apps, and services the phone runs. The Librem 5 does not track its users by default, and Purism promises not to collect or sell user data. We cannot imagine a greater departure from current industry standards, and

anxiously await the release of the Librem 5. For more information visit https://puri.sm/_shop/librem-5/.

A communications solution like the one described by Purism for their Librem 5 phone may not appeal to everyone's needs. The hardcore privacy and security enthusiasts will likely be very excited about the list of benefits it offers. Both authors have committed financially to backing this project by pre-ordering a Librem 5 phone. The project exceeded its all-or-nothing initial fund-raising campaign and the phone is currently scheduled to ship to customers early 2019.

As our communications strategy evolves, we choose to embrace new ways circumvent surveillance efforts and secure our communications. Exactly how the Librem 5 may replace our existing set-ups remains to be explored; but we are very excited to see companies like Purism spearheading this important effort. No matter where your needs currently fall of the privacy and security spectrum, we encourage you keep an eye out for the “what's next” and ways to improve all aspects of your strategy

[1] In reality, the hacker could name the network the exact same name: #SANfreewifi. Devices that receive a stronger signal from the malicious AP will connect to it rather than the “real” Wi-Fi hotspot. This is also slightly riskier for the attacker, as the airport may be scanning for devices transmitting the same SSID. It may also have a lower probability of success as fewer devices may connect to the malicious hotspot, and those that do may not remain connected for very long.

[2] Intercepting data from “leaky” applications is a tactic that has been used by state surveillance actors for many years. This is another reason to carefully consider the applications to which you give close persistent access by installing them on your device.

[3] You may be concerned that your phone will not be covered under warranty if you do not provide personal information. In most US states a receipt is sufficient proof-of-purchase to validate warranty claims.

[4] Even if you decide not to use Privacy.com to pay your wireless bill, you should still consider opening an account with them. Privacy.com allows you to create virtual cards for every single merchant you have. Each card is tied to that merchant, and that merchant is the only party that is allowed make a charge to that card number. This means that if your credit card number is spilled it cannot be used by a malicious third-party.

[5] n-day vulnerabilities are those that have been discovered “n” number of days ago. Zero-day vulnerabilities are those that are still in the wild and have to yet been discovered by security researchers or antivirus authors.

[6] OpenVPN Connect, available for free in the App Store.

[7] Before placing any battery-operated device into storage, you should charge it, then drain the battery to 50%. This will ensure the longest possible battery life. Justin did not heed this advice. He stored an iPod Touch with a full charge for several months, only to find that it would not power on when he finally retrieved it.

[8] This is likely done to preserve the iPod’s already-limited battery life.

[9] Facebook, Google, and similar companies have both invested heavily on research into applied neuroscience to better understand - and exploit - how our brains respond to color.