Digital Privacy, Security, & Data Hygiene

Daly Barnett *(she/her)*

The leading nonprofit defending digital privacy, free speech, and innovation

What's Here, What's Not

IN: Basic terminology, concepts, threat modeling, safety techniques, where-to-go-next

OUT: Deep technical analysis, product recommendations, security cure-alls,

Intro to Threat Modeling

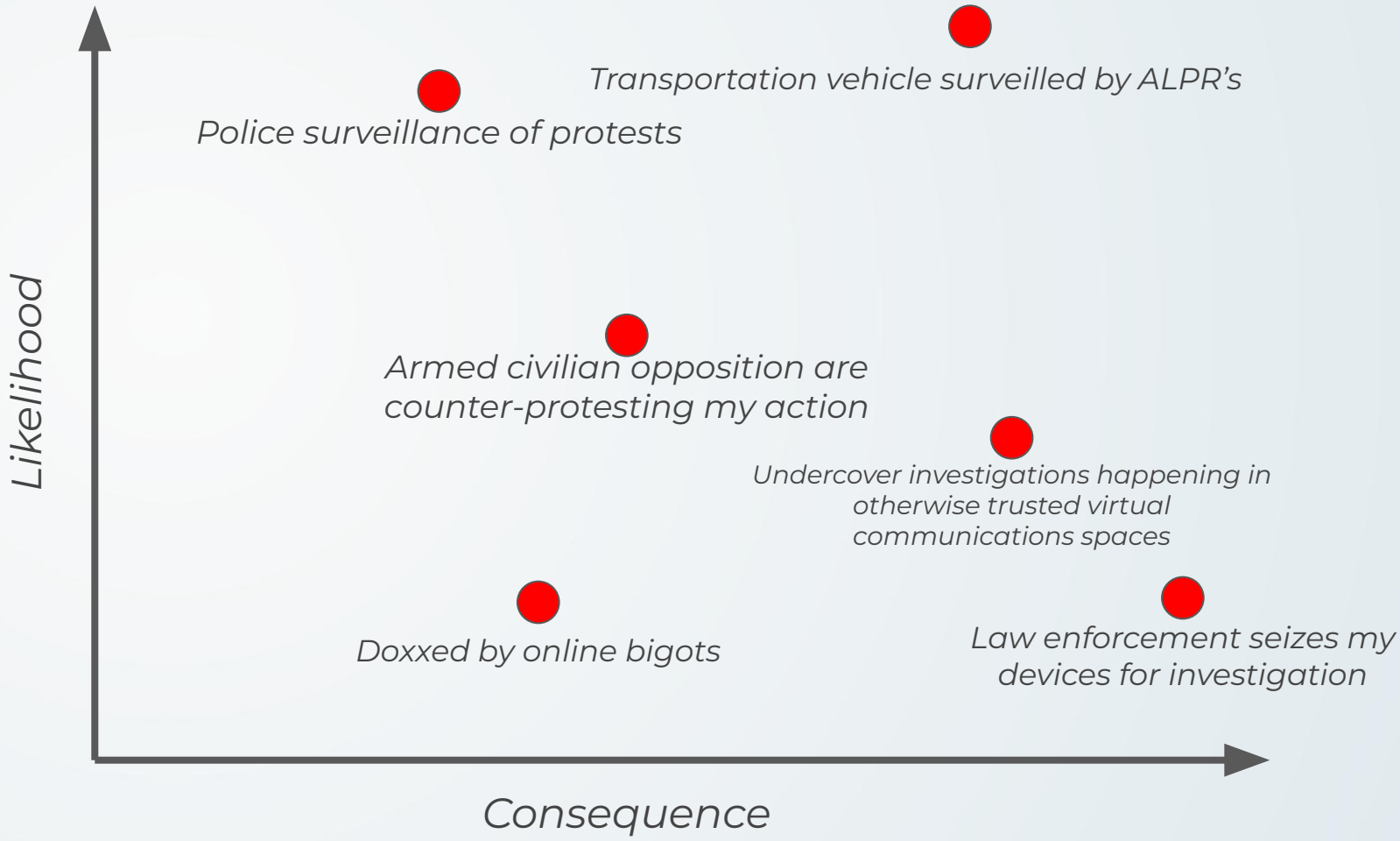
Threat modeling is a loose methodology of brainstorming your individual security point-of-view. The point is to identify and then prioritize the potential security risks that you face.

What do I want to protect?
Who do I want to protect that from?
How bad are the consequences if I fail?
How likely are those consequences?
How much trouble am I willing to go through to prevent that?
Who are my allies?

