Digital copies available here.


good trouble,
necessary trouble

# Digital Defense for Mischief Makers

Practical tips and tricks for humans in a hyper-connected world.

Take a gander inside for easy, everyday things you can do to protect yourself while you stick it to The Man.

- Protect your data from search.
- Prepare your phone for a protest.
- Use encrypted messaging apps.
- Scrub your photos of metadata.
- Hide your network traffic.
- Make a fashionable tinfoil hat.
- and Keep safe from space lasers.

**Spring 2025**

## Post-Protest Clean-Up

Had fun did you? Time to clean up and get back to looking like a productive member of society? Here are a few things you can do to make sure you keep everyone safe.

If you're using disposable devices, transfer everything you need from them, then perform a "factory reset" which puts everything back to how it was when you first purchased the device. (Every device is different so you'll have to search for the instructions.)

Then, either recycle or donate the device. Note that all modern devices have permanent hardware serial numbers, and may be traceable back to you.

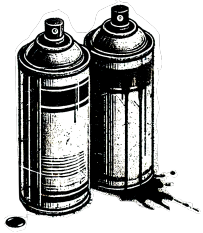
Is the person in your photo safe if you publish it now?

If you're going to share or post media from the event, make sure to scrub the metadata from images and files. It's also important to consider the privacy and consent of the people who appear in your shots.

Remember to remove SIM cards and memory cards before donating electronics.

Do you have automatic "cloud backup" or "cloud sync" enabled? Better check for evidence online, too.

It's useful to look around and make sure you're comfortable with your own digital exposure. It's okay to ask allies to remove or blur media that might be used against you.



Know what other mischievous MFers love a protest? Quakers.

Long before blogs and tweets, text messages and airdrops, there was the zine. This grungy little handbook is a love letter to the past, and a heads-up to the present. It's pure information in a cheap-ass format, and it wants to be free. Pass it along, copy it, scan it, remix it, or try to ban it. Freedom of the press is guaranteed to those who own one, and now that all the presses seem to be owned by billionaires, we're going to have to take things into our own hands.

Times are tough for troublemakers. A sprawling surveillance apparatus has been erected in the interest of commerce and propaganda, and it seems to be wired into every facet of our daily lives. You're not paranoid if they're actually after you ... and these days it's hard to tell.

Whether you're a high-profile dissident, or just a garden variety rabble-rouser, there are things you can do to minimize the information that's collected on you and on the people you associate with. It can and will be used against you. Even folks with "nothing to hide" have friends who aren't so fortunate. Particularly now. Do the polite thing -- take a few precautions for the safety of everyone involved..

****

- Buttons the Gnome
  Spring 2025

# Understanding your digital footprint

Our modern, connected lifestyles produce an endless "data exhaust" from the interactions we have with online services. This information is correlated, packaged, and sold to the highest bidder.

Personal data is worth big money, so once it's collected, it's usually saved forever.

Every time you access a website or use a network-connected app -- **even if you're not logged in and are browsing incognito** -- the operator knows at least:

- Your device's unique network "IP" address
- Your network provider's name
- Your approximate location (from IP address)
- Your device's manufacturer
- The pages you view and interact with
- The browser/app version
- A rough unique "fingerprint" of your device from the combination of these and other facts.

By correlating these data points, it's possible to deduce that you were/are in a certain place at a certain time.

Do you trust the maker of that application you're about to install?

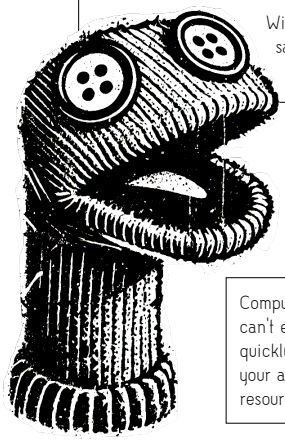
Check out the Electronic Frontier Foundation's Panopticlick to see how easy you are to track.

# Getting AI to Replace You

Oh for Fnaard's sake, really!? You want me to put a whole page in here on AI? Though come to think of it, it's a useful time-saver for everyday tasks. Maybe we can do something.

AI is fantastic at making stuff up. If you're creating fake profiles it's incredibly easy to just ask an AI to generate an image of a person matching an arbitrary description. While you're at it, have it write your profile and bio, too.

With all that spare time you just saved, you can afford to set up a dozen alternate profiles!



Caveat simulator: everything you type into a ChatBot is logged and may be used against you.

Note: most AI-generated images are easily detected.

Computers will believe anything you tell them and can't easily discern truth from fiction. Use AI to quickly generate plausible noise that can obscure your actual activities and make surveillance more resource-intensive for your adversaries.

Have you asked AI to summarize you to yourself? Know what the machine sees!

Ask AI to help you target your posts to your target audience. Brainstorm!

But, sometimes the best digital "hack" is to go analog. Meet in person, build real trust, and know when to put the devices away. No AI can replace genuine human connection and solidarity. That's still your most powerful tool for mischief and change.

# Preflight for Protests

Attending a social gathering where there's a possibility that your devices will be seized? Here are some things you can do to improve your odds of not getting compromised.

