Digital Privacy for the Paranoid

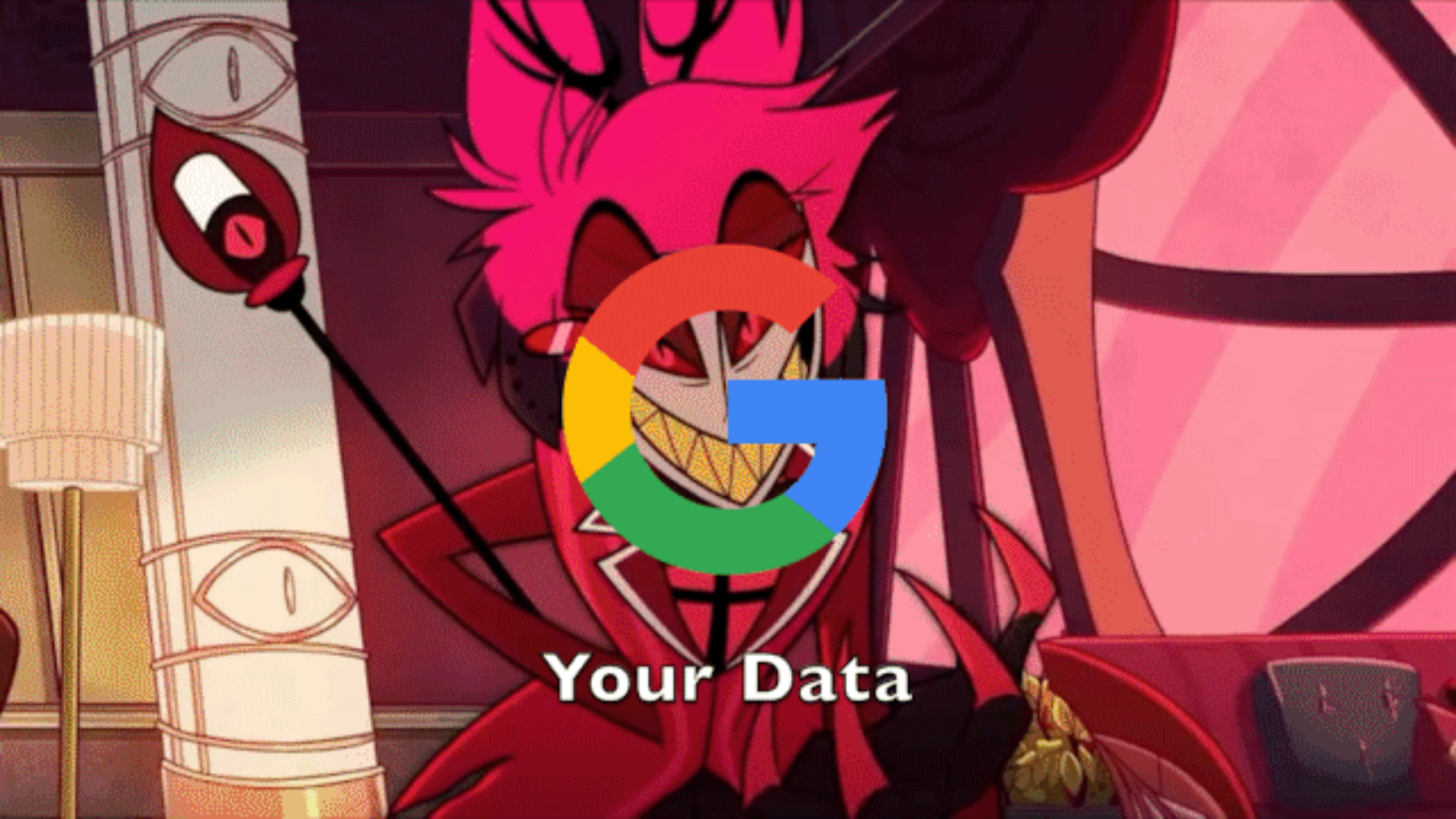
An introduction to tools for whistleblowing, evading censorship, and government surveillance.

An info dump by Jake Derouin

Disclaimer 1: Any political topics or positions referenced in this presentation are not guaranteed to represent my own political beliefs.

Disclaimer 2: Some scenarios presented in this presentation might reference activity that is illegal here or may be in another country. These are for examples only and I am not encouraging you to break the law.

Disclaimer 3: I am not a lawyer nor am I studying law. Additionally, if you are in a dangerous situation where your life depends on your privacy, do additional research on your own for additional op-sec tactics. I do not know your personal threat model.