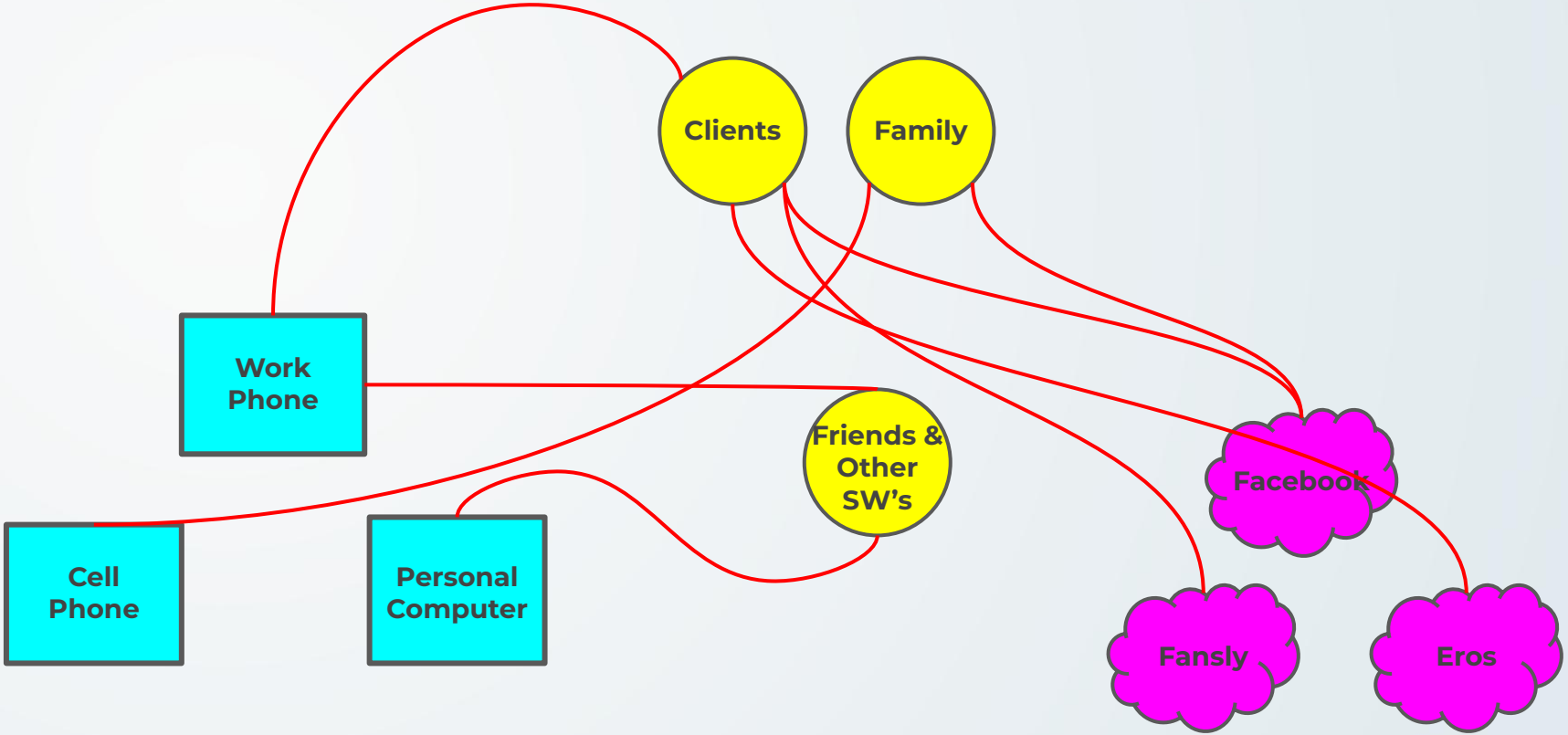
EFF

List answers to these six questions:

What do I want to protect?
Who do I want to protect that from?
How bad are the consequences if I fail?
How likely are those consequences?
How much trouble am I willing to go through to prevent that?
Who are my allies?


Likelihood
Consequence
Police surveillance of protests
Transportation vehicle surveilled by ALPR's
Armed civilian opposition are counter-protesting my action
Undercover investigations happening in otherwise trusted virtual communications spaces
Doxxed by online bigots
Law enforcement seizes my devices for investigation

- Data footprint mapping



Common Threats

- Abusive clients
- Law enforcement raids & seizing of digital devices
- Digital platform collaboration with law enforcement
- Street-level surveillance
- Weaponization of public records & open-source intelligence
- Platform shutdowns
- Financial censorship
- Information leakage from work life to civvie life

Doxxing

Weaponization of open-source intelligence & public records to lead to further harms (stalking, SWATing, networked harassment, and more)

Doxxing

Weaponization of open-source intelligence & public records to lead to further harms (stalking, SWATing, networked harassment, and more)

In Nevada, voter records are by default made public, meaning that if you are registered to vote in Nevada it is likely that your legal name, address, and other information are available online.

Doxxing

If you are a registered business owner, your business registration information is made public, including registrant address, name, and more.

As an individual worker, your name, address, SSN, and more are not available via public records requests unless you are criminally charged, then those court records may be public.

