How to Thwart Digital Surveillance

This guide covers some best practices for digital security, specifically to thwart surveillance of communications and location. Remember, ultimately, there is no perfect security -- a well-resourced adversary with virtually unlimited time and money will eventually be able to overcome your security protocols. But the tougher you make their job, the less likely they will try, and the fewer resources they will have to devote to others. Don't make yourself an easy target.

Collectively increased security is the best way to ensure individuals are not being routinely surveilled. Remember too that the digital security landscape is ever shifting-- new software is developed and deployed, new vulnerabilities are found, and new tactics employed. You should stay up to date on best security practices, and to keep your systems protected from new attacks.

To begin with, **make your password long and memorable:** The longer a password is, the less likely it is that a computer program will be able to guess it in a reasonable amount of time. Some people use pass*phrases* that contain several words, with or without spaces between them. Passphrases are a great idea for services that allow longer passwords. **Make it complex:** Where possible, you should include upper case letters, lower case letters, numbers and symbols in your password. Some services require you to use different characters. **Don't make it personal,** this means anything at all guessable by someone you know or someone who knows your biographical details.

Step 1: Start with a clean slate

1a. Creating a persona - there are a variety of open source tools available to generate a random persona. See: https://backgroundchecks.org/justdeleteme/fake-identity-generator/ or https://www.fakenamegenerator.com/ or https://randomuser.me/

1b. You can download a profile picture here: https://thispersondoesnotexist.com/

1c. Associating persona with new digital assets: withdrawing cash → one-time use debit card → purchase burner phone → crypto wallet with burner email which you need a burner phone to create. For a guide see: https://theintercept.com/2020/06/15/protest-tech-safety-burner-phone/

For a guide see: https://www.dailydot.com/debug/how-to-create-digital-identity/

Step 2: Masking your location

A. Location (current and historic)
   a. Default phone settings
      i. Android: https://support.google.com/accounts/answer/3467281?hl=en
      ii. Apple: https://support.apple.com/en-us/HT207092
      iii. https://lifehacker.com/psa-your-phone-logs-everywhere-you-go-heres-how-to-t-1486085759
   b. Advertising trackers
      i. Some VPNs can block trackers and cookies (PrivacyPro)
      ii. You can check if websites use tracking cookies here: https://www.cookiebot.com/en/

iii. Test here for laptops: https://panopticlick.eff.org/

c. Faraday bag / cage is a device that prevents radio signal emissions. Emissions can be used to track your location. We recommend keeping a phone and laptop in Faraday bag when it is not in use or while you are going to, and in, a protest.
   i. Some potential options include: https://www.amazon.com/Mission-Darkness-Non-Window-Faraday-Laptops/dp/B01A7NDHZO/
   ii. https://www.amazon.com/Mission-Darkness-Non-Window-Faraday-Phones/dp/B01A7MACL2/
d. Unauthorized listening can be enabled by software, use a tool like Mic Lock to prevent it
   i. https://www.amazon.com/Mic-Lock-Microphone-Blocker-Pack-Surveillance/dp/B01LPQJGA2/

Step 3: Securing your data and communications

A. Local data - email, contacts, photos, videos, etc.
   e. Encryption of data at rest to prevent full exploitation of your device if it is seized by law enforcement
      i. Turning on encryption for mobile phones
         1. iPhone - https://www.zdnet.com/article/how-to-turn-on-iphone-ipad-encryption-in-one-minute/
         2. Android - https://www.androidcentral.com/how-enable-encryption-android
      ii. Turning on encryption for laptops
         1. MacOS - https://support.apple.com/en-us/HT204837
         2. Windows - https://support.microsoft.com/en-us/help/4028713/windows-10-turn-on-device-encryption
   f. Turn off biometrics entry (FaceID, fingerprint), turn on passwords and passcodes
      i. This prevents physical forced entry of your biometrics to open your device
B. TOR browser: https://www.torproject.org/
C. Tails Operating System: operating system meant to run off of a USB drive, utilizes TOR protocol for web-browsing, somewhat complicated to get running but most secure
   a. https://tails.boum.org/about/index.en.html
D. VPN - there are various Virtual Private Network options available for free which make it hard to trace your online activity back to you.
   a. NordVPN, ExpressVPN, TunnelBear are all good options
   b. ProtonVPN noted for protection with Swiss laws
      i. Also recently open sourced their systems: https://protonvpn.com/blog/open-source/
   c. OpenVPN - set up your own, requires a higher level of technical sophistication but security is reliant on the user as opposed to a third party: https://openvpn.net/
   d. Bottom line: find one that works and that is well rated by third party organizations
E. Internet access - when do you trust wifi and bluetooth?
   a. What happens when you access a random wifi base-station? http://www.libelium.com/products/meshlium/smartphone-detection/

b. Keep off it unless you are sure of the network you're joining
c. Use a Faraday bag while in transit to protect your laptop and phone

F. End-to-end encrypted (E2EE) chat and messaging
   a. Many E2EE options available: Signal, Telegram, WhatsApp, Wickr, Confide, Dust, Wire
   b. Is Telegram secure? Not by default-- ensure secure chat function is turned on
   c. Signal is more secure than WhatsApp due to its privacy policies
   d. Wire is a good alternative too, and Semaphor for group chats
   e. Discord, Slack, Mattermost (self-hosted, open-source version of Slack)
   f. NSA created a guide to it here: https://media.defense.gov/2020/Jun/03/2002310067/-1/-1/0/CSI-SELECTING-AND-USING-COLLABORATION-SERVICES-SECURELY-LONG-20200602.PDF
G. Encrypted video conferencing solutions
   a. Many options available: Google Meet, Amazon Chime, Facebook Messenger Rooms, WhatsApp videoconference, Microsoft Teams
   b. Zoom re-enabled E2EE for its free users
   c. Jitsi is a viable open-source solution (self-hosted)
   d. See this guide: https://www.frontlinedefenders.org/en/resource-publication/guide-secure-group-chat-and-conferencing-tools
H. Encrypted email - there are free, encrypted emails available, including
   a. Protonmail (does not encrypt subject line) https://protonmail.com/
   b. Tutanota (encrypts subject line) https://tutanota.com/
   c. To encrypt attachments use Sendsafely https://www.sendsafely.com/

Step 4: Protecting yourself from malware (for more information see: https://securityinabox.org/en/guide/malware)

   a. Mobile
      i. Phishing via SMS
         1. Don't click on links from senders you don't know or recognize
   d. Laptop
      i. Phishing via email
   e. Antivirus - free solutions
      i. Sophos at home https://home.sophos.com/en-us.aspx
      ii. Bitdefender https://www.bitdefender.com/
      iii. Adaware https://www.adaware.com/
      iv. AVG https://www.avg.com/en-us/homepage#mac

Step 5: Use Anonymous File Transfer

A. Check this list of online file storage services that do not require sign up and comes with encryption for up to 30 days.

Other Suggested Reading:

https://securityinabox.org/en/

https://www.securityplanner.org/#/

https://media.defense.gov/2020/Jun/03/2002310067/-1/-1/0/CSI-SELECTING-AND-USING-COLLABORATION-SERVICES-SECURELY-LONG-20200602.PDF