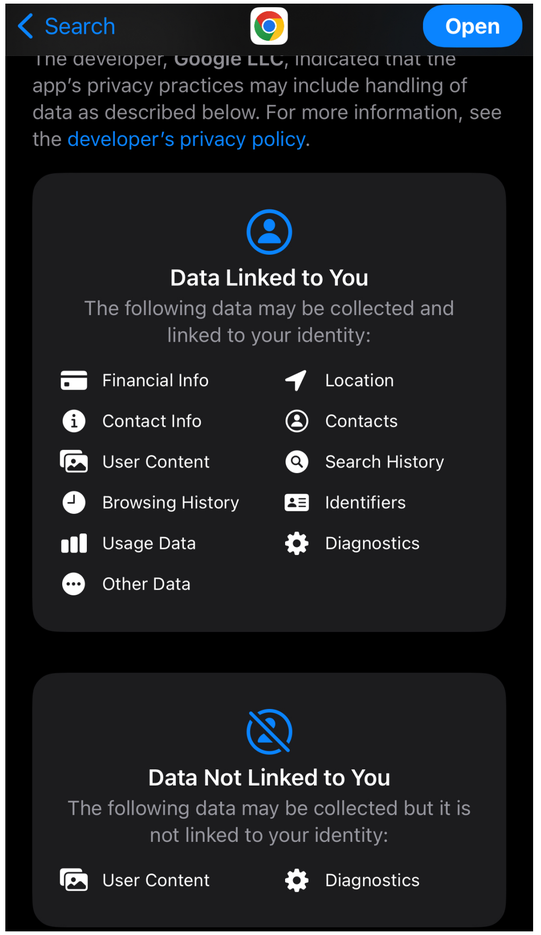

Your Data

Your browser

Example: Google Chrome

According to the App Store page for Google Chrome, Google may collect:

- Browsing History
- Search history
- How you use the app



Your operating system

Example: Windows 11

According to the the Data Collection Summary for Windows Microsoft may collect:

- Browsing History
- Apps you have installed
- Keystrokes and what you type.
- Much more

*some of these can be turned off but are on by default.

Data Category	Description	Examples
Browsing history data	This type of **Optional diagnostic data** includes details about web browsing in the Microsoft browsers.	• Browser activity, including browsing history and search terms in Microsoft browsers. • Changes to browser configuration impacting search experiences.
Device connectivity and configuration data	This type of **Optional diagnostic data** includes details about the device, its configuration, and connectivity capabilities.	• More detailed information about device settings and configurations.
Inking, typing, and speech utterance data	This type of **Optional diagnostic data** includes details about the voice, inking, and typing input features on the device.	• Samples of the content you type, write, or dictate on the device. • Details about status of transcribing input into text.
Product and service performance data	This type of **Optional diagnostic data** includes details about device or service health and performance.	• More detailed information about device and service health.

Your internet provider

Example: CenturyLink

CenturyLink may collect:

- Network activity
- Websites visited.
- Devices you connected.

- **Internet Services** - We gather and use data generated on our networks to manage, plan for future network development, market our services, and for operational efficiencies.
    - We may monitor our networks to check for viruses, to control spam, to prevent attacks that might disable our services, to ensure that your traffic does not violate your subscriber agreement or our acceptable use policies, and to guard against other inappropriate or illegal activity. This may include network traffic patterns, such as traffic volumes, beginning and ending points of transmissions, and the types of electronic applications.
    - We may also gather details from gateways, modems and/or routers; for example, the number and types of devices connected and the method of connection (Wi-Fi versus wired).
    - We may analyze some elements of your online activity, including websites visited, cookies, session logs, search history and website interaction analysis of your activity to include third party analytics, any changes you made to your account and other communications, such as past customer service calls, for purposes relating to new services, service changes, or promotional offers that may improve your customer experience. Please see our cookie notice for more details.

Your social media platform

Example: Instagram

Meta may collect:

- Your contacts you uploaded.
- How you engage with posts.
- Who you follow.
- How long you spend on a post
- Type of device
- More

racial or ethnic origin, philosophical beliefs or trade union membership) could be subject to special protections under the laws of your country.

- **Networks and connections.** We collect information about the people, accounts, hashtags and Facebook groups, and Pages you are connected to and how you interact with them across our Products, such as people you communicate with the most or groups you are part of. We also collect contact information if you choose to upload, sync or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping you and others find people you may know and for the other purposes listed below.
- **Your usage.** We collect information about how you use our Products, such as the types of content you view or engage with; the features you use; the actions you take; the people or accounts you interact with; and the time, frequency and duration of your activities. For example, we log when you're using and have last used our Products, and what posts, videos and other content you view on our Products. We also collect information about how you use features like our camera.

The websites you visit

Example: Google services (i.e Search, YouTube, Docs)

Google may collect:

- What you search.
- What you watch
- Who you contact.
- Ads you engage with.

Websites can also use trackers to follow your browsing activity online.

- Terms you search for
- Videos you watch
- Views and interactions with content and ads
- Voice and audio information
- Purchase activity
- People with whom you communicate or share content
- Activity on third-party sites and apps that use our services
- Chrome browsing history you've synced with your Google Account

If you use our services to make and receive calls or send and receive messages, we may collect call and message log information like your phone number, calling-party number, receiving-party number, forwarding numbers, sender and recipient email address, time and date of calls and messages, duration of calls, routing information, and types and volumes of calls and messages.

