This guide is dedicated to S.E.. Your heart for justice and reckless determination have been a source of inspiration on many occasions. Thank you for asking questions.

This guide serves as a reference for campers who want to keep their favorite spots a well-kept secret. The guide covers:

1. How to use End-to-End Encryption.
2. How to use VPN/ToR.
3. How to Organize with the Principle of Least Privilege.
4. How to Share Files with Overly Paranoid Encryption (OPE).
5. How Entities Collect Information about You.
6. Example Scenario

End-to-end Encryption

The important thing to know about End-to-end Encryption is that **both** parties need to be using the same service. For example, someone using Signal and another party using their cell phone SMS provider will not be End-to-end Encrypted. There are several service providers. My favorites are:

1) Signal: for messages

2) Proton Mail: for email

3) Both for highly sensitive information. We'll discuss this more later in Overly Paranoid Encryption.

End-to-end Encryption is a method of communication that prevents third parties from accessing data while in transit. It is not perfect security in itself. If a device used by one of the members is compromised it could expose the conversation to an adversary. This technology could be susceptible to advancements in quantum computing or any unknown technology that breaks encryption. My preference to maximize privacy would be to use a dedicated email/name to establish the accounts and treat the conversation as if it will be exposed eventually.

How to use VPN and ToR

Virtual Private Networks are a way of sharing private and secure network connections across the internet with an encrypted tunnel. Many businesses use this technology to allow for workers to operate remotely. It can also be used to pipe traffic to countries that have strong privacy laws like Switzerland. One of the most well regarded privacy VPNs is NordVPN which costs 3-5$ a month.

ToR is short for The Onion Router, it is a Free and Open-Source Software used for enabling anonymous communication. It works by bouncing traffic between servers such that not one server knows the entire route back to the origin. There is potential for this technology to be subverted if enough of the ToR servers are controlled by the same entity. The entry node is presented with your IP address (which can expose your location and/or identity), using a VPN first can be a better privacy practice.

If a communication is particularly sensitive, I might use VPN **before** ToR so that if a communication is traced through ToR, it would point to the VPN and need authorization from the hosting country to be accessed. This methodology can provide time which is critical in sensitive operations. Here is a guide from on how to use NordVPN with ToR: https://nordvpn.com/features/onion-over-vpn/

How to Organize with the Principle of Least Privilege

The Principle of Least Privilege states that a subject should be given only those privileges needed to complete the task. In the context of Operational Security, agents of the plan should only be given enough information to complete their part of the plan. Furthermore, the most critical information should only be made available when the time to operate is short. An agent might be told to go to an area at a specific time then only once arrived and confirmed clear would the meeting place and agent code-phrase(s) be delivered.

Time Sensitive Mission Brief:

Using short time-frames in the final stages of the plan can help to ensure that adversaries have as little time to react as possible. This can be critical to the success of an operation but it can be hard to arrange with the Principle of Least Privilege. There should be an expectation that using the highest security standard for communicating will take more time than traditional communications. I might use a code phrase on an End-to-end Encrypted channel to notify an agent to go into standby mode and confirm availability. Then once confirmation is received, communicate with a second agent to verify timing availability. If both checks are good it's time to send initial guidance which points to the when, where, and how of the general plan. Once agents are in place and confirming all clear, the final Short Term Mission Brief is sent with meeting location, code phrases, and a visual identifier (usually a worn garment per agent). The Time Sensitive Mission Brief should be sent with the Overly Paranoid Encryption (See section 4).

Code Phrases:
In the Time Sensitive Mission Brief, include phrases that would be used by average people in normal conversation associated with a secret meaning. These call and response codes can

be used to indicate if the meeting is safe to proceed without revealing a connection to observing parties.

In example, “I heard the weather is supposed to be nice next week.” could be an agreed upon phrase that both agents know. Then, if the response is, “I look forward to the sunny days.” it could mean that the mission is safe to continue but if the response is, “I hope it cools down soon.” that the mission is not safe and should be postponed.

Separate Duties:
The purpose of separating duties is to limit damage in case of a compromised agent. Agents should not know or retain Personally Identifiable Information about another agent to the best extent possible. This should also be true for details about missions such as timelines, locations, code phrases, and code names. By segmenting the knowledge and details of the operation you can limit the risk of a large-scale disruption.

How to Share Files with Overly Paranoid Encryption

Overly Paranoid Encryption is a procedural methodology designed to provide the highest standard of privacy and data integrity assurance. I wrote this methodology explicitly for this guide, and consider it my first meaningful contribution to the world of Information Security. The technologies and tools used will vary over time but the intent of the methodology is to default to the highest available standard of encryption and password complexity.

OPE Procedure:

1) Encrypt the target file with 7-Zip. The password on the encrypted file must be 99+ characters in length, contain upper, lower, numeric, special character, and be randomly generated by a Password Manager.
Follow this guide to save a file as an encrypted zip file:
https://www.boisestate.edu/oit-cybersecurity/how-to-use-7-zip-to-encrypt-files-and-folders/

2) Generate the SHA256 file hash (this is like the fingerprint of the file) of the encrypted file.
Follow this guide:
https://docs.hak5.org/general/general-articles/how-to-verify-the-sha256-checksum-of-a-downloaded-file

3) Send the **encrypted zip(.7z) file** over an End-to-end Encrypted channel like Proton Mail

4) Send the **password** to the zip file **and the SHA256 hash** of the file over a **different** End-to-end Encrypted channel like Signal.

