Personal Opsec

Staying Safe Online Under a Trump Presidency

Batman's Kitchen

Content Warning and Disclaimer

This presentation will talk directly about political violence, domestic abuse, stalking, and discrimination. If this hits too close to home and you need to step out at any moment, we will not judge or take offense.

We are not lawyers and the following is not legal advice.

Outline

- Intro
- What is opsec?
- Personal threat modeling
- General security tips for at-risk groups
- Specific tips for
  - People seeking abortions
  - Queer people
  - Domestic violence/stalking victims
  - Immigrants
  - Activists

Part 1: Intro

Motivation

Trump Administration Seeks to Expel a Green-Card Holder Over Student Protests

Immigration officers arrested a Columbia University graduate for helping lead campus protests against Israel's treatment of Palestinians. President Trump said the case was "the first arrest of many to come."

Motivation


EXCLUSIVE
Justice Dept. agrees to let DOGE access sensitive immigration case data
About a half-dozen DOGE "advisors" won approval from the the Justice Department to access the ECAS system, according to documents reviewed by The Washington Post.
April 21, 2025

Motivation

Deported Ivy League doctor Rasha Alawieh will remain in Lebanon as judge hears arguments over Trump ignoring court order

Brown Medicine doctor was detained at Boston's Logan Airport last week after returning from a trip visiting family in Lebanon

Rhian Lubin in New York, Alex Woodward • Monday 17 March 2025 15:28 GMT

• 26 Comments

Motivation


Green card holder from New Hampshire 'interrogated' at Logan Airport, detained
New England News Collaborative | By Sarah Betancourt, GBH
Published March 14, 2025 at 4:14 PM EDT

Motivation

Trump weighs revoking legal status of Ukrainians as US steps up deportations

By **Ted Hesson** and **Kristina Cooke**

March 6, 2025 6:25 PM PST · Updated 2 months ago

Aa

Motivation

Trans women transferred to men's prisons despite rulings against Trump's order

Incarcerated trans women report being groped by male guards and suicidal thoughts: 'I'm punished for existing'

Motivation

LGBTQ+ TEXANS

Texas attorney general's office sought state data on transgender Texans

> The behind-the-scenes effort by Ken Paxton's office to obtain data on how many Texans had changed their gender on their licenses came as he and other Republican leaders in the state have been publicly marshaling resources against transgender Texans.

BY MOLLY HENNESSY-FISKE, **THE WASHINGTON POST** DEC. 14, 2022 9 AM CENTRAL **SHARE**

Motivation

GENDER & LGBTQIA+

More bounty laws offering cash for reporting trans people, abortions, and librarians expected in 2025

Texas lawmakers pre-filed so-called bounty bills for the 2025 session, as other states continue to allow private citizens to sue over issues targeting marginalized groups

by Sarah Prager January 8th, 2025

Motivation

Abortion Bans Have Delayed Emergency Medical Care. In Georgia, Experts Say This Mother's Death Was Preventable.

At least two women in Georgia died after they couldn't access legal abortions and timely medical care in their state, ProPublica has found. This is one of their stories.

by Kavitha Surana, Sept. 16, 2024, 5 a.m. EDT

Motivation

Texas Attorney General Sues New York Doctor for Mailing Abortion Pills

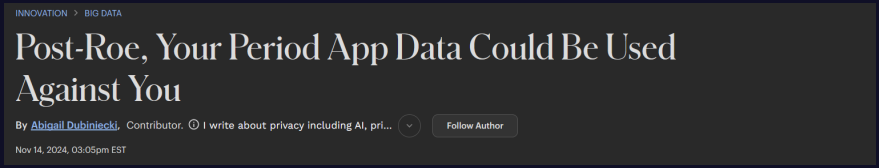
The lawsuit appeared to be among the first attempts to stop doctors from mailing the medication to states that ban abortions.

Motivation

When a Woman's Questions About Her Right to Choose Is Proof of Intent to Kill at Birth

By Isabelle Raquin

Motivation



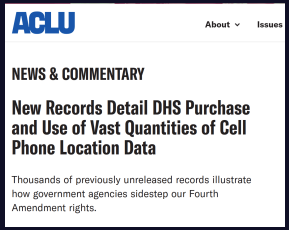
INNOVATION › BIG DATA

Post-Roe, Your Period App Data Could Be Used Against You

By Abigail Dubiniecki, Contributor. ⓘ I write about privacy including AI, pri... Follow Author

Nov 14, 2024, 03:05pm EST

What do these all have in common?



