The Cell Phone and Its Double

Anonymous

09/02/2024

Contents

Digital Doppleganger 3
The Burner Phone 4
What a Typical Week Might Look Like 4
A Story 4
Phones and Actions 4
Staying on the Move 5

Cellular phones are common targets for digital surveillance, along with all the software and applications they enable. These phones can be purchased anonymously — in person, in cash, with a covid mask and hat, and with a car parked far away — meaning only surveillance footage of the purchase is available once you walk out of the store. Yet, after purchasing these devices, we often bring them to houses, apartments, squats, camps, and hideouts. Cellular phones can be tracked using GPS or triangulation information from the cellular network provider, to determine your identity after purchase. Here we discuss a method to minimize the risk of unintentionally revealing your identity and location to law enforcement through use of a cellular phone.

Before getting to the main method, we recommend first reviewing digital security techniques described in prior zines, such as this one https://theanarchistlibrary.org/library/anonymous-how-and-why-to-use-a-burner-phone.

Among other things, we assume your phone's GPS and location history is turned off, private browsing is always used with all browsing data cleared upon closing the browser, emails or other information in the phone are not tied to government identity (except for limited cases with the civ phone), VPNs are always used, and TOR or VPNs are used when researching or sending communiques. Most importantly, you communicate on a need-to-know basis, using coded language, and never discuss sensitive topics near digital devices, buildings, or cars.

Digital Doppleganger

Ideally we would not interact with our government names at all, but in practice this becomes quite difficult. Our method is designed to handle the case when an individual must have some information related to their phone tied to their government name. For example, the person needs a phone to call a parole officer, bail bondsman, medical doctor, or do banking.

The idea is to have two phones, a civilian phone or ”civ phone”, that uses only Wi-Fi, and is limited in use to specific times and places away from the individual's place where they typically sleep (their dwelling) and any other digital signatures, including their other burner phone and phones of friends. The purpose of the civ phone is to allow you to make contact with untrustworthy entities, particularly entities that require your government name and related information. Banking, medical appointments, and untrustworthy family are common ones. The civ phone user might frame their periodic responses to family and government entities as daily or weekly or monthly ”check-ins.” The civ phone is purchased anonymously and only Wi-Fi calling is used, so you do not need a phone plan. Use Signal for texting and VPN whenever you can, just like a burner phone.

The important idea is to only use this phone at specific places and during specific times away from your other digital devices. This limits the ability of nefarious entities to track your location, particularly the location of your dwelling where they would love to wake you up in the early hours of the morning and put you in handcuffs. One might choose a single hour a week to check email that might be associated with your government identity, and make calls to family. Do this in a coffee shop, away from where you normally spend time. When you are not in the coffee shop for that hour, take the battery out of the civ phone and store it in a safe place, using a password and encryption.

The Burner Phone

The burner phone provides complementary functionality outside of your civilian life. The burner phone is only used to stay in touch with trusted friends using secure messaging apps like Signal, VPNs are always used, and TOR is used when appropriate. It is never associated with any entity, application, or device, that knows your government name. The burner phone must never be used near your civ phone, not physically or in time. The two phones should be separated by at least a half hour and several miles.

This strategy of separation protects the user by preventing the compromised civ phone from leaking information about the burner phone. Because the civ phone and burner phone are never in close proximity, law enforcement cannot make an association between them, and because the civ phone is never close to your dwelling, law enforcement can never associate your government name to your dwelling location.

What a Typical Week Might Look Like

A simple example shows what a typical week might look like for a user who only needs to use their civ phone for 2 one hour ”check-in” sessions per week. The user keeps their civ phone off most of the time, with the battery out. Only on Thursdays and Sundays does the user turn the phone on for about an hour, and this is only done at a coffee shop or library that are away from the user’s dwelling. During the rest of the time, the user has their burner phone on to communicate with trusted entities.

A Story

Imagine a location where there are two plots of land separated by a creek. On one side the user only uses their burner phone, which is only connected to an affinity group who are also using burner phones. Before crossing the creek, the user turns the burner phone off, and pulls the battery out of the phone. A bit past the creek, the user grabs their civ phone, which is turned off with its battery out and located in a secret stash spot. From there, the user bicycles to a local library wearing a mask and hat, puts the battery in the civ phone and turns it on, and uses the civ phone for calling family, dealing with banking and government-id-related email, among other things, but never for calling or texting the affinity group. The user does this once or twice a week, and more or less frequently depending on need.

Some improvements on this approach might be to: stash the turned off and battery removed burner phone on the other side of the creek in a very safe spot; change the location where the civ phone is used each time; come up with a method to decorrelate the on-off patterns of the two phones (although their on and off patterns are not perfectly correlated because the user waits a bit before turning on the civ phone, they are highly correlated).

Phones and Actions

It is very important to never bring civ phones or burner phones that you use for normal communication to actions. If you absolutely must use such a phone, never have any identifying or incriminating information on it, burn the phone after the action, and never bring it to the place where you normally dwell. You must not have a burner phone at your dwelling, then bring it to an action, then burn it; law enforcement can look at the phone's cellular network location history to pinpoint your dwelling. Any phone brought to an action must be a brand new clean burner phone that has never been near your civ phone, other burner phone, dwelling, or the devices and dwellings of friends.

Staying on the Move

If you do not provide law enforcement with your location information through your phone, you may be able to stay in one place. However, staying on the move, for example by hitching rides with friends, or anonymously through Greyhound or Amtrak or freight train, provides an extra layer of security, particularly when things get hot. Combining a nomadic lifestyle, without a formal government address (you're a homeless digital nomad!), with burning phones frequently and keeping civ phones away from burner phones, will make you very difficult to track.

Anonymous
The Cell Phone and Its Double
09/02/2024

https://unravel.noblogs.org/the-cell-phone-and-its-double/

theanarchistlibrary.org