



# Digital Privacy

counter surveillance tactics in the  
age of SESTA/FOSTA

Every t4tech event, online platform, organizing space, and networked communications space adheres to the following code of conduct. No hate speech, including racist, misogynist, xenophobic, white-nationalist, transphobic, homophobic, classist, ableist, or police-endorsing language of any kind is permitted, and anyone doing so will be removed and barred from the space as well as any following events. Our events are for the sole purpose of creating safer spaces for trans and GNC people to learn about computer science, software development, virtual technologies, and digital security.

tldr: refer to the line from Grandmother Kate Bornstein, "Don't be mean."

# Threat modeling

*“A way of narrowly thinking about the sorts of protection you want for your data. It's impossible to protect against every kind of trick or attacker, so you should concentrate on which people might want your data, what they might want from it, and how they might get it. Coming up with a set of possible attacks you plan to protect against is called threat modeling. Once you have a threat model, you can conduct a risk analysis.”*

- EFF

1. What do I want to protect?
2. Who do I want to protect it from?
3. How bad are the consequences if I fail?
4. How likely is it that I will need to protect it?
5. How much trouble am I willing to go through to try to prevent potential consequences?

What are my *assets*?

Who are my *adversaries*?

What are the *capabilities* of my adversaries?

What is the *risk* level?

# Bike Courier Marijuana Delivery Person

Assets:

Adversaries:

Capabilities:

Risk:

# Bike Courier Marijuana Delivery Person

**Assets:** Bicycle, Supplies, Personal Identity, Identity of Employer, Money

**Adversaries:** Law enforcement, bicycle thieves, reckless drivers

**Capabilities:** Wiretapping, arrest, steal bicycle, run over with car, DEA sting

**Risk:** High                      Medium                      Low

# Bike Courier Marijuana Delivery Person

**Assets:** Bicycle, Supplies, Personal Identity, Identity of Employer, Money

**Adversaries:** Law enforcement, bicycle thieves, reckless drivers

**Capabilities:** Wiretapping, arrest, steal bicycle, run over with car, DEA sting

**Risk:** High Medium Low

The diagram consists of four colored arrows originating from the 'Risk' labels and pointing to specific capabilities: a red arrow from 'High' to 'Wiretapping', a red arrow from 'High' to 'arrest', an orange arrow from 'Medium' to 'run over with car', and a yellow arrow from 'Low' to 'DEA sting'. The 'Low' label also has a yellow arrow pointing towards the right, ending near the 'DEA sting' capability.



# Sex Work Provider in NYC

**Assets:** *Photos, legal id, address, social media accts, email, communications, texts, bank acct, payment legers, contacts,*

**Adversaries:** *Cops, stalkers, family, exes, journalists, careless ppl, catfish, trolls, anti prostitution ideologues, the ALGORITHM*

**Capabilities:** *Location tracking spyware, doxxing, blackmail, report police, steal photos, intercept, falsified charge reason/arrest reason, reporting status as sex work provider to 'vanilla' job*

**Risk:**                      High    Medium    Low

1. What do I want to protect?
2. Who do I want to protect it from?
3. How bad are the consequences if I fail?
4. How likely is it that I will need to protect it?
5. How much trouble am I willing to go through to try to prevent potential consequences?

# intermission

Digital privacy is self care

Self care sometimes means caring for others

The most efficient practice of digital privacy accounts for ensuring others care for you, and you reciprocate

Set ground rules for friends, clients, anyone of digital intimacy

“...in a legal scheme where buying sexual services is criminalized, some clients will seek sexual services in indoor settings. For street sex workers, fewer clients means increased competition, and the resulting pressures to agree to less safe sexual practices...

... Singling out sex clients as a deviant class and celebrating those who do not buy sex as good sexual citizens contributes to veiling the violence that happens to women in private, sanctified settings.”

- Ummni Khan, “Antiprostitution Feminism” - Feminist Surveillance Studies

## PART II:

# Addressing the threat model

## PART II:

# Addressing the threat model

**Obfuscate Your Online Activity:** Browsers, Browser extensions, VPNs

**Lock Down Your Social Media:** 2FA, Password Managers, Best Practices

**Encrypt Your Communications:** Email, Messaging, Phone Calls

**Secure Your Devices:** Encrypting mobile devices, Operating Systems, Habits

## Browsers

Tor

Brave

Firefox Focus (iOS)

Firefox (android)

Orbot (android)

## Browser Extensions

HTTPS Everywhere

Privacy Badger

Disconnect.me

uBlock Origin

# VPNs - Virtual Private Networks

## Providers:

AirVPN

TunnelBear

FeralHosting

CyberghostVPN

## Clients:

AirVPN

Viscosity

TunnelBlick

OpenVPN



# 2FA - Multi Factor Authentication

Authy

Google Authenticator

Yubikey

# Password Managers

LastPass (freemium)

KeePass (free and open source)

# Passwords

Long

Random

Use dice + wordlist

Never reuse

# Social Media Best Practices

Beware security questions

Never reuse passwords

Compartmentalize registry emails

Review privacy policies, opt for higher security

Be mindful of where/how you log into accounts

# Email

ProtonMail (provider)

PGP (protocol)

Allow account forwarding to mitigate  
DDOS attempts from trolls and  
stalkers

# Messaging

Signal

WhatsApp

Whisper

Avoid SMS when possible

# Phone Calls

Signal

Hiya

\*67

# Encrypt Your iPhone

Enable passcode (preferably 8+ characters)

Disable iCloud backups

Remember Emergency Services Triggers

Avoid SMS

Use Firefox Focus

# Encrypt Your Android

Enable lock screen pin (preferably 8+ characters)

Disable cloud backups

Use Orbot or Firefox (w/ extensions)

# Operating Systems

Don't use Windows 10

Be mindful of how you use OSX

Use Tails (high learning curve)

Linux (ubuntu most user friendly)



- <https://ssd.eff.org/>
- <https://hackblossom.org/cybersecurity>
- <https://eff.org>
- <https://libraryfreedomproject.org/>
- <https://www.torproject.org/>

[www.lastpass.com](https://www.lastpass.com)

[www.eff.org/privacybadger](https://www.eff.org/privacybadger)

[www.eff.org/httpseverywhere](https://www.eff.org/httpseverywhere)

[www.signal.org](https://www.signal.org)

[www.torproject.org](https://www.torproject.org)

[www.brave.com](https://www.brave.com)

[www.airvpn.org](https://www.airvpn.org)

[www.tunnelbear.com](https://www.tunnelbear.com)

[www.authy.com](https://www.authy.com)

<https://t4tech-nyc.github.io>

[t4technyc@gmail.com](mailto:t4technyc@gmail.com)

[daly.barnett@protonmail.com](mailto:daly.barnett@protonmail.com)