What is Opsec?

- "**Operational security**" - The practice of keeping yourself safe through **proactive defensive actions** which limit what information your adversaries have.
- Used in many different contexts throughout the industry
- Potential adversaries for **individuals**:
  - Surveillance agencies
  - Stalkers
  - Law enforcement
  - Corporations
  - Extremists

"Why Should I Care About Opsec?"

- Society is filled with systems designed to harm **at-risk groups**
- Things are **getting worse** and will only **continue to get worse** in this administration
- Minimizing the amount of information your enemies have on you minimizes their harm to you

"I'm A Straight White Man; Why Should I Care About Opsec?"

- You **will** have friends who are put at risk by the Trump admin
- Everyone in this room knows more about security than the average person
- It is **our responsibility** to help our loved ones stay safe
- Being a trusted voice on security is one of the most direct ways for us to help people

Part 2: Threat Models

What is a Threat Model?

- A theoretical **framework for understanding the threats** that affect a person, organization, or system.
- Important components:
  - Subject
  - Assumptions
  - In-scope threats
  - Possible mitigations
  - Out-of-scope threats

Personal Threat Models

- **Who** might try to harm you
- What **powers** they have over you
- What **information** they have on you
- How you can **limit** their information

Example Threat Model: Jane Doe

Subject: Jane Doe

- Lives in Kentucky
- Has a conservative family

Threat Actors:

- State government
- Federal government
- Abusive ex

Example Threat Model: Powers & Threats

- State government:
  - Prosecute abortions
  - Prevent reproductive care
  - Access healthcare information
  - Access chat logs, location data, etc.
- Federal government:
  - Same stuff as State
  - Outlaw medications
  - Inter-state surveillance
- Abusive ex:
  - Track her location
  - Control over some "shared" accounts
  - Physical violence

Example Threat Model: Mitigations

- Limiting location data gathering on her devices
- Using secure messaging apps
- Physical safety measures
- And more, coming up

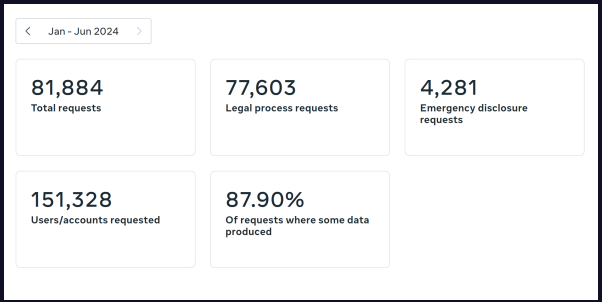
A Note About Crime

- The current administration is actively **criminalizing basic human rights**
- Some people will be **forced to commit crime to survive** in the coming years
- This talk will assume that:
  - Some crimes are **ethical** to commit
  - In those cases, law enforcement must be treated as an adversary
  - Being **complicit** in these crimes is ethical

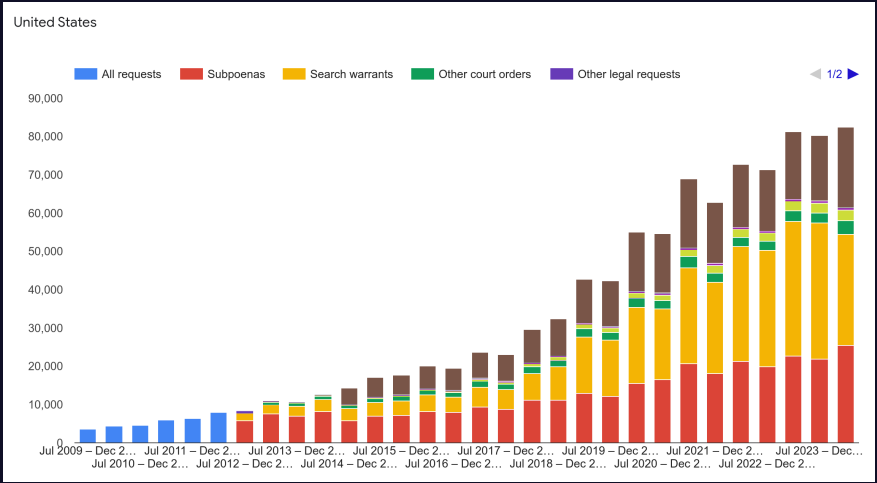
Part 3: Secure Messaging

Why is normal messaging "insecure"?

