Digital Privacy & Security Basics

Jay Colbert (he/they)
@_WildeAtHeart

jaylcolbert@gmail.com
jaylcolbert@tutanota.com
jaylcolbert@protonmail.com
jaylcolbert@disroot.org

What is Privacy?

Privacy is the *right* of an individual to control how much information about themselves they share with others, including governments and corporations.

What is Security?

Security is the *freedom from or resilience to* potential harm. In our case, it protects us against hacking, government surveillance, and corporate tracking.

This protection allows us to have privacy.

So will all this make me anonymous?

Privacy is the right to be selective about what you share about yourself.

Security protects your information from outside threats to provide that privacy.

But anonymity relies mostly on behavior. If you have the security to control your privacy, it is then up to you to take measures to make yourself anonymous. True anonymity is very difficult and often involves lifestyle changes and software investments (there are a lot of amazing free tools though).

Example: I have invested in the past month

- Over $100 for three years of a VPN
- $90 for physical encryption keys
- $10/year for password manager
- Will have to pay for my email services if I want to upgrade them.
- Might get routers and laptops dedicated to Linux/Qubes OS later

I’ve got nothing to hide, why should I care?

1. It’s your right to choose what you share about yourself.
2. If I asked for your bank password, would you give it to me? No? ***Then you should care about protecting it.***
3. The amount of data that corporations and governments take from us and use for financial gain and surveillance is huuuuuuge.
   a. If you’re using a completely free service, odds are *you’re the product.*
   b. Google monetizes your data gathered from search results, emails, YouTube, on and on and on
   c. Facebook and Google follow you around the internet to learn what you like, your behaviors, and your purchases.
   d. Geolocation
   e. Anything you’ve shared freely
   f. Photo metadata, and other metadata in general

Your Security Plan (or threat model)

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

Basic tools

FOSS if you can.

Check privacytools.io, Freedom of the Press Foundation, and Electronic Frontier Foundation for recommendations and criteria.

Avoid services based in the US (or the other 5 Eyes countries) if you can.

End-to-end encryption

Passwords

- Strong passphrases
  - Diceware
- Password managers
  - I use Bitwarden, with KeePassXC as an offline backup not connected to any servers.
  - Who owns the servers? Where are they? How are they encrypted? What information does the company get and keep? How do they use it?
- 2FA for added security
  - Apps tend to be flawed, most experts recommend a physical key, like Yubikey (which is what I have); you have to plug it in as the authentication.
- Password hygiene
  - Don’t use the same password twice, especially for important accounts
  - Lie in the recovery questions; it takes about two seconds for somebody to look up your mom’s maiden name and where you went to high school.

Browsers (for day-to-day use)

Google Chrome and all Google products (I say this, while having a Google account) collect data from you and aren’t very transparent about how they use it.

If you like the Chrome experience, it is recommended to use a Chromium-based browser instead. I use Brave, which comes with privacy tools built in. (I would use Firefox, but I play D&D and Roll20 acts up on Firefox for me.)

Firefox (with some modifications) is recommended above all others because of their business model and the level of control you get. Privacytools.io has a good guide for setting up Firefox.

Browser Extensions

- Ad Blocker
  - uBlock Origin
- Third-party tracker blocker*
  - Privacy Badger
- Forced HTTPS connections
  - HTTPS Everywhere
- Block Content Delivery Networks
  - Decentraleyes

Note that some of these might be redundant, and some browsers have these features already built in (like Brave and Tor)

Search Engine

Find a search engine that doesn't track your queries or build an advertising profile based on your searches.

- DuckDuckGo
  - Based in US, partly uses proprietary software
  - But Tor uses DuckDuckGo
  - Has an optional .onion address (only accessible on the Tor network), which guarantees your searches aren't tracked, collected, or identifiable
- Searx
  - PrivacyTools has their own public instance
  - Has optional .onion address

Secure Communication

- Signal for phone
  - People will try to tell you that the CIA has a backdoor, or that the CIA can bypass it. What the Wikileaks info actually revealed is that the CIA could hack people's smartphones due to user error to get into Signal. Signal's end-to-end encryption is still safe.
  - A tool is only as good as the person using it!
  - Endorsed by Edward Snowden
- Encrypted email
  - Protonmail or Tutanota. Benefit of Tutanota over Protonmail is that the subject line and who sent it etc is also encrypted, not just the content of the email. Neither is hosted in US.
  - PGP for Riseup/Disroot/Gmail/Outlook
    - PGP is pretty advanced, so I'll leave more info about it and maybe do another workshop on it. There are good tutorials online to follow.
    - Tutanota does not support PGP as it is slowly becoming outdated and there are better tools. It's really awesome for software validation and Canary watches, though!
- Jitsi for video calls
  - E2ee requires some extra setup
  - If you must use Zoom (for work, for instance), there are guides to doing that in a Virtual Machine.

Alright, let’s talk about Tor

What is Tor?

Tor (The Onion Router) is a network of virtual tunnels that allows you to improve your privacy and security on the Internet. Tor works by sending your traffic through three random servers (also known as relays) in the Tor network. The last relay in the circuit (the “exit relay”) then sends the traffic out onto the public Internet.