Disable biometric login, just to be safe. You cannot be compelled (legally) to provide your password, but you *can* be compelled to provide your fingerprint or face to unlock your device.

Authorities use "stingray" devices to log all powered-up cellphones in an area.

Practice quickly shutting down your device. It's safest from authorities' hacking when it's powered down, or right after it has started back up. Most hacking attempts require a phone to be powered up and have been logged into at least once since start-up.

Even a powered-down device can send beacons that reveal its presence nearby.

Write down important contact information and keep it handy in case you need to call a friend, but don't want to unlock your device in order to get their number

Consider using a pre-paid or "burner" phone that can't be tied to you.

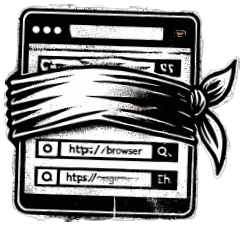
You might want to disable full-text notifications on your lock screen.

A "faraday bag" will make it impossible for any wireless communication to reach your device, preventing all communication and tracking. In a pinch, a microwave oven also blocks all radio signals ... just make sure not to turn it on!

Cash is less traceable than plastic.

# Incognito Browsing

While **private browser** windows provide some protection against people seeing your browsing history, or sites setting long-lasting cookies to track you between sessions, they don't keep sites from logging your access and activities. They're useful, but not as private as you might think.




Starting an incognito browser window begins with a cookie-less session, but site operators will quickly re-populate your cache. If you don't shut *all* of the private windows, those cookies will persist.

Did you really think a browser created by the largest ad-serving company on the planet was going to just ignore where you're going in that window?

If you log in to any services, your browsing is now completely traceable to you. Even with a VPN masking your network location, your browser has a fairly unique fingerprint based on things like plug-ins and fonts available, screen size, keyboard language, &c

That's the best stuff!

For maximum security, log out of websites when you're done with them.

Consider using a privacy-enhancing browser like Safari or Brave. Or install a plug-in to block or curtail cookies from shady tracking sites.

Be sure to kill off *all* private windows after a session, to clear cookies and history.

Chrome or Firefox users might consider the EFF's Privacy Badger extension

# Virtual Private Networks

A **VPN** will let you hide your traffic from the local network provider (e.g. a coffee house or library) and can help you appear to be coming from a different geographical spot.

VPNs function by encrypting all the traffic coming from your device and sending it to a server in another location, where it's *then* sent on to its final destination. It stops prying eyes between you and the VPN provider's servers, but not beyond that on the internet at large. Your digital footprint is still visible to sites and services. Anyone who promises more than that is selling something.

Apps that share your location are unlikely to be fooled, and will probably report your exact location just fine

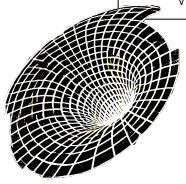
They have access to your GPS..

Buyer beware: don't trust overblown claims of perfect security or anonymity. VPNs can be useful, but aren't a silver bullet.

If you don't trust the local network you're on, a VPN will keep your local provider from divulging the sites and services you've visited. Internet providers must comply with subpoenas of this information, and many straight-up sell it to data brokers.

The Consumer Reports review of VPN providers is a good starting point.

When you use a VPN, it's usually obvious to anyone trying to snoop on your traffic. Be aware that many sites will refuse to create new accounts for you, or will decline credit card use, when they detect that you are on a VPN.

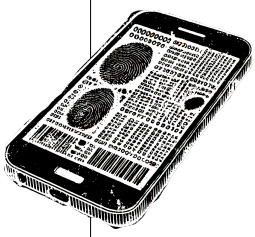


Try the EFF's detailed explainer on VPNs.

**More intrusive** apps and websites also know:

- The other sites you've visited recently
- Your search history
- Your exact location (GPS) and history
- Your contacts' names and details
- Other installed applications
- Keyboard typing patterns
- Battery charge level and screen brightness

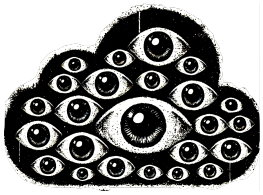
These are most often used to target advertising, and are frequently sold to third-parties. Governments, companies, and individuals can easily purchase these datasets without any legal oversight.



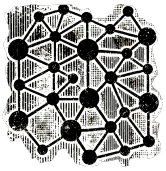
Free games and apps often make their money by selling your info.

**Data brokers** tout their ability to infer your:

- Income and financial status
- Education level and occupation
- Political and religious affiliation
- Associates and coworkers
- Health conditions and concerns
- Risk tolerance
- Daily patterns and rituals



You may only be sharing a few small details with each site or app, but they pass these along to aggregators who can form remarkably detailed pictures of you and your associates from the composite of all the data points.



Prepare a personal strategy with Consumer Reports' Security Planner.

Curious what's in an image? Check out They See Your Photos to get an analysis of what an advertiser can glean about you from a photo.