- Any messages you send on Discord, Instagram, Google, etc. are stored on their servers
- The cops can force social media platforms to **turn over your data**
- This happens **very often**
  - 80k requests to just Meta in just the US in half a year



Why is normal messaging "insecure"?



Why is normal messaging "insecure"?

How We Enforce Rules

HOW DISCORD WORKS WITH LAW ENFORCEMENT

Discord

February 16, 2024

Request Type	Requests	Information Produced
Court Orders	55	45
Pen Register / Trap and Trace	6	5
Search Warrants	576	548
Subpoenas	629	604
Total	1,266	1,202

Encryption

- "Wait, I thought that modern services used encryption!"
- How encryption usually happens:
  - Message is encrypted on its way to e.g. Discord with Discord's key
  - Discord decrypts it then sends it to the recipient encrypted with the recipient's key
  - The platform (and the feds) have **full insight into the message contents!**

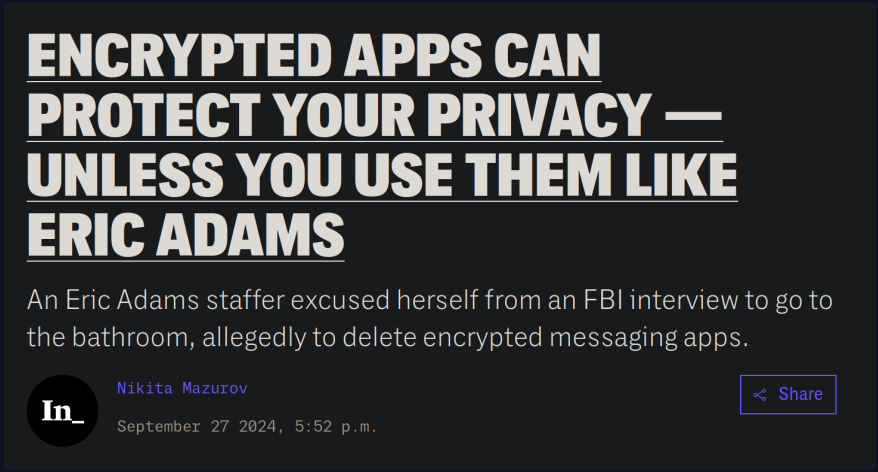
End-to-End Encryption

- Messaging is only secure if it uses **end-to-end encryption** (E2EE)
- E2EE -> Messages can only be read by the person sending and the person receiving it
- The platform/feds physically cannot see what is being sent, only whom it's sent to

"like Signal and Telegram"

- Do **not** use Telegram
- It only does E2EE for direct messages and even then only kinda
- **Signal** is the gold standard for civilian secure messaging: https://signal.org/download/
- You can't just use Signal, you need to use it right
- Use disappearing messages, check your group chat members
- For more information: https://www.washingtonpost.com/technology/2025/03/25/signal-tips-encrypted-messaging/

Don't Be Him



ENCRYPTED APPS CAN PROTECT YOUR PRIVACY — UNLESS YOU USE THEM LIKE ERIC ADAMS

An Eric Adams staffer excused herself from an FBI interview to go to the bathroom, allegedly to delete encrypted messaging apps.

In_

Nikita Mazurov

September 27 2024, 5:52 p.m.

Share

Or Him

POLITICS

The Trump Administration Accidentally Texted Me Its War Plans

U.S. national-security leaders included me in a group chat about upcoming military strikes in Yemen. I didn't think it could be real. Then the bombs started falling.

By Jeffrey Goldberg

Email

- Use ProtonMail: https://mail.proton.me/
- It uses end-to-end encryption
- Gmail, Outlook don't even pretend to protect your messages

File Sharing

- As you might guess, Google Drive is similarly insecure
- Opt for end to end encrypted solutions
- Use Cryptpad.fr (hosted in France) or Proton Drive (hosted in the US)

Part 4: Secure Browsing

Threats During Normal Browsing

- Surveillance Capitalism
- Google, Facebook, data brokers
- Internet Service Providers (ISPs)
- The websites you are visiting
- Law enforcement
- Chinese hackers who backdoored law enforcement

Data Brokers

- Companies which collect massive amounts of data on **everyone**
- This data is then sold to:
  - Cops
  - Insurance companies
  - Advertisers
  - Political campaigns
  - Other data brokers
  - Stalkers
  - Creditors, banks, etc.
- Data is collected from websites, apps, browsing history, devices (all of them), passive surveillance, credit history, and a million other things

What data do they have?