Your email provider

Example: Gmail, Yahoo, AOL, Outlook

Your mail providers may be collecting:

- Who you email.
- The content of your email.

AMERICA

Google Says It Will No Longer Read Users' Emails To Sell Targeted Ads

JUNE 26, 2017 · 5:40 PM ET

Laurel Wamsley

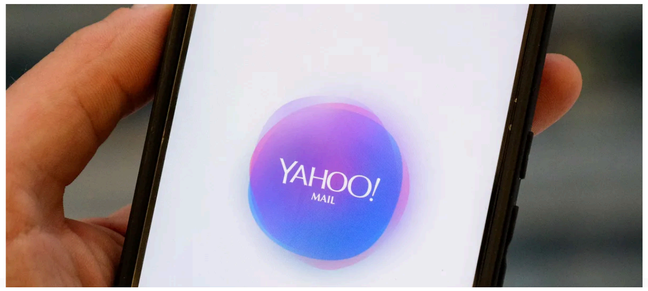
REUTERS

Exclusive - Yahoo secretly scanned customer emails for U.S. intelligence: sources

By Joseph Menn

TECH

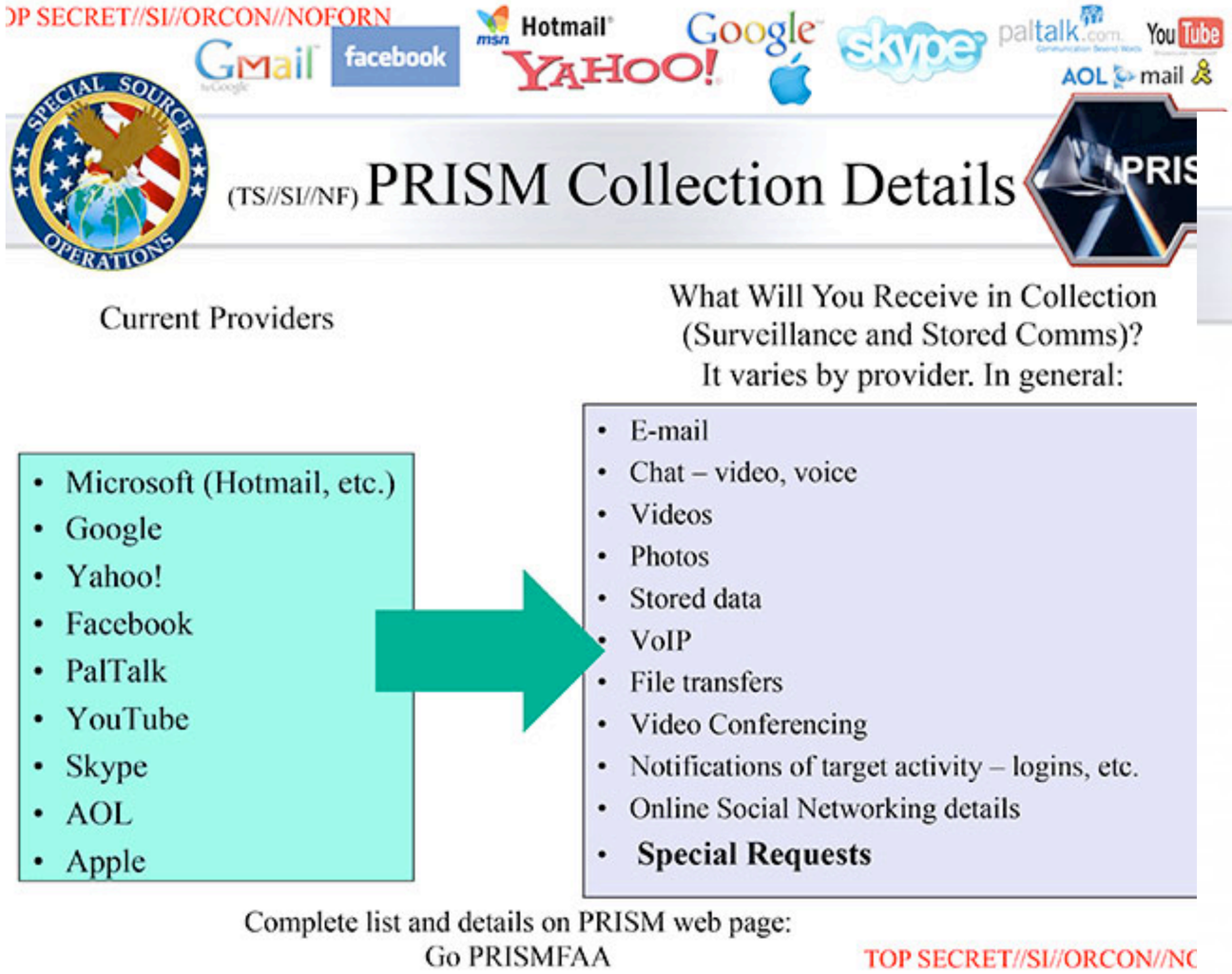
Yahoo Mail is still scanning your emails for data to sell to advertisers

