“Fuck the Feds” Security Guide v1.0

Why?

Well, that is question.

This is a response to the continued overreach of the federal government. Including certain three letter agencies such as the: CIA, NSA, FBI, etc.

There are basic ways you can protect yourself and your privacy online from state surveillance and prosecution.

Who is this for?

I am writing this from the perspective of someone has been the target of doxxing, coordinated surveillance, and law enforcement.

This guide is meant to be used as a general introduction to important aspects of online security.

You can freely distribute this document. It is a public work available to be edited and distributed.

Enjoy!

Contents:

DISCLAIMER: I AM NOT LIABLE FOR HOW YOU USE THIS DOCUMENT. THIS IS INTENDED AS A PRIVACY AND SECURITY GUIDE. DO NOT DO ILLEGAL STUFF AND THEN BLAME ME. THIS IS NOT A GUIDE TO EVADE LAW ENFORCEMENT.

About Law Enforcement (USA):

Right to remain silent:
Most Western countries have the concept of the right to remain silent. Essentially this is a right against self-incrimination. **USE IT**. 98% of people questioned in the United States do not invoke their right to remain silent because they think it will make them look more suspicious or law enforcement might “give a better deal”.

The simple fact is LAW ENFORCEMENT IS **NOT** YOUR FRIEND. They are building a case and anything you say can and will be used against you. Law enforcement in the United States can **legally lie to you**. If they promise a good deal or they will “go to bat” for you with the prosecutor it’s a fucking lie, unless you have a lawyer present to help you and a paper to sign do not believe it for a second.

How to invoke your right to remain silent:
In the United States it is not enough to say “I should have a lawyer”, “I don’t want to talk”, “I’m going to stay silent”. No, because the legal system is so messed up you have to specifically say something like “**I invoke my right to remain silent**.” (any good lawyer will just tell you to shut up if you ask for one). They likely WILL try to get you to talk even after this, so just don’t.

The only questions you should potentially ask:
1. Why am I here?
2. Am I being detained or under arrest?
3. (If no to both of the above) Am I free to leave?
4. (If yes to the above) LEAVE.

Biometrics are not safe from law enforcement. However, you can “forget” your password and remain silent, and your security devices can also “go missing” in an accident.

Passwords:

Passwords should be:

1. At least 12 characters
2. A mixture of uppercase and lowercase letters
3. A mixture of letters and numbers
4. At least one special character (#, ?, @, !)

Weak passwords consist of:

1. Words that can be found in a dictionary
2. A word with some of the letters replaced with numbers
3. Repeated sets of characters
4. A series of characters such as “qwerty”
5. Personal information like SSN, birthday, etc.

If you are storing sensitive information nobody else should ever have access to the password should be far longer (mine tend to be 30+ characters). You can remember multiple sets of smaller passwords and chain them together.

I tend to use passwords in the “Fort Knox” section at https://randomkeygen.com if not generating them from within a password manager like KeePassXC.
ex.]xH~g~@Z^8#L~XXHSUgY(O;Z=AaUes

DO NOT WRITE YOUR PASSWORDS DOWN! (unless it is to store in a remote location unknown to everyone else as a physical backup). If this is a master password or another important password DO NOT SAVE IT IN THE BROWSER.

Use a password manager like **KeePassXC** which is an open source password manager. The master password to this database should be 30+ characters following the guideline above and preferably other factors like Multi Factor Authentication. The database is encrypted with **AES-256**.

Multi Factor Authentication:

Authentication factors include the following:

1. Something you know:
   A password you know or remember.

2. Something you have:
   A hardware security device / token.

3. Something you are:
   Biometrics (NOT generally recommended unless it becomes an option AFTER using an above factor first.)

If you are using a password storage database (or even not) I recommend the use of a hardware security device such as a YubiKey or OnlyKey. This can be done easily by setting these devices in One Time Password Mode. Combine this with something you know, and now you have 2FA.

ONLYKEY
ONLYKEY
crp.to
▶ PASSWORD MANAGER
SECURE YOUR COMPUTER & ONLINE ACCOUNTS
▶ UNIVERSAL SECURITY KEY
▶ PORTABLE PHISHING-RESISTANT 2ND FACTOR

Secure Encrypted Storage:

YOUR SECURITY IS ONLY AS GOOD AS YOUR OS ENCRYPTION:
If you do not fully encrypt your operating system drive and or leave on your computer without shutting it off when you leave, even if the drive is fully encrypted, then you are making a mistake. Law enforcement and others could access your device when you are away and plant viruses, keyloggers, remote access software, or incriminating material to frame you. I find Linux LUKS to be decently trustworthy as a full disk encryption method.

VeraCrypt:
This program allows you to create encrypted volumes, or in the case of Windows you can also encrypt the entire OS.

https://www.veracrypt.fr/

If you have anything extremely sensitive use an encrypted storage container. You can set and change the master password (2FA recommended) and also choose the encryption algorithms and hashing algorithm.