- All of it
- If you haven't been actively paranoid about privacy, they almost certainly have:
  - Address
  - Birthdate
  - Demographic data (race, gender, age, politics, sexuality, economic bracket, etc.)
  - Health history
  - Family and friends
  - Personal interests & hobbies
  - Location history
- Anything their giant AI systems are able to infer from their other data

How do you get this data deleted?

- Ask nicely :)
- They may or may not comply, depending on which state you live in
- The process is often very annoying
- https://github.com/yaelwrites/Big-Ass-Data-Broker-Opt-Out-List
- https://inteltechniques.com/workbook.html
- There are services like Incogni and DeleteMe which automate this
  - We cannot personally vouch for their success rate
- **The only way to ensure a data broker doesn't have your data is to not give it to them in the first place.**

Virtual Private Networks

- Virtual Private Networks (VPNs) mask traffic from ISPs and sites
- All your traffic gets encrypted and sent through a VPN provider's server first
- **Masks your IP address** from websites you visit
- Pretty good for privacy against ad tracking campaigns

Don't Rely On VPNs

- VPNs do not save you from fed wiretapping
- The feds can just request your browsing data from your VPN provider
- Proton and others claim not to keep logs, but they might still be wiretapped
- **VPNs are good but not foolproof**

Tor

- Tor is like a **more secure, decentrallized** VPN
- Routes traffic through a circuit of several random volunteer-run nodes instead of one singular provider
- Each node either knows who you are **or** where your traffic is going, never both
- Nearly impossible to track / wiretap if used right
- https://www.torproject.org/download/

Part 5: Passwords

Passwords

- Passwords should be long, memorable, and hard to guess, and distinct
- My rule of a thumb is a complete sentence
- Use a password manager like ProtonPass
  - https://proton.me/pass

Multi-Factor Authentication

- Turn on multi-factor authentication (MFA) for all accounts
- Factors of authentication include
  - what you know
  - what you have
  - what you are
- Estimated it would **prevent 90% of attacks**
- Do not use SMS/text based if possible
- We recommend Aegis Authenticator

Part 6: Interacting With Law Enforcement

How To Talk To Cops

Don't

If You Have To Talk To Cops

- Much like a vampire, do not let them anywhere without a **warrant**
- "I do not consent to search"
- **Disable biometric authentication**
  - The cops legally cannot force you to provide a PIN
  - The cops can* force you to unlock a device with biometrics

Arrest

- Write down phone numbers on a card in your phone case
  - You never want to have to unlock your phone when in custody
- Ask which jail you're at before calling
- The **prison phone line is actively wiretapped**. Say nothing about what you did
- Assume data on any seized device is compromised
  - Cellebrite and Grayshift products will extract data regardless of passwords
- Do not talk without a lawyer!

Part 7: Abortion

Another Disclaimer

- We are still not lawyers

Threat Model

Federal Government

- FDA may change abortion pill legal status
- Department of Justice controls the Comstock Act enforcement

Anti-abortion friends, families, and communities

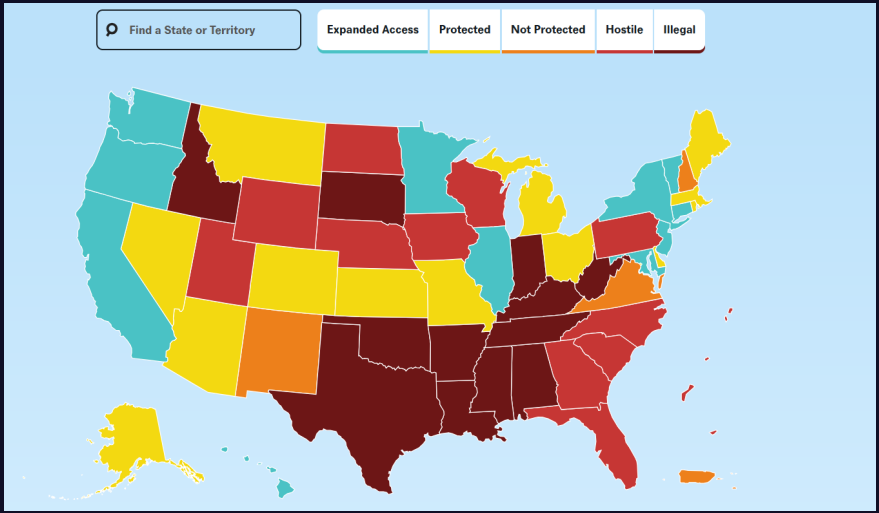
- Some states have "bounty laws"

