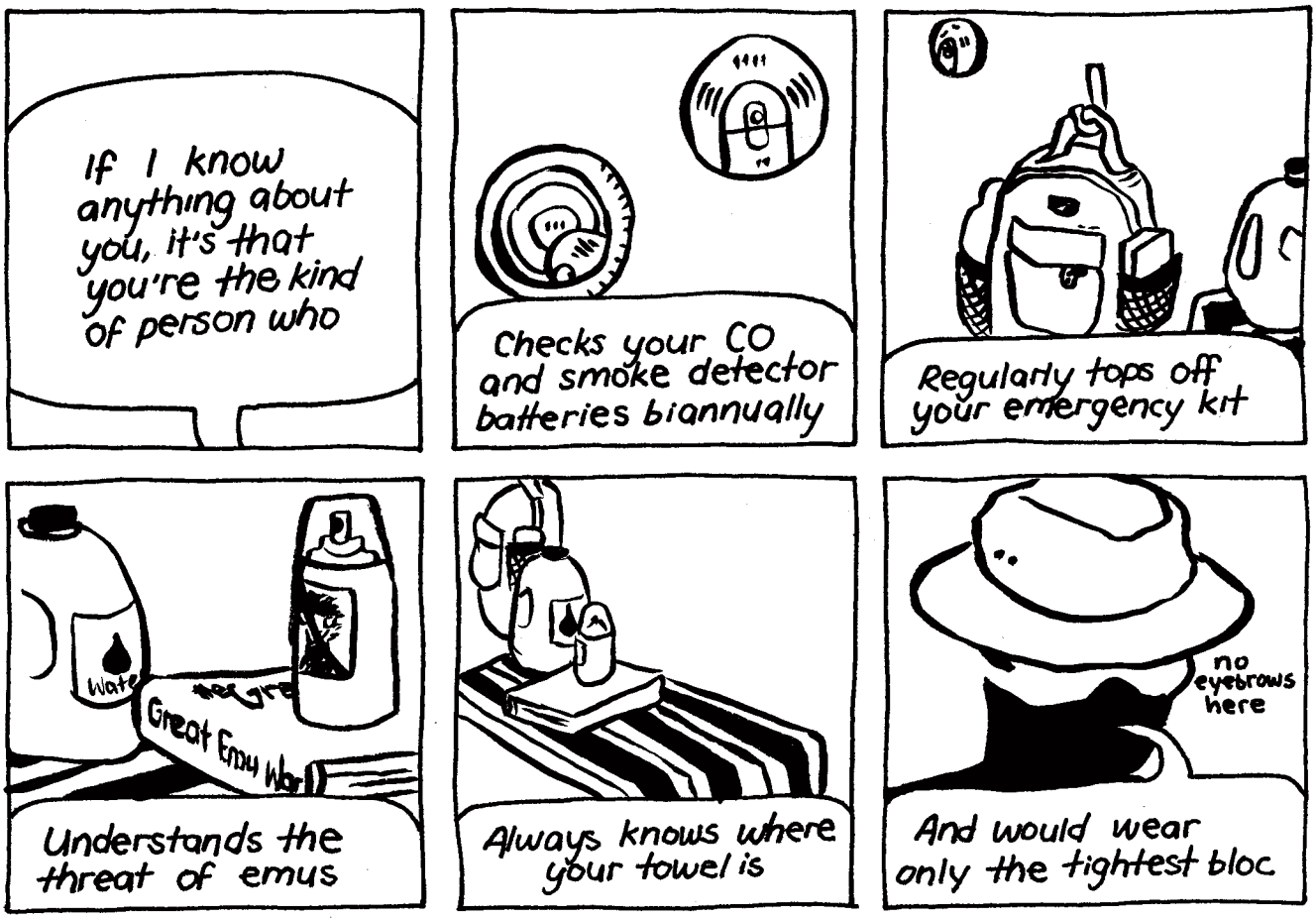
Digital Security FOR PORTLANDERS

VOL III

Learn to manage your overwhelming internet dread!