Encryption algorithms: AES, Camellia, Kuznyechik, Serpent, Twofish, Cascades (I use Kuznyechik-Serpent-Camellia. Each cipher in the cascade uses its own key, and all keys are mutually independent).

Hash algorithms (recommended): SHA-512, Whirlpool (I use Whirlpool).

Plausible deniability:
1. Hidden volumes (one password for real data, another for real data).

2. Until decrypted, VeraCrypt volumes have **no signature**. This means it cannot be proven your container is a VeraCrypt container.

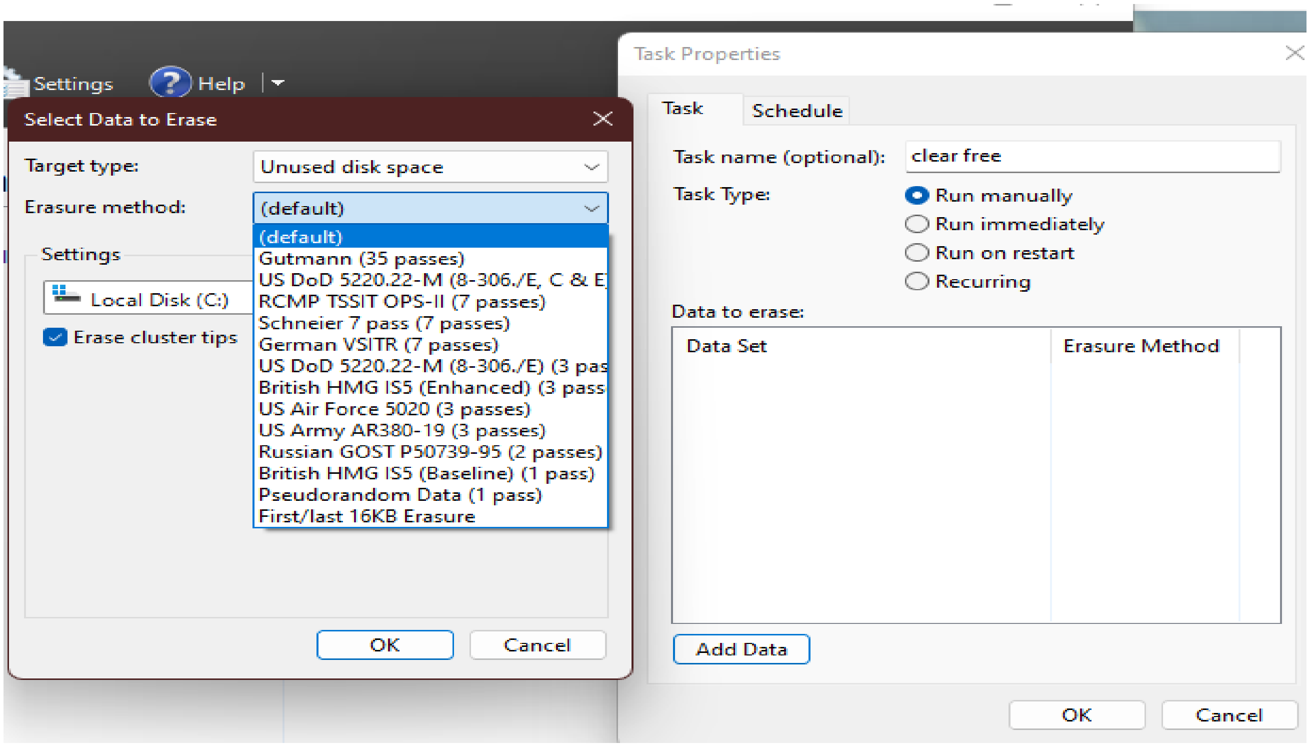
Secure Storage and Free Space Erasing:

At this point you should be using some kind of encrypted file system or container which was described above for desktops and laptops.

Simple deletion does not work:
If a file at any point touches your hard drive without it being encrypted, and you delete that file, IT IS NOT ACTUALLY GONE. The data is still **100% fully retrievable** which will be taken advantage.

If you are going to delete a sensitive file, or moved it to an encrypted device or volume but at one point it touched your unencrypted drive, use a free space eraser or secure eraser tool.

A popular tool for this job on windows is Eraser. https://eraser.heidi.ie/
By overwriting the free space of the drive you are making it FAR harder to ever retrieve that deleted information.



Select Data to Erase

Target type: Unused disk space

Erasure method: (default)

Settings

Local Disk (C:)

☑ Erase cluster tips

Task Properties

Task name (optional): clear free

Task Type: ● Run manually ○ Run immediately ○ Run on restart ○ Recurring

Data to erase:

Data Set	Erasure Method

Settings
Help
(default)
Gutmann (35 passes)
US DoD 5220.22-M (8-306./E, C & E
RCMP TSSIT OPS-II (7 passes)
Schneier 7 pass (7 passes)
German VSITR (7 passes)
US DoD 5220.22-M (8-306./E) (3 pas
British HMG IS5 (Enhanced) (3 pass
US Air Force 5020 (3 passes)
US Army AR380-19 (3 passes)
Russian GOST P50739-95 (2 passes)
British HMG IS5 (Baseline) (1 pass)
Pseudorandom Data (1 pass)
First/last 16KB Erasure
OK
Cancel
Task
Schedule
Add Data
OK
Cancel

Mobile Secure OS, Storage and Free Space Erasing:

If you use iPhone: don't store sensitive material on that ever, if law enforcement is motivated enough they will get into it and it is not a secure device in my opinion.