State governments

- May prohibit various forms of reproductive care and assistance
- Targeting pregnant people, medical professionals, and other supporters

Tech companies

Threat Model



Information Gathering and Leakage

Abortion decisions can leak inadvertently

- Browsing history
- Targeted advertisements
- Texts
- Receipts, credit card or medical bills

Mitigations

- Access abortion-related websites **only through Tor**
  - If you use a period tracking app, use privacy focused ones like **Euki**
- Communicate securely (Signal, talks in person)
- Pay in cash / prepaid cards so it doesn't appear on your credit card statement

Abortion Pills

- Abortion medication is **safe and effective**
- Telehealth is legal in some states
- Review symptoms with a trusted person
- Available to buy in every state: https://www.plancpills.org/in-advance
- You can buy pills in advance in some states
- Ship them to a state where legal
- If you experience adverse effects
  - Go to Planned Parenthood if possible
  - Urgent care otherwise
  - Tell them you had a **miscarriage**
  - The symptoms and treatment are the same

Contact Planned Parenthood

How do you contact Planned Parenthood in an abortion-hostile state?

- Access websites through Tor
- Use Proton Mail email
- Pay in cash and prepaid gift cards
- Whenever possible **do not use your real name**
  - Planned Parenthood does not want your real name
  - You will likely need to give it out if you need to use insurance

Abortion Procedures

- If abortion is partially or fully legal in your state:
  - Go to Planned Parenthood
  - Still take the same precautions, but you should be good
- If you need to travel
  - Don't tell people **why or where** you are going
  - Continue to use secure messaging, browsing, payment

A Note on Travel

Your car is a **federal informant**

Automatic License Plate Readers track movements, associations, and patterns

Car companies can log:

- Location
- People you text or call, call contents*
- Videos recorded by onboard cameras

Fourteen car brands **willingly hand over data to cops** without a warrant

A Note On The Note On Travel

- Many modern cars have subscription plans (OnStar, Drive Smart)
- These are often billed as entertainment or safety programs
- They are data collection programs for insurance and cops
- Disable all subscriptions/accounts/etc. on your car

Back To The Note On Travel

- Take public transit if possible
- Traditional Taxis
- Trusted people's cars
  - Preferably old ones without internet connectivity
  - Note: Your accomplices may be prosecuted
- Do not use directions to an abortion clinic in Google/Apple Maps
  - Choose a **location nearby** if necessary

Resources

- Figuring Out Options:
  - https://www.ineedana.com/
  - https://www.abortionfinder.org/
- Locating Abortion Pills:
  - https://www.plancpills.org/
- Legal Help:
  - https://reprolegalhelpline.org/
- Miscellaneous
  - https://www.mahotline.org/
  - https://digitaldefensefund.org/ddf-guides/abortion-privacy/
  - https://www.plannedparenthood.org/

Part 8: Opsec for Queer People

Threat Model

- Governments blocking access to HRT
- Legal persecution
- Discrimination by employers and other authority figures
- Harassment by extremists

Hormone Replacement Therapy

- Obtain it legally if possible
- If that is not possible:
  - https://diyhrt.wiki/
  - https://hrtcafe.net/
  - https://crimethinc.com/2022/12/15/producing-transdermal-estrogen-a-do-it-yourself-guide
  - **Access these sites through Tor only.**
- It is currently possible to order HRT from other countries
  - This is very risky, especially so for testosterone
  - As far as the feds are concerned, you are smuggling drugs
  - Unrelated talk from a former drug smuggler
    https://www.youtube.com/watch?v=01oeaBb85Xc

Online Privacy

- Nuke your X: The Everything App account
- Seriously
- It's run by a nazi
- Avoid making it easy for data brokers to identify you as queer
  - Only search queer-related things through Tor
  - Remove pride flag emojis and such from your bio imo
  - Consider ditching social media as much as possible
  - Watch queer-related videos through a method like yt-dlp or Nebula when possible