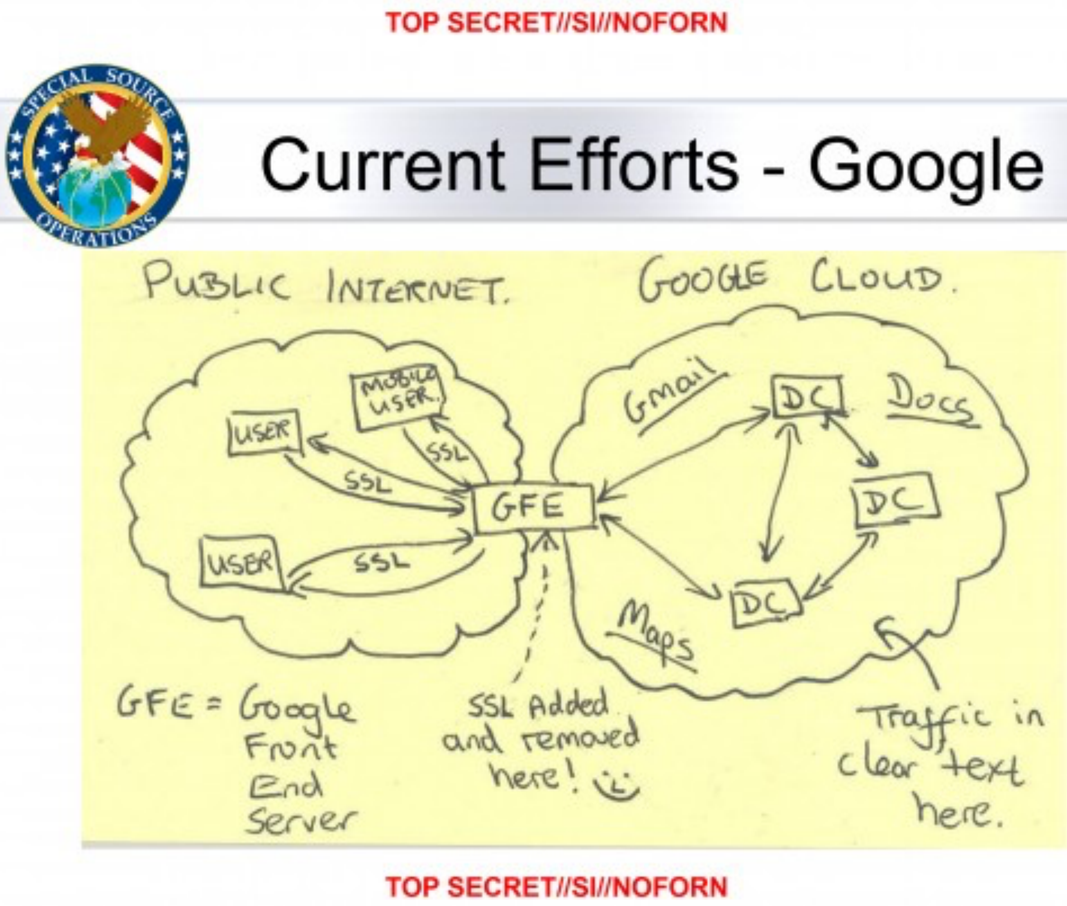


/ It knows you use Yahoo to contain your spam and retail emails, so it's going to analyze those and sell the data to advertisers

The US government is also in on this!

Example: NSA





What is this data used for? (It's not all bad)!

- Improving services
- Finding bugs and problems.
- Allowing for new features such as health devices that can detect potentially serious illnesses before they advance.
- Creating safer smart vehicles!
- Serving you targeted ads. (Yahoo scans your emails for this purpose).
- Selling your data to data brokers or other advertising services.
- Handing over information to the government when compelled to via a court order. (Or without a warrant in the case of some top secret national security deals).

A service advertised as "Free" usually means they profit off of your data in some way… and that might be ok!

This is NOT a doom and gloom presentation. It is a presentation that emphasizes that you have options if you are interested in having more control over your data.

Why should you care?

“But I don’t do anything illegal. I have nothing to hide.”