Contains homework (there may be a test)

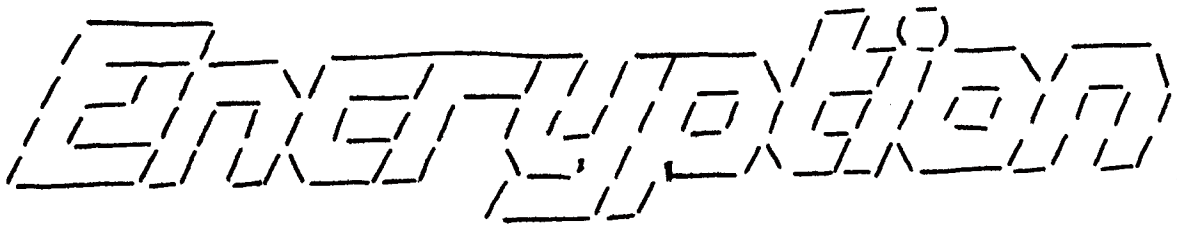

If I know anything about you, it's that you're the kind of person who
Checks your CO and smoke detector batteries biannually
Regularly tops off your emergency kit
Great Emu War
Understands the threat of emus
Always knows where your towel is
no eyebrows here
And would wear only the tightest bloc


your ISP
Smart speakers
But are you equivalently prepared electronically?
Your web browser & search engine
Even a smart fridge could be leaking your data
Rewards cards
I'm your friendly neighborhood anti-fascist, and I'd like to check in with you about your digital security
1

Activities Terminal

fnaf@home

(When Alice and Bob wish to talk to each other very badly, they turn to)