Anti-Harassment Measures

- Vocal queer people on social media can get doxxed, harassed, SWATed, etc.
- Do not reveal any unnecessary personal info on public socials
- If you post a photo, assume that **the location will be found**
- Wait to post photos of where you are until you have left the area
- Do not post photos from within a mile of your house
- Look through your posts every month to see if anything needs to be nuked

Keeping Your Friends Safe

- **Prevent listmaking**
  - Don't tag your friends in posts
  - Discuss queerness-related things over Signal
  - Avoid giving unnecessary information to official organizations (incl. nonprofits)
- Have a trusted emergency contact group on Signal

Other Tips

- Every-day carry pepper spray or spray paint
- Stockpile meds while you can
- Travel in groups at night
- Stay out of prison. Prison is especially hellish for queer people
- Don't get gender marker changes at this point imo
- If you work for a big corporation, avoid being out at work
  - Your manager might be chill but the people above them aren't

Lifelines

- https://thrivelifeline.org/
- (313) 662-8209

- https://translifeline.org/
- US (877) 565-8860 / Canada (877) 330-6366

- https://www.thetrevorproject.org/get-help/
- (866) 488-7386

- You can't have good opsec if you're dead.

Part 9: Opsec For Domestic Violence Survivors

Threat Model

- The threat model for DV survivors is different than any other
- Abusers and stalkers may know locations, passwords, and life history
- Abusers and stalkers may have physical access to survivors and devices
- This access is often persistent and dangerous to revoke

Mitigations

- Traditional cybersecurity advice operates under a completely different model
- Cybersecurity people who give advice without understanding this fail survivors
- We are out of our depth and unqualified to give advice.

Resources and Orgs

- The Digital Defense Fund: https://digitaldefensefund.org
- Coalition Against Stalkerware: https://stopstalkerware.org/
- National Domestic Violence Hotline: https://www.thehotline.org/

Part 10: Opsec for Immigrants

Threat Model

- Immigration & Customs Enforcement (ICE)
- Employers
- Snitches
- Extremists

Documented Immigrants

- Keep a **copy of your immigration documents** on you at all times
- Keep in mind that activists are having their statuses revoked
- If you have an immigration lawyer, communicate over Signal
- Don't talk to cops
- Understand that ICE is deporting documented residents for no reason and prepare accordingly
  - It seems that for latinos, having tattoos increases risk
- Educate your family about scams targeting immigrants
  - "This is ICE calling, give us all your personal info"

International Travel

- **CBP does not need a warrant** to search your devices
  - Citizens can technically refuse but risk detainment
  - Everyone else is fucked
- Turn on airplane mode when going through Customs
- Turn off biometrics
- https://www.washingtonpost.com/travel/2025/03/21/travelers-entering-united-states-rights/

Undocumented Immigrants

- Stay the fuck off social media
- Make plans with friends/family/kids for what happens if you're detained
- Find a local Rapid Response Network which sends out alerts about ICE presence
  - NOTE: Language encouraging evading the cops can be seen as obstruction of justice
  - Simply notifying about ICE presence is covered by free speech though

Resources

- Latin American Legal Defense and Education Fund: https://laldef.org/
- ACLU: https://www.aclu.org/
- Rapid Response Networks in your area https://www.ccijustice.org/carrn
- https://ilrc.org/resources/community/know-your-rights-toolkit

Part 11: Opsec for Protesters and Activists

One Last Disclaimer

- In the last hour, we have not become lawyers

Threat Model

Local, State, and Federal Law Enforcement

- Arrest and detain
  - Deportation to foreign gulag
- Investigations
  - Physical surveillance as an intimidation tactic
- Waste money through litigation

Trade-Offs

- There is always a trade off between security and achieving your other goals
- It is faster to not have a password but we generally decide in favor of security
- The fundamental question of protest security is **how much do you need your phone?**

Pros & Cons to Bringing Your Phone

- Pros
  - Internet and navigation
  - Communication
- Cons
  - Location at the protest leaked through
    - Cell-site simulators
    - Global Positioning System
    - Tower dumps
    - Geo-fencing
    - MAC address tracking
  - Coordinating messages may be seized

No Phones

- The most secure strategy is to not bring your phone
- Plan out meeting spots for before and after
- Know public transit routes

Prepaid Phones

- Buy a prepaid, disposable phone and SIM card (ideally in cash)
- Only use it in areas that are not linked to you
- Do not keep your regular phone on at the same time
- Turn off at home/anywhere linked to you
- Dispose after use away from locations linked to you