The Tor Browser is the primary/recommended way of accessing the Tor network. It comes pre-configured to allow for privacy, security, and censorship circumvention.

Important note: the software is completely free and open source. You can look at the source code on GitHub and examine it. If there were hiding something, we would know.

Who uses Tor?

- Activists
- Whistleblowers
- Journalists
- People in censorship-heavy countries
- Completely normal people who care about having control of their privacy

But also...

The Government & Tor

- Tor was not written by the government. Tor was written by Roger Dingledine, later on joined by Nick Matthewson, with the funding from the Naval research lab through Paul Syverson.
- Some developers on the Tor Project work for the Naval research lab still
- A good chunk of the Tor Project’s funding comes from various government agencies
    - This makes sense because they use it heavily
    - The Tor Project folks are actively searching for more sources of funding so that they don’t rely on government funding as much
    - Aside from funding, no government agency is involved with its development and maintenance

Tor Myths

- The government has a backdoor in Tor because it was developed by them and still funded by them. And you're helping the government by using it because you help them blend in!
  - Nope! Edward Snowden leaked a NSA presentation called "Tor Stinks" that shows how they still can't de-anonymize specific Tor users, nor can they do every Tor user. (They can, however, de-anonymize small random chunks, but never specific targets!)
  - If it didn't actually keep your privacy, then why would the government use it?
  - The more people use Tor day-to-day for normal things, the less it stands out for everyone (but sadly yes, this includes the feds).
- Tor keeps me completely anonymous!
  - Nope! While it does offer a shitload of privacy and security, anonymity is largely from *behavior*. It will anonymize where your internet traffic originates. *But your ISP will know you're using it, and there's always a chance websites you access will provide info if you give it to them.*
- What about the Deep Web? Is Tor just for criminals and drugs and pedophiles?
  - The Deep Web is just the parts of the internet that regular search engines don't index. The Dark Web requires specific configuration and networks (like Tor) to access.
  - Yes, you can do illegal stuff on the Dark Web. Please don't. (Unless those illegal things include overthrowing fascist regimes.)
  - Tor protects *all* privacy, so you are responsible for what you do and don't do.

But what about VPNs? All my favorite podcasts and YouTubers recommend them!

VPNs make sure that your IP address (which can be linked back to you) is not visible to the rest of the internet, and your ISP doesn't know what you're doing on the internet. Because they mask your true IP address and give you another one in another location, you can use it to access geo-locked services like Netflix. Good for basic day-to-day web browsing, but definitely not necessary.

VPNs do NOT make you anonymous. You should NOT have your VPN turned on if you're using Tor. (Except if you know what you're doing in extreme circumstances.)

Your VPN provider should not keep logs on you, nor should they be hosted in the US.

PrivacyTools recommends Mullvad, and so do I. I also use NordVPN because it has some extra bonus features, and was having a really good sale. I also like having options.

Behaviors

Digital Behaviors

- Change your passwords a few times a year
- Delete apps you don’t need
- Use Tor, Signal, and other privacy tools often to establish the habit and normalize it
  - Don’t just use these tools for things you definitely need to hide
- Encourage your friends to do the same!
- Be conscious about what you share online
  - Regularly check your Google activity and wipe it
- Check your social media security settings regularly
- Encrypt your devices
- Cover your webcam!

Protest Behaviors and Tactics

- Leave your phone at home.
  - If you can't, have it turned off
  - If you can't, put it on airplane mode with location services off
  - If you need to use it during a protest to coordinate, have your location services off
  - IMPORTANT NOTE: Even if you have your phone off or otherwise make it so it isn't giving any data, it isn't that hard to correlate that with the times of protests and connect the dots. If your security plan requires it, start randomly turning your phone off at random times of the day so that the behavior isn't abnormal anymore. Drive around with it on, etc.
  - Have a good unlock code. DON'T HAVE ANY BIO UNLOCKING ON DURING A PROTEST.
  - Make sure everything is backed up and encrypted.
- Don't take pictures of protestors. Only cops/violence.
  - For any pictures, blur out faces/identifiable features of protestors.
  - Remove metadata from the photos.
- Dress as plainly as possible. Cover up anything identifiable.
  - If you aren't worried about looking intimidating, wear all black. Sturdy boots, a hoodie, dark glasses. Make sure you're covered from head to toe. Wear different color layers in case you need to run, so you can strip while you run. If you can afford it and your security plan requires it, by shoes and clothes each time, from bargain bins, and don't rewear them: remember your footprint is identifiable.

- Don't use real names.
- Only tell people who need to know that you're going, and do so in an encrypted way.
- Bring water and first aid.
  - I also bring a charging block and a pocket knife (which is perfectly legal, and can be used for many more things than physical harm).
- Go with a buddy. A group is even better.
  - The reason black bloc is such a good tactic is that a large group all doing the exact same thing makes it harder to pick out individuals. *The person who punched Richard Spencer still hasn't been identified.*

Your privacy, security, and anonymity are only as good as your tools, network, and behavior.