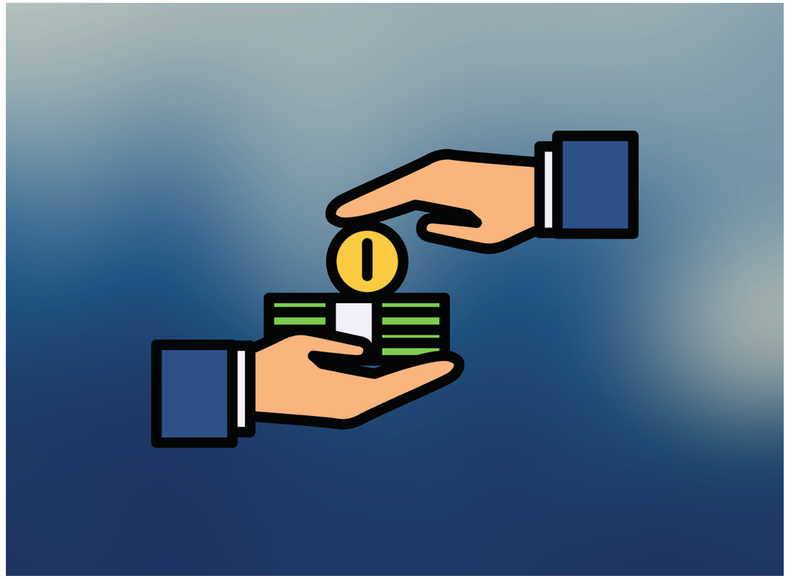
-Me prior to going down this rabbit hole.

Data on you is power over you.

Your attention and opinions and beliefs: Content you view and consume

How you are perceived by those with your data

When you give your data you give influence over



What you buy

How you fare in a legal setting.

For the rest of this presentation we will be focusing on

How you are perceived by those with your data

How you fare in a legal setting.

“But I don’t do anything illegal. I have nothing to hide.”

-Me prior to going down this rabbit hole.

What is legal today might not be legal tomorrow

Example: Roe v. Wade

Supreme Court overturns Roe v. Wade, ending right to abortion upheld for decades

UPDATED JUNE 24, 2022 · 10:43 AM ET

HEARD ON ALL THINGS CONSIDERED

By Nina Totenberg, Sarah McCammon

What is legal here might not be legal elsewhere

Example: LGBTQ Rights

WORLD NEWS

Mass arrests target LGBTQ+ people in Nigeria while abuses against them are ignored, activists say

Uganda's anti-LGBT laws: Man faces death penalty for 'aggravated homosexuality'

Your data might be used against you

Example: Political targeting of activists and evidence in legal cases

WORLD NEWS

China gives suspended death sentence to Chinese Australian democracy blogger Yang Hengjun

POLICY / TECH / META

Meta-provided Facebook chats led a woman to plead guilty to abortion-related charges

Cracking Down on Dissent, Russia Seeds a Surveillance Supply Chain

Russia is incubating a cottage industry of new digital surveillance tools to suppress domestic opposition to the war in Ukraine. The tech may also be sold overseas.

And…

If you are believe in something taboo or illegal today, using your voice and freedom of speech can push towards future change!

Sometimes one might want to be able to use their voice or freedom of information without being punished by governments or social circles for doing so.

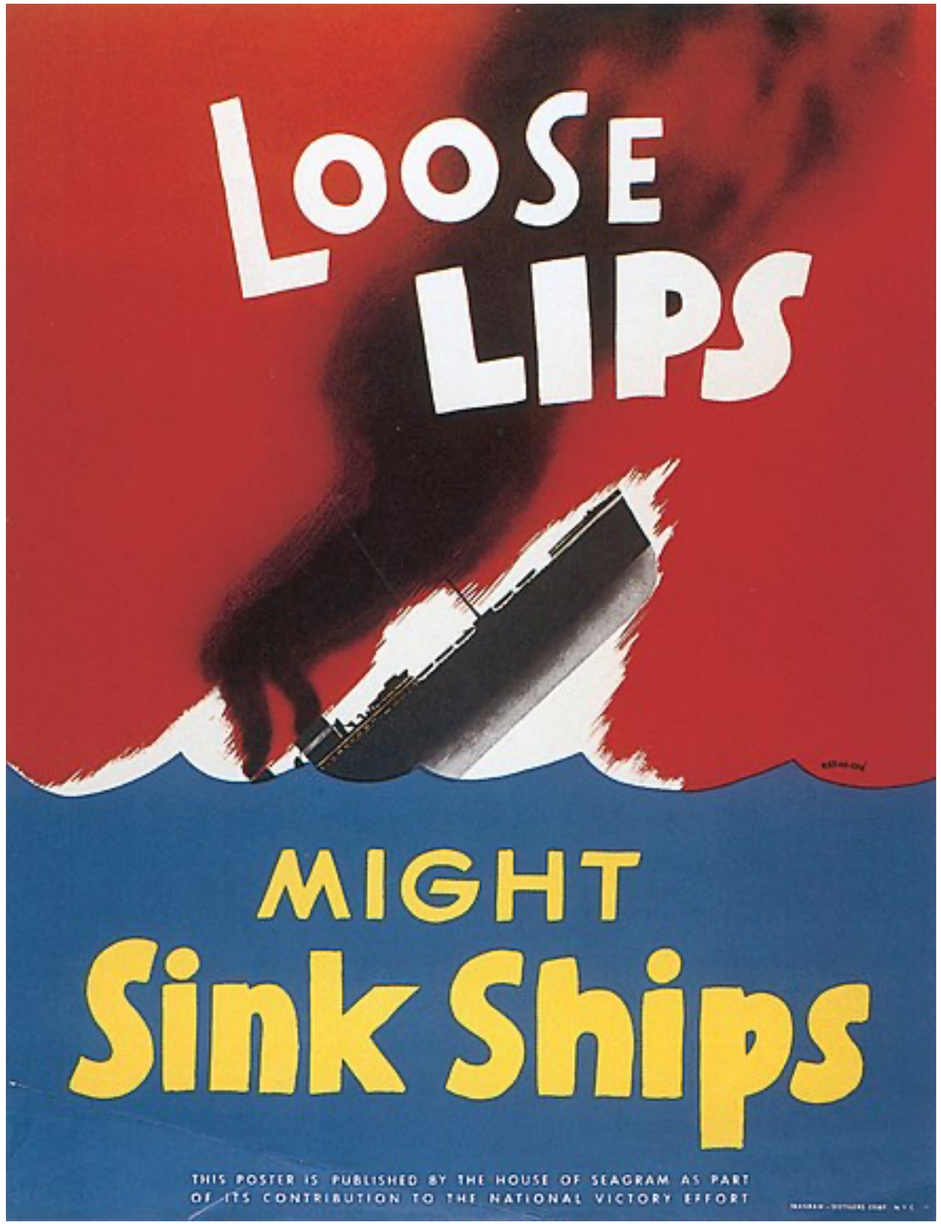
So what can you do?