# Risk vs. reality

Before you put on that tinfoil hat, take a moment to realistically assess your situation. Sure, those space lasers are lethal, but are they actually aimed at *you*?

air mail / par avion

Security comes at a cost. It's essential to match your efforts with the true value of the information at risk. There's no sense spending more effort protecting something than it would cost you if you lost it.

- How sensitive is this really?
- What are the actual consequences of exposure?
- Could heightened security actually *draw* attention?

They're less likely to break your encryption than they are to break you. (xkcd)

When you first realize the unbelievable resources that can be brought to bear on surveilling you, it's easy to think that those resources *will* be brought to bear. The reality is:

- Mass digital surveillance makes it hard to target individuals
- Bureaucracy foils most attempts at speed

Organizations are much more likely to:

- Exploit human relationships/ trust
- Employ physical surveillance
- Use legal pressure
- Threaten your job/ acquaintances
- Make your life difficult

Try the EFF's surveillance self-defense project

# Identifying critical assets

You have ten minutes to save or delete as much of your digital existence as you can. What would you save? What would you make sure to delete?

Plan ahead by making a list of essential digital assets. What do you have that fits in one of these categories:

- Hard/impossible to replace if destroyed
- Difficult to access if you don't have a network
- On a device that might be seized
- Critical for maintaining access/identity

Make sure you have a physical or digital copy of these items in a safe and secure location. Keep your backup in a separate location from the originals! Make sure to encrypt (not just password protect) sensitive data.

I don't have any good online resources to link to so here is a video of some baby goats running around and jumping on stuff.

Now flip it. Imagine the goons are at the door and you have just minutes to delete your most sensitive data. What can be used to:

- Track your location, activity, and identity
- Provide unauthorized access to accounts
- Reveal patterns and relationships

Can you simply delete the data now? If not, have you encrypted it? It's essential to know ahead of time what to destroy fast. (It's why shady accounting firms have big shredders.)



# Hidden Metadata

**Metadata** is data *about* your data. If you think of data as a message's contents, or a photo's image, the *metadata* on it is the sender, photographer, camera, application, and other peripheral information about it.

Digital photos often have highly detailed metadata attached to them. (Usually as "EXIF" data.) The metadata can betray the time and date the photo was taken as well as details about the camera or phone, and likely also include the GPS coordinates.

Before you share an image, ensure that the application you're using will strip the metadata, or do it yourself. (Or get clever and add fake data!)

Be careful to scrub metadata before sending documents.

Even if your phone is not tapped, agencies have access to call metadata, which includes who talked to whom, for how long, and additional details such as which cellular towers you were closest to, which can be used to infer your rough location. These data are automatically collected by carriers no matter who you are. (Necessary for billing purposes.)

See an image's metadata with jimpl.

Most digital documents have metadata attached, which can indicate the original authors, time of modification, and even the whole history of the changes to the contents!

Some spectacular leaks have happened due to metadata. Look it up!

# Basic Hygiene

There are simple, low-effort, everyday things you can do to protect your data from getting hacked or falling into the wrong hands.

Most hacks happen against out-of-date devices and software. Enable **auto-update** and **apply patches** as soon as they're available.

Don't backup or save sensitive files to "the cloud" unless they are encrypted. These files are out of your control and can be easily leaked or subpoenaed.


Deleting files doesn't necessarily destroy them, it simply marks the space as being reusable. The data is not gone until something else is written over it. Those deleted files can be recovered in many cases.

Best to destroy old storage devices to make sure they're unusable

*Password protected" files aren't necessarily encrypted. Double-check it's encrypted.

Use **unique passwords** for all of your accounts, especially your **primary email**, so that the breach of one system doesn't automatically lead to the breach of others.

Enable two-factor authentication any time it's offered to you.

It's sensible to use a password manager to keep track of all your unique passwords. Most can also generate strong passwords for you.

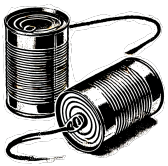
Make sure to back up your password manager's database, or have it synchronize across multiple devices, for safekeeping. You don't want to get locked out, so consider sharing your master password securely with someone you *really* trust.

Here's a good primer on encryption for you.

# Encrypted Messaging

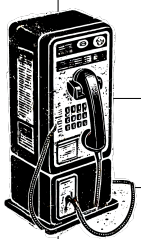
While most internet traffic these days is encrypted between you and the server, your data is still readable by the organization that's providing the service. Most messaging can be read by companies and governments.

**End-to-end encrypted** messaging overcomes the "man in the middle" problem by encrypting your messages such that they are only readable by the recipient, not the server that's relaying them. Simply "encrypted" is not enough, it needs to be "end-to-end" encrypted.



Unless you own the network and servers. There's a potential for snooping.

If you use **vanishing** or **disappearing messages**, you'll add a layer of protection against device seizure. Authorities can't read messages that have already deleted themselves.



When sending email, imagine you're sending a postcard. Anyone who handles it can read it.

**Email** is trickier, and unfortunately not easy to implement. You can, however, go with a provider who will try to hide your identity, even if your messages are vulnerable to interception.

For instant messaging, there's nothing better than Signal. You'll be surprised how many of your friends are already on it.