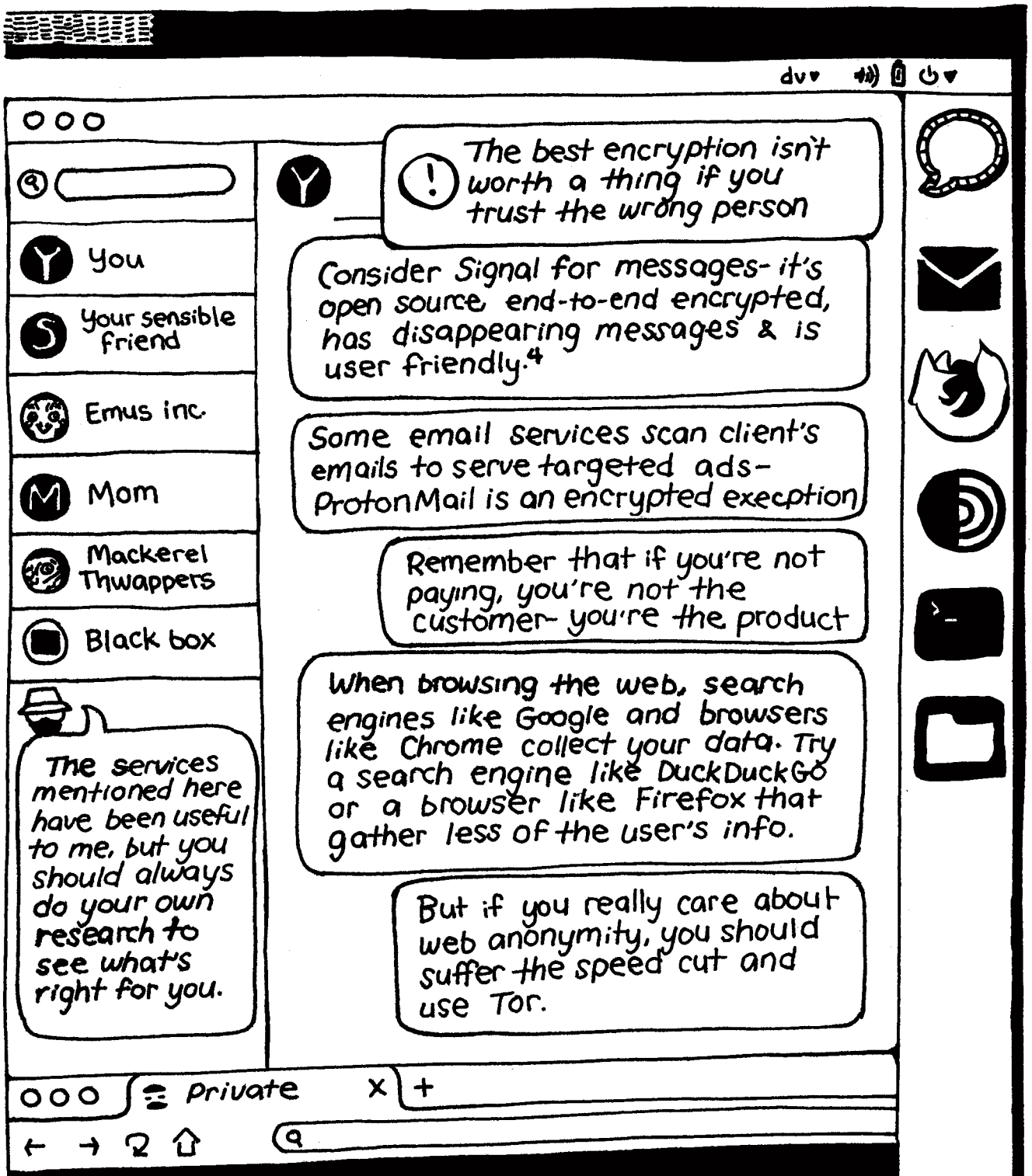


 ncryption matters when you're sending data that has the potential to be inspected by uninvited third parties. It works by making this data look like gobbledygook to those without the decryption key. Encryption is everywhere-- from your bank account to your interaction with nearly every website you visit. (Terms like 'military grade encryption' don't mean much-- modern encryption standards are 'military grade')

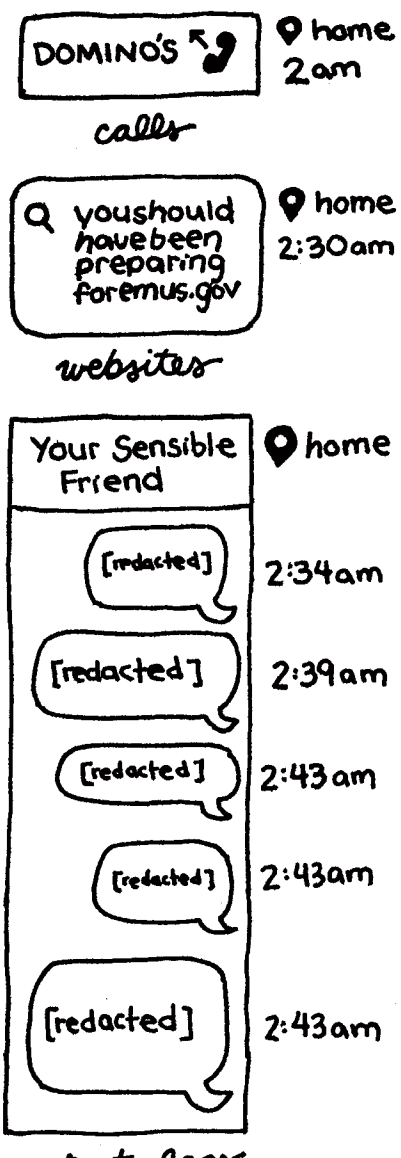
 ommunication: for messaging and email you want END TO END ENCRYPTION where your messages are encrypted both on their way from your phone to whoever you're talking to, and also encrypted from the app you're messaging on, so the app's servers can't see them. That way even if your messaging service is subpoenaed or hacked there's nothing to see.[2]

 asswords: the best encryption is worth nothing if you don't have a strong password.[3] You knew it was coming-- it's time to actually change all your passwords. EVERY password you use should be long, unique and random. If you can't remember all your passwords, you should get a password manager. DON'T reuse passwords.

-- INSERT --


You
Your sensible friend
Emus inc.
Mom
Mackerel Thwappers
Black box
The services mentioned here have been useful to me, but you should always do your own research to see what's right for you.
The best encryption isn't worth a thing if you trust the wrong person
Consider Signal for messages- it's open source, end-to-end encrypted, has disappearing messages & is user friendly.[4]
Some email services scan client's emails to serve targeted ads- ProtonMail is an encrypted exception
Remember that if you're not paying, you're not the customer- you're the product
When browsing the web, search engines like Google and browsers like Chrome collect your data. Try a search engine like DuckDuckGo or a browser like Firefox that gather less of the user's info.
But if you really care about web anonymity, you should suffer the speed cut and use Tor.
Private
Common Misconceptions
• Going incognito does not erase your digital tracks
• Not all disappearing messages are secure
• VPNs are useful for concealing your activity from your ISP only when you trust your VPN provider.[5,6]

Have you heard about METADATA?