It depends on your threat model and operation security needs!

Operation Security

Op-sec for short!

A counter espionage technique where one evaluates whether or not information about their own actions could be collected and used by an adversary.



Threat Modeling

A technique where possible threats to a person and or their goals are evaluated and necessary measures are taken to reduce the risk of this threats.

Persona 1: Ally wants to be in charge of her reproductive system.

Name: Ally

Location: Nebraska, United States

Goal: Obtain information on how to get a safe abortion out of state without fear of prosecution.

Threats:

- Internet service provider monitors and logs website activity.
- State has a history of obtaining a warrant against those accused of illegal abortions to search communication data.
- Harsh penalties for conviction.

Censorship

The most blatant example of Hong Kong's increasingly authoritarian moves to control speech online has been the efforts to ban 'Glory to Hong Kong' – a protest anthem that has become a symbol of the Hong Kong democracy movement, and which the authorities consider a threat to national security. The Hong Kong government has been seeking an injunction order to prohibit anyone from circulating the song 'in any way' and apply to 'any internet-based platform or medium' and its global operations.

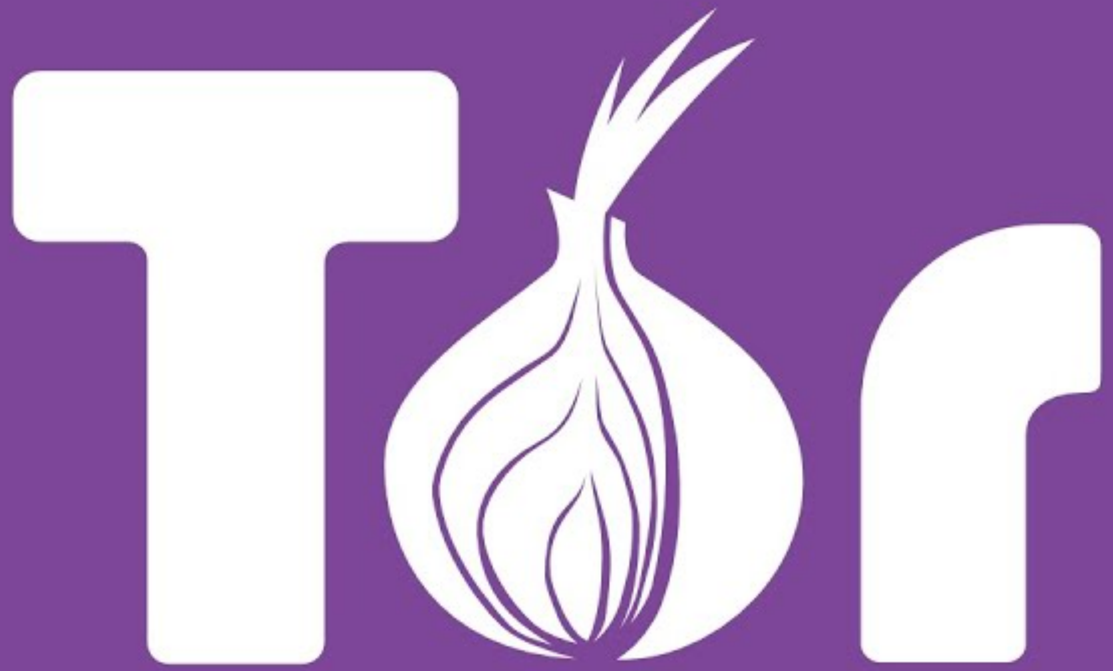
The legislation, signed into law by President Vladimir Putin on July 30, 2017, bans anonymous use of online messenger applications and prohibits the use of software to allow users to circumvent internet censorship. The new laws are part of Russia's widespread crackdown on online expression, in violation of human rights law and democratic safeguards.