Other OSINT

Use any kind of investigatory tools at your disposal to locate areas of the Internet where information about you exists. Mark those areas as either places where you need to appeal to have that information taken offline, or if that's beyond your control, areas/types of information to keep note of in case they are weaponized against you in the future.

Other OSINT

Start with Google. Branch out to other search engines.

OSINTFramework.com for a suite of tools that are used for investigatory work.

Public records like business registration, voter registration, court records, and the like.

Other OSINT

- Username search engines
  - https://namechk.com/ & https://www.namecheckr.com/
- Breached account databases
  - https://haveibeenpwned.com/ & https://dehashed.com/
- Person verification / reverse address lookup
  - https://thatsthem.com

Scraping Tools & PimEyes

Web scraping tools are automatic bots that regularly copy, store, and share online sex worker profiles. Sometimes they're commercial tools, sometimes law enforcement, sometimes both.

PimEyes is one example of the convergence of scraping and AI – it uses sophisticated facial recognition algorithms to match images to faces all across the web. It's purportedly made for privacy and research purposes, but of course, it's commonly used for abuse.

Scraping Tools & PimEyes

Protecting against these threats is difficult because once you share data with a platform, it is then usually owned by that platform and copied, shared, distributed elsewhere.

Use PimEyes to determine where sensitive data might exist, try to get those things taken down, and at least mark them as potential areas of risk.

Setting Community Data Sharing Standards

Set rules for your social groups about how data can be shared.

You can do this for yourself, if insider threat is a possibility.

You can also do this with trusted groups that share the same privacy and security concerns.

Push a culture of consent when it comes to sharing data about one another. Get used to checking with each other before sharing names, pictures, or any other data about one another.

Multiple Browsers

Browsers are free so use multiple for different use cases. Consider the tradeoff between privacy, convenience, and security.

Some, like Chrome, might be convenient and easy to use, but the tradeoff is at the expense of your privacy.

Firefox is a good middle of the road option and offers thorough privacy and security settings that you can manually go in and harden yourself.

Tor is a good option for utmost privacy, but will be less convenient for more casual browsing activity.

Passwords and Password Managers

Always use long, unique, and random passwords for every single account that you access.

You can use a dice and wordlist to generate long unique and randomly chosen phrases to do so. Or you can generate them with a password manager.

Passwords and Password Managers

Password managers are databases of passwords that you control and access via a single main password. They often sync across devices, can be compartmentalized into vaults that you can share with others, and can be chosen specifically to never go online if that is within your threat model.

Bitwarden is a good free and open source option. KeePassX is a good option for one that lives entirely on your device without any need to go online.

Multi Factor Authentication

Turn on 2FA on every account you log into online. Instead of regular SMS or text message options, go for ones that are authenticated using an app like Authy, Google Authenticator, or others.

For a more secure & physical option, as long as you don't lose it, is a Yubikey.

Encrypted Messaging

Keep end to end encrypted messaging apps available for communications with others that require higher privacy.

Signal is a good option for phone and desktop because it's easy to use, is open source (and therefore vetted by the privacy developer community), and is free. Turn on disappearing messages!

Keep in mind that when you communicate with others they can still screenshot and share elsewhere.

Mobile Security

Be mindful of how your phone is sensitive to tracking at most times, to various types of tech.

Location and ID tracking:

Phone towers are constantly picking up on your phone's ID.

Law enforcement in your area (especially where protests are happening) may have "IMSI Catchers" - a phone tower spoof made just to capture your phone's ID.

Devices for radio-wave signals like WiFi and Bluetooth are also capable of learning your phone's ID and storing that information.

Mobile Security

Phone app behavioral data tracking:

Do a careful review of all the permissions that different apps on your phone are using. Turn off any unnecessary ones, and any that are necessary, see about limiting when they are active.

Mobile Security

Turn off Ad identifiers on your phone!

Knowing When To Turn Things Off or Leave Them At Home

As much as you need to know when to have hardened privacy and security on your devices and how you use them, it's important to know when it's better to leave them off, or away from where you are going.

One consideration is your local laws, how law enforcement often deals with seizing and inspecting devices.

You can also simply just be mindful of turning off phone and other devices location services, cell service, internet connection, etc.

Conclusion

Remember that good privacy and security can only be reached with a multilayered approach.

There is no perfect security, though, and the best you can do is sense when you need to put in good OPSEC to keep yourself safe.

SURVEILLANCE SELF-DEFENSE

TIPS, TOOLS AND HOW-TOS FOR SAFER ONLINE COMMUNICATIONS

A PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION

We're the Electronic Frontier Foundation, an independent non-profit working to protect online privacy for over thirty years. This is Surveillance Self-Defense: our expert guide to protecting you and your friends from online spying.

Read the BASICS to find out how online surveillance works. Dive into our TOOL GUIDES for instructions to installing our pick of the best, most secure applications. We have more detailed information in our FURTHER LEARNING sections. If you'd like a guided tour, look for our list of common SECURITY SCENARIOS.