Your *personal data* - the contents of your texts and calls, your photos and emails are protected and require a warrant to search. It's hard, if not impossible, to see this data w/out physical access to your device.

Your *metadata* is not so well protected. Metadata is everything except for the content of your data - it's the data about your data. This includes timestamps, subject lines, geolocation, who you call, the websites you visit.[7] Much of this information is stored by your ISP and could be accessed without your knowledge.

Legal precedent concerning metadata remains uncertain. Different police departments and courts have different standards.

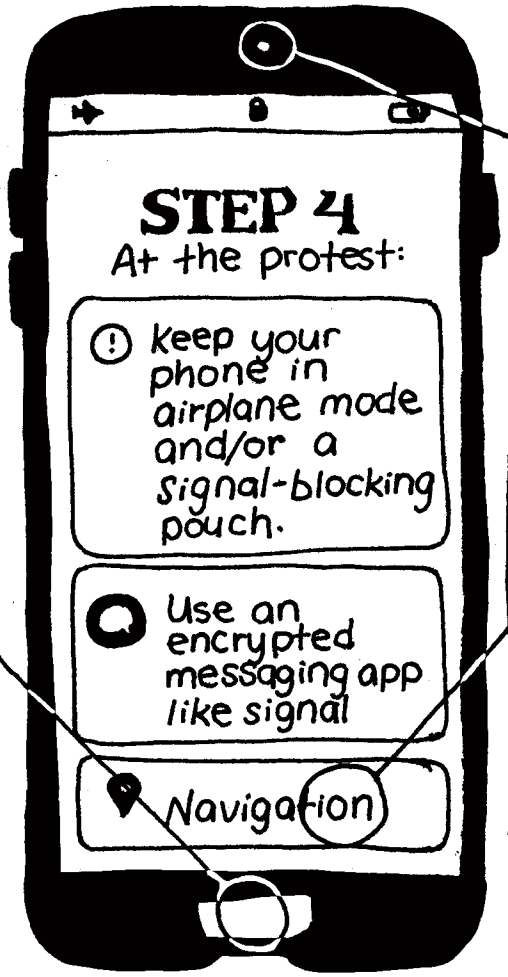
Photos include the time they're taken & the location they're taken at, which is visible to anyone with the image. One easy way to remove this metadata is to send the image to yourself through Signal.[8]

You know Google Docs saves your edit history, but did you know Word does too? Next time, consider a PDF.

SO YOU BROUGHT YOUR PHONE TO A PROTEST[9]

STEP 1. Reconsider: Try a brief digital detox, or acquire a phone without your personal information that you only turn on at protests

STEP 2. So you'll bring a phone: Assume it will be confiscated. Remove any sensitive data from it (messages, images, etc)