Inside America's School Internet Censorship Machine

A WIRED investigation into internet censorship in US schools found widespread use of filters to censor health, identity, and other crucial information. Students say it makes the web entirely unusable.

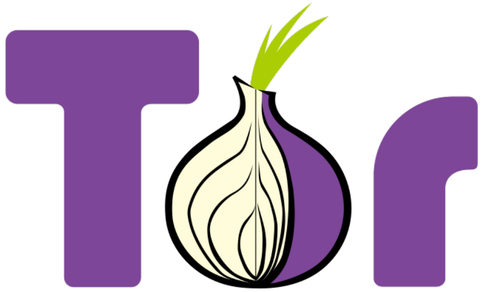
As important country-wide local elections loom, the Turkish authorities are once again intensifying efforts to control social media platforms through use of the restrictive internet law, demanding the blocking of content critical of the government. Social media platforms should take a firm, united stance against formal and informal pressure targeting expression protected under international human rights law, and adopt heightened transparency in the face of increasing online censorship.

The Tor Browser


Tor

Tool: Tor Browser

Category: Private web browsing



A free and open source browser that can circumvent **censorship** and allow for near total **anonymity** when browsing the internet when used correctly. Allows access to the dark/deep web.

Pros:

- Run by volunteers.
- Can circumvent censorship
- Funded by the US Department of State!
- Can be used to access the deep web and host websites without the host being known.

Cons:

- Slower than a VPN.
- Some websites block Tor access.
- Can raise suspicion in certain countries if used without a bridge.
- Despite the similarity in the name, you cannot torrent over Tor

Download Tor on your laptop

static.cyberwisp.com/deepdive.html

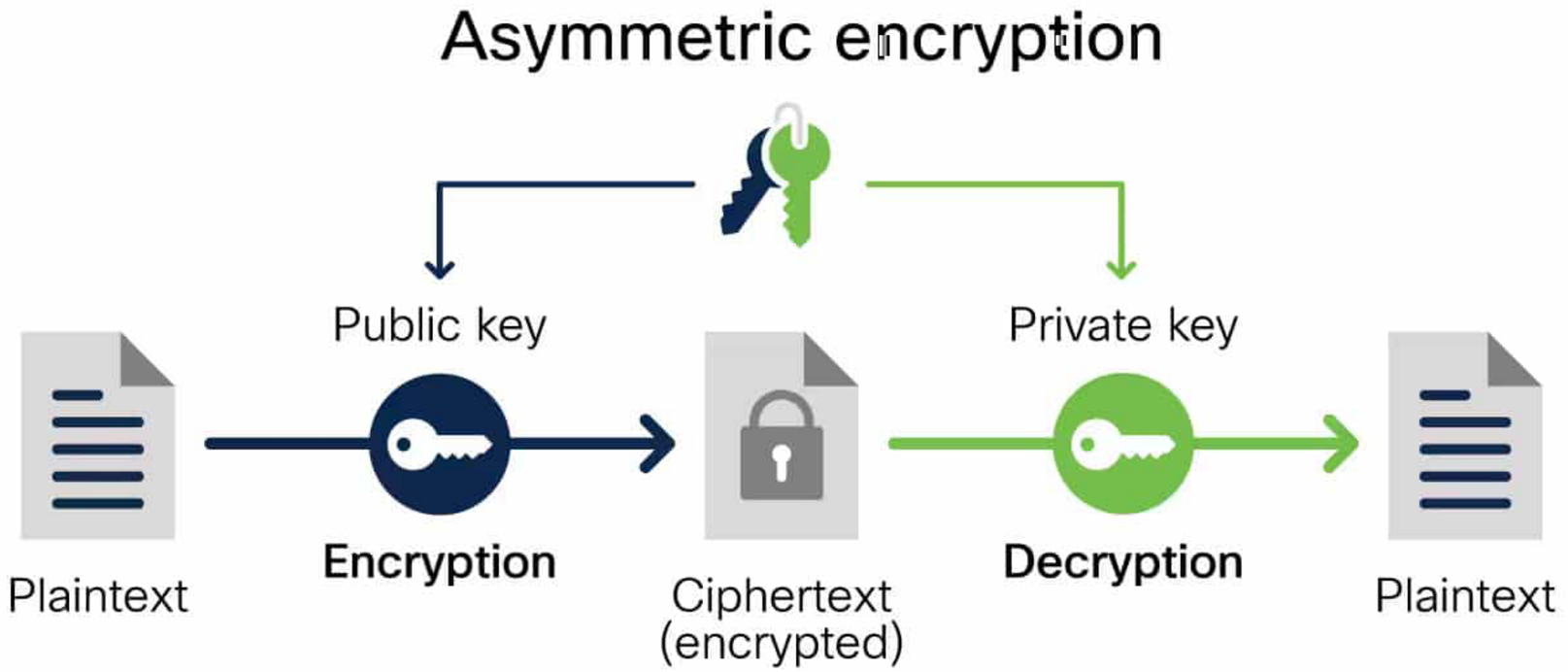
If you only have an iPhone with you, search

for Orbot in the App Store. Tor Browser is also

available on Google Play

Encryption

The process of scrambling data into an unreadable format such at only a person with a key can read it.