Limited Phones

- If you want to keep your phone on person
- Use strong passwords (8+ characters) and turn off **biometric authentication**
- Turn on **Lockdown Mode** for iOS or turn off 2G on Android
- Use secure messaging methods discussed earlier
- Prepare for device seizure by backing up devices, passwords, and MFA tokens
  - Make sure backups are E2EE
- Revoke access to devices or change passwords after seizure
  - This may be considered obstruction of justice -- talk to a lawyer

Airplane Mode

- Security is about trade offs
- It is best to use Airplane Mode, disable WiFi, Bluetooth, and Cellular
- This means you can not communicate with people while at the protest
- Even if you don't turn on Airplane Mode, turn off WiFi and Bluetooth

Dress

- Dress in dark monochrome colors
- Cover tattoos, distinct colored hair, other identifying features
- The feds maintain tattoo recognition software and databases

Photos

- Security is about trade-offs
- Block out all faces in photos/videos you post
- Signal has a face blurring tool built in and scrubs metadata
- https://everestpipkin.github.io/image-scrubber/

Transport

- Keep in mind the dangers of travel mentioned before
- Walk or bike if possible, especially for the last leg of transport
- Public transport paid in cash
- Automatic License Plate Readers are everywhere

Organizers

- Secure your phone
  - Turn on MAC randomization
  - Turn on Lockdown Mode on iOS
  - Install GrapheneOS on Google Pixels
  - Check if LineageOS supports your device otherwise
  - If not haha good luck lmao
- Know who you are going to call
- Know who is going to pay bail
- Do not discuss any activism in public

MAC Randomization

- Defense technique against NSA surveillance tactics
- iOS: On by default
  - If you're a college student, enable rotating addresses in the settings for the eduroam network
  - Ask me later why if you're interested
- Android: On by default
  - Enable Developer Options and then enable "Wi-Fi non-persistent MAC randomization" for better results
- Windows: "Random Hardware Addresses"

iOS Lockdown Mode

- Disables 2G, connecting to insecure WiFi
- Disables biometric authentication
- Blocks most message attachments, some link previews
- Restricts web technologies, fonts, and images
- Restricts FaceTime, blocks SharePlay and Live Photos
- Blocks Shared Albums, removes location data from photos
- Requires authentication to connect to devices or computers
- Blocks configuration profiles and device management software

GrapheneOS

- Fork of Android with all the Google shit removed
- Much better security than normal Android
- Has cool features like:
  - Duress PIN
  - Autoreboot/encrypt on inactivity
  - Automatically disable Bluetooth
  - Better sandboxing for apps
  - Good MAC randomization
  - Enable all of these!
- Install apps from F-Droid (preferable) or Aurora Store

Mutual Aid (Crime Edition)

- But who distributes the abortion pills and hrt?
- There is a lot more you need to do
- You can start here:
  - Darknet Opsec: https://www.youtube.com/watch?v=01oeaBb85Xc
  - Catching Cyber Criminals With Good Opsec: https://www.youtube.com/watch?v=zXmZnU2GdVk

Resources and Orgs

- Electronic Frontier Foundation's Guide for Protests
  - https://ssd.eff.org/module/attending-protest
- https://crimethinc.com/2017/03/27/burner-phone-best-practices
- ACLU Know Your Rights
  - https://www.aclu.org/know-your-rights/protesters-rights

Part 12: Final Thoughts

Where do we go from here?

- This has been a depressing talk
- We cannot allow ourselves to become overwhelmed
- You alone cannot fix the entire world
- You can help make it better for your loved ones

Things you should do ASAP

1. Download Signal
2. Download Tor
3. Download ProtonVPN
4. Get a password manager (ProtonPass)
5. Turn on MFA on your important accounts
6. Nuke unnecessary info from socials
7. Make an emergency contact card
8. Locate important life documents
9. Disable biometric
10. Disable any accounts in your car
11. Watch this talk: https://youtu.be/6ihrGNGesfI
12. Get a passport and passport card
13. Turn on MAC randomization on your phone + laptop
14. Use eduroam instead of UW WiFi
15. Send some data broker opt-out emails

What to do for your loved ones

1. Figure out their needs and risks
2. Prioritize defense measures that address these most directly
3. Get them to use Signal & ProtonMail
4. Make sure they know to trust you on matters of security & privacy
5. Tell them you love them.