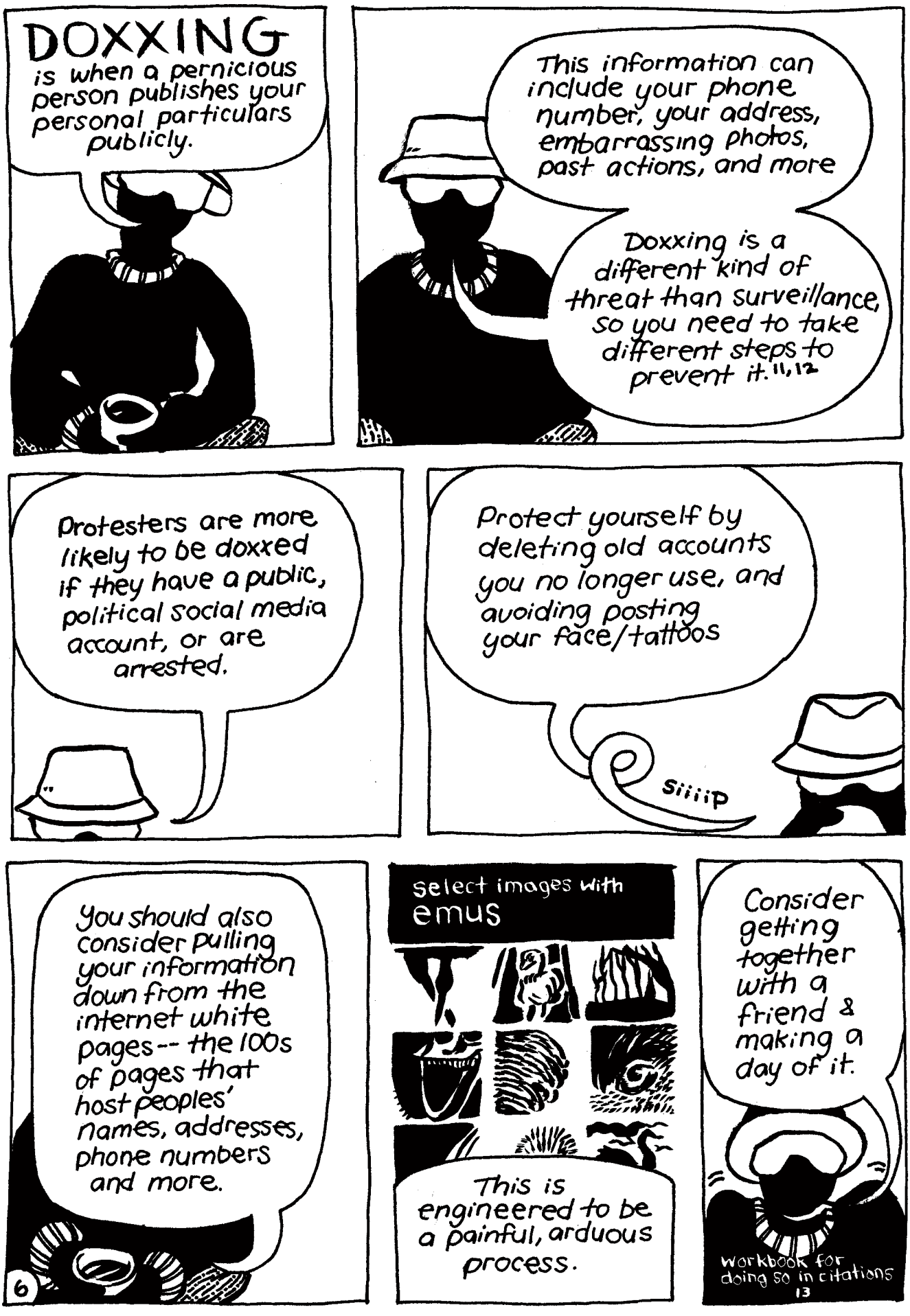
STEP 5. Think carefully before you film: Are you documenting or protesting? If you film, do it while your phone is locked.

STEP 3. Turn off biometrics: Unlock your phone with a long, random pin - not your face (cops can't legally search your phone w/out a warrant

STEP 6. Heading home: If you'll need a map, download it beforehand and navigate with your phone still in airplane mode (GPS is receive-only)

YOU MAY ENCOUNTER[10]

- Cheap devices that mimic WiFi networks and intercept all activity on them - always be suspicious of open networks and never connect at protests.
- Stingrays mimic cell phone towers and collect any outgoing data from your phone - texts, calls, location, searches... They're usually operated in vehicles.
- Dirtboxes, a similar device with a wider range, mounted on an aircraft. To protect against this, use airplane mode


DOXXING
is when a pernicious person publishes your personal particulars publicly.
This information can include your phone number, your address, embarrassing photos, past actions, and more
Doxxing is a different kind of threat than surveillance, so you need to take different steps to prevent it. 11, 12
Protesters are more likely to be doxxed if they have a public, political social media account, or are arrested.
Protect yourself by deleting old accounts you no longer use, and avoiding posting your face/tattoos
SiiiiP
You should also consider pulling your information down from the internet white pages -- the 100s of pages that host peoples' names, addresses, phone numbers and more.
6
select images with emus
This is engineered to be a painful, arduous process.
Consider getting together with a friend & making a day of it.
Workbook for doing so in citations 13

CRITICIZED A CELEB ! ACTIVIST/JOURNALIST ! TWEET WENT VIRAL ! UNDER THE RADAR ! NEVER TOUCHED THIS 'INTERNET'

It would be a full-time job to protect your everything from everyone; prioritize by conducting a

THREAT ASSESSMENT

The Electronic Frontier Foundation (EFF) suggests asking:[14]