If you use Android there is significantly more you can do:

1. If you can root the device:
The golden standard in my opinion currently is getting an unlocked Google Pixel 6, rooting the phone, and installing GrapheneOS which sandboxes apps and permissions, and uses secure memory allocation stopping essentially all common attacks. Another good privacy OS is CalyxOS.

If you do not have a Pixel then the recommendation is LineageOS. While it does not come completely configured for privacy out of the box, you can follow some online guides and turn it into a highly secure OS.

If you cannot root the device the rest of this advice will likely still be fine, however you are more vulnerable to being spied on by having your phone become compromised or backdoored.

2. Use an extra layer of encryption:
DroidFS is a tool to create encrypted volumes inside of Android with its own built-in file explorer. You can use the stream ciphers AES-GCM or XChaCha20 (I recommend XChaCha20). This makes it extremely fast without sacrificing too much security. It will not protect you from screen recorders, keyloggers, compromised root, or memory dumps. Stay away from unsafe features.

3. Use Extripater to overwrite free space:
If anything sensitive ever touches anything outside of DroidFS, use an app like Extripater (configured to SecureRandom in settings!) to wipe free space.

Secure Social Media and Communications:

If you are sharing sensitive information over platforms like Discord, Twitter, Facebook, etc. STOP for the love of god. All of that can be easily subpoenaed by law enforcement. These platforms have data retention policies that will keep any photos, files, or texts you post for up to 90 days or more.

Secure apps courtesy of this **FBI document**:
https://therecord.media/fbi-document-shows-what-data-can-be-obtained-from-encrypted-messaging-apps/

qTox**:**
***Fully encrypted and user friendly by default.**

Signal**:**
***No message content.**
***Date and time a user registered.**
***Last date of a user's connectivity to the service.**

Telegram:
***No message content.**
*No contact information provided for law enforcement to pursue a court order. As per Telegram's privacy statement, for confirmed terrorist investigations, Telegram may disclose IP and phone number to relevant authorities.

Threema:
***No message content**.
*Hash of phone number and email address, if provided by user.
*Push Token, if push service is used.
*Public Key
*Date (no time) of Threema ID creation + Date (no time) of last login.

Matrix:
***No message content** (end to end encrypted by default)
*Metadata risk

VPNs or TOR or I2P:

Personally I always use a VPN to conceal my IP. However I am not hiding from the federal government or doing anything strictly illegal so I do not take more serious precautions others might. I use ProtonVPN and Proton Mail. I do not recommend using ProtonMail besides on a throwaway basis depending on what you are doing. Using free public WiFi is a good way of not being able to tie internet traffic back to you.

If you use a debit or credit card to purchase a VPN, that information is likely stored and with that information the government can monitor you

If you want to buy an anonymous VPN, use **Monero** cryptocurrency.

Also if you ever connect a VPN to your home internet, you have automatically lost some privacy in most cases.

VPNs that are reliable and accept Monero as payment:

1. iVPN
2. cryptostorm
3. Mullvad

TOR and I2P are fundamentally different from a VPN. A VPN is somewhat of a centralized entity, and your data is tunneled through that entity. TOR and I2P are decentralized networks operated by volunteers that provide anonymity and access to hidden services (referred to as the dark web).

TOR:
TOR is more mature and larger, focuses on accessing the clearnet anonymously and hidden services secondary.

I2P:
Far higher security threshold and not as exploitable, no central directory servers, focuses on hidden services primarily and clearnet secondarily.

Further Advice:

Depending on your situation there are a few routes you should be aware of.

If you are fully doxxed consider going to a state where you can get a sealed name change and do so, or change your name when heat dies down in roughly ~6 months or less when people get bored. Using that new name should be done with new accounts, and a new phone number (like a burner)

Do not say anything incriminating or stupid:
Are you being accused of being a pedo, grooming, or other acts? You are truly shooting yourself in the foot if you ever make an **admission** to anything of the sort. Admissions and confessions are golden standards for law enforcement and also the hate mob.

Let the idiots continue to throw a fit:
Let stupid people whine and cry about you, doctor screenshots and falsify evidence, run around with their heads cut off with conflicting doxxes and evidence reporting to law enforcement. The longer this goes on, the less there is a chance of any serious investigation and people ruining any kind of evidence if it does exist.

Screenshots do not equal guilt:
For this to have any weight at all law enforcement will need to subpoena the social media provider for information. If this information is deleted or unavailable, screenshots are absolutely meaningless. Even archives can be doctored, but is much better than screenshots. Luckily most people are too stupid to realize that.

Disappear for awhile:
People tend to get bored after a few months of you being quiet, and by the 6 month mark people usually completely forget who you are anyway.