5) The recipient verifies the SHA56 hash of the file is the same as in the second message **then** uses the password to access the file.

It is only when all of these steps are done with the highest available standard of encryption and password complexity that it can be considered Overly Paranoid Encryption.

How Entities Collect Information about You

Entities use a wide variety of Tactics, Techniques, and Procedures to collect information about a target system, group, or individual. This field is always changing and what works now in detection versus detection avoidance will adapt over time. This guide is meant to give a broad overview of some of the detection capabilities and the available counter strategies.

Data Presence:
The data you create by using technology leaves a trail across time. If an entity has a sufficient quantity of data they can make educated guesses about your social circle, behaviors, preferences, and ideological beliefs. Outliers from normal behavior could be used as an indicator for further analysis.

Counter this by reducing the data made available for collection by keeping your device in a Faraday Cage when not in use or during travel. A Faraday Cage is a container that blocks the transmission of electromagnetic signals like Wi-Fi and GPS.

Don’t use applications that collect or share your information (Social Media, etc.). Actively request that your information be deleted if you are granted this privacy right by law. Right now, the right to be forgotten is primarily described in European and Californian law, check your local state digital privacy laws. Turn off services when you are not using them like Wi-Fi/Mobile Data/GPS/NFC(Near-field Communication)/Bluetooth.

Visual Surveillance:
Visual surveillance is the practice of recording visual input from optic sensors. Cameras are the most common surveillance sensor but there are also sensors that detect motion, heat, and/or physical geometry. Visual information can be used to identify an individual by the characteristics of their face, scars, tattoos, and visually distinct body parts. There is some evidence that supports visual surveillance as a means of identifying an individual based on the characteristics of their walk.

Counter this by wearing a disguise, you can use makeup or, wear a face-mask, dark/reflective glasses, and hat. The objective is to obfuscate your usual visual appearance to the point that it is not recognizable in the new state. Any information presented to visual surveillance should be considered a potential indicator to identification.

Audible Surveillance:
Audible surveillance is the practice of recording audible information from sensors that collect sound. It is noteworthy that systems have been demonstrated that use lasers over long distances to read sound vibration from the glass of a window. This practice has had an increase in availability over the past decade with the mass adoption of smart devices. IoT and Smart Phones often come embedded with a microphone and who controls when they listen is not always up to the consumer. Audible information can also be used to identify individuals.

Counter this by having audible conversations in a space that is separated from all devices that have a microphone. In practice, set down the phones and go to the yard or another room that doesn't have any smart devices before speaking about the important stuff.

Forensic Evidence:
Cause and effect is the nature of our reality. Wherever you go and whatever you do there is a risk that the impact of your existence can serve as an indicator to your identity. Forensic identifiers can be biological like DNA and fingerprints, to almost anything like tire tracks and border crossing records.

Counter this if necessary by making an effort to contain or obfuscate your biological nature. Hair-net, gloves, bathing, anything that will reduce your identifiable impact on the world around you. In reality there is only so much you can do without leaving some evidence.

Example Scenario

Let's say a young woman named Alice needs a life saving medical procedure but her country has made it illegal for her to have life saving medical procedures. You find a list of doctors that would be willing to help and know two people in your local activist community who would be willing to drive. Let's put what we've learned from this guide into practice.

Alice has heard about your group and connects with you through Signal using the passphrase of the day that indicates which group point of contact the referral is from. You reach out to the doctor and make an appointment for Alice then confirm the day of meeting via Overly Paranoid Encryption.

You invite your two community contacts over at different times, you set your phones down in the living room then go to the backyard to discuss where and when to go to the city where the meeting takes place.

On the day of the appointment or the day before, activate the driver via the prearranged passphrase and issue a passphrase telling Alice to get ready to go to the meeting site one hour before (padded for travel time to the meeting site). When the driver arrives in Alice's home town it’s time to issue the Short Term Mission Brief (STMB) with Overly Paranoid Encryption.

Driver code-named Bob meets Alice at a bus stop and offers her a ride using the phrasing described in the STMB. Alice is wearing a disguise and responds with the all clear passphrase, having recognized the visual marker which is a pair of fuzzy dice on the rear view mirror. Bob drives Alice to the town where the doctor is located.

Bob drops off Alice and messages you with the passphrase associated with the drop position chosen. A new STMB is issued to the second driver code name Charles. Alice has the second passphrase from the first STMB which directed her to put her phone in a Faraday Cage and put it in Airplane Mode for the duration of the trip. Charles takes Alice to the doctors office and picks her up when the doctor is finished with the procedure. Charles drops Alice off to wait for Bob.

Finally you issue a STMBs for Bob with the pickup location. Bob takes Alice back to her hometown. Alice takes her device out of the Faraday Cage and hails a ride share app home.

By using two drivers you ensured that the agent with the knowledge of the doctors office was different from the agent who knew where Alice’s hometown is. Alice's disguise prevented visual surveillance from recording her presence and the Faraday Cage enabled her to use technology once back home.

I hope this example illustrates why I wrote this guide. Privacy is an important part of our lives and for some people it can mean the difference between life and death. I wish we didn’t live in a time that needed such a guide but here we are. All we can do is, give what we can, when we can, and hope it can do some good.