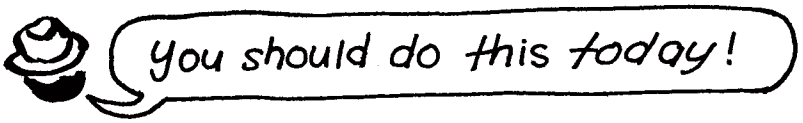
- What do I want to protect?
  (messages, location, passwords)
- Who do I want to protect it from?
  (people, the government)
- How bad are the consequences if I fail?
  (humiliation, arrest, assault)
- How likely is it that I'll need to protect it?
  (do you have a public presence? been victim of a breach?)
- How much hassle am I willing to go through?
  (having a secret phone number is a lot of work, for example)

For more information, check out the EFF's digital security guide for activists in the citations[15]

I've never done anything illegal-- why should I care about internet security?

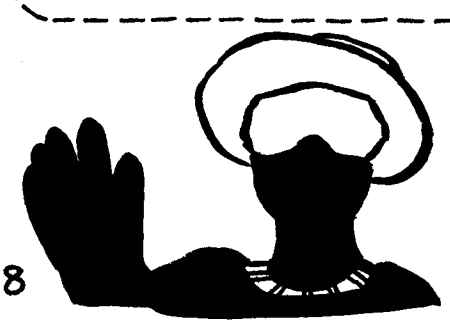
- You could still be targeted by malicious actors
- If you're secure, then the people around you- your friends, neighbors, contacts- will be more secure, too
- Security shouldn't be a precaution- view it as a right

ACTIVITY SECTION



Digital Security Action Items

- ☐ Get a password manager & change all your passwords to secure, randomly generated ones. (Consider Dashlane, 1Password, or LastPass)
  - ☐ Check your emails at haveibeenpwned.com to see what data breaches you've been involved in and prioritize changing those passwords
  - ☐ Sign up for services with a different email from the one you use for essential accounts (bank, etc)
- ☐ Turn on 2-factor authentication everywhere (and use an authenticator app or Yubikey rather than your phone number)
- ☐ Lock your credit (only unlock for credit checks) (For instructions, look at the FTC site in citations)[16]
- ☐ _____



Thanks for reading and see you next time!

CITATIONS

1. "What Should I Know About Encryption?" Surveillance self-Defense, Electronic Frontier Foundation, March 7, 2019.
2. "Communicating with Others." Surveillance Self-Defense, Electronic Frontier Foundation, June 9, 2020.
3. "Keeping your Data Safe." Surveillance self-Defense, Electronic Frontier Foundation, November 12, 2019.
4. "Attending a Protest." Surveillance Self-Defense, Electronic Frontier Foundation, April 1, 2019
5. Scott, Tom. *This Video Is Sponsored By* [redacted] *VPN*, 2019
6. "Choosing the VPN That's Right For You." Surveillance Self-Defense, Electronic Frontier Foundation, April 2, 2019.
7. "Why Metadata Matters." Surveillance Self-Defense.
8. "Why Metadata Matters." Surveillance Self-Defense.
9. "Attending a Protest." Surveillance Self-Defense.
10. Quintin, Cooper. "A Quick and Dirty Guide to Cell Phone Surveillance at Protests." Electronic Frontier Foundation, June 25, 2020
11. "Doxcare." CrimethInc, August 26, 2020
12. "A Guide to Doxxing Yourself on the Internet." The New York Times
13. Bazzell, Michael. *Extreme Privacy What It Takes To Disappear: Intel Techniques.* 2.5 ed., 2020
14. "Your Security Plan." Surveillance Self-Defense, EFF, April 1, 2019
15. "Activist or Protester?" Surveillance Self-Defense, EFF, April 1, 2019
16. "Credit Freeze FAQs" FTC Consumer Information, September 24, 2019

FURTHER READING

- The EFF's website is an amazing resource with a lot of information we didn't have room to get into. Check out their Surveillance Self-Defense Guide (ssd.eff.org), maybe read an article about securely deleting your data.
- If you'd like to know more about doxxing & its aftermath, read the CrimethInc "Doxcare" article.
- If you like podcasts, check out Reply All episodes 130: The Snapchat Thief and 97: What kind of Idiot Gets Fished?

print your own from
zines.headingnorther.com!

 @headingnorther

 @ heading_norther

Questions? Compliments? Corrections?

headingnorther@protonmail.com

September 14th 2020

From southeastman and
headingnorther