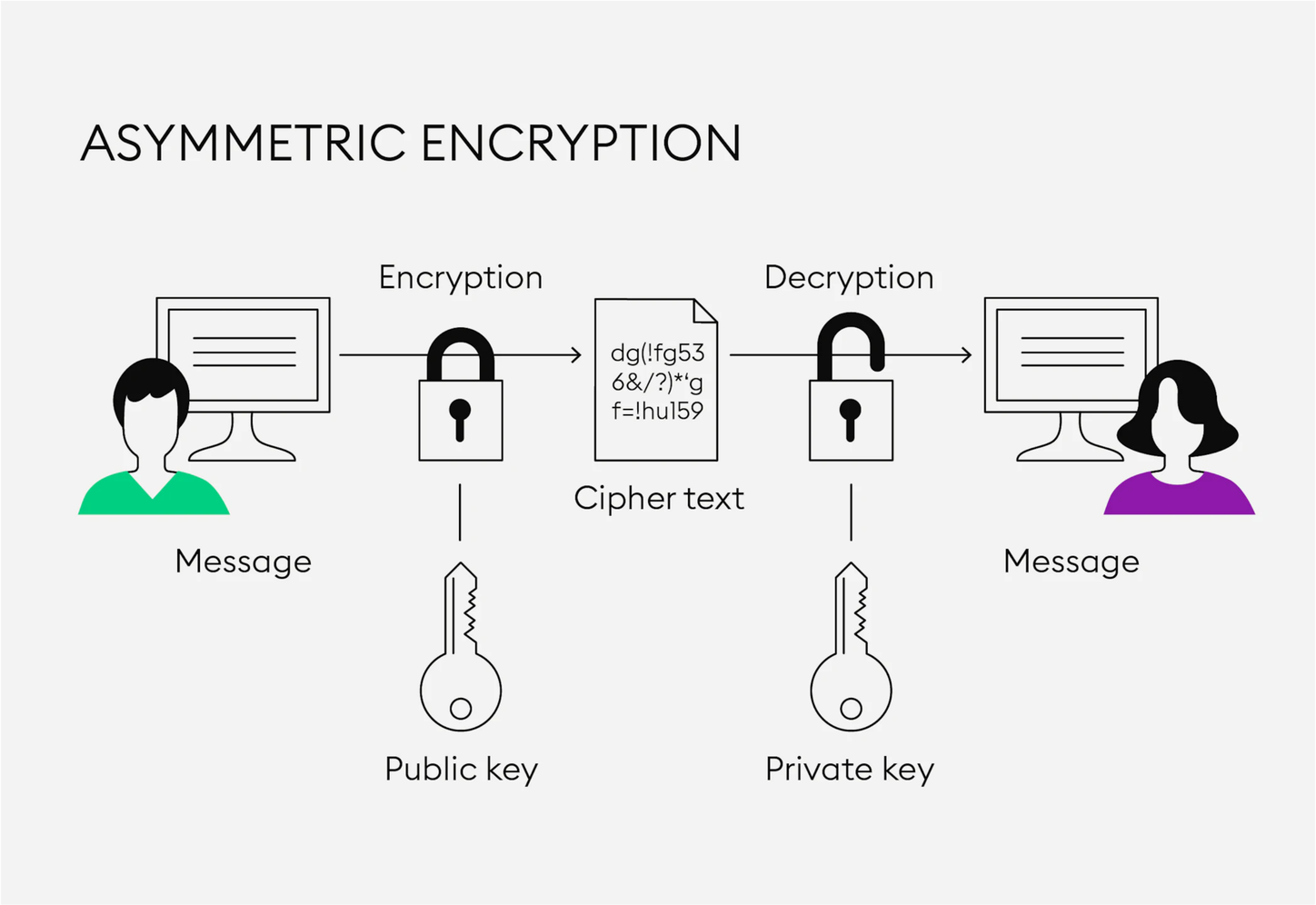


Asymmetric Encryption

Encryption involving two keys. A public key to “lock” the data and a private key to “unlock” the data.

Keys are exchanged first!

It does not matter if a third party intercepts your public key!



Asymmetric Encryption

Encryption involving two keys. A public key to “lock” the data and a private key to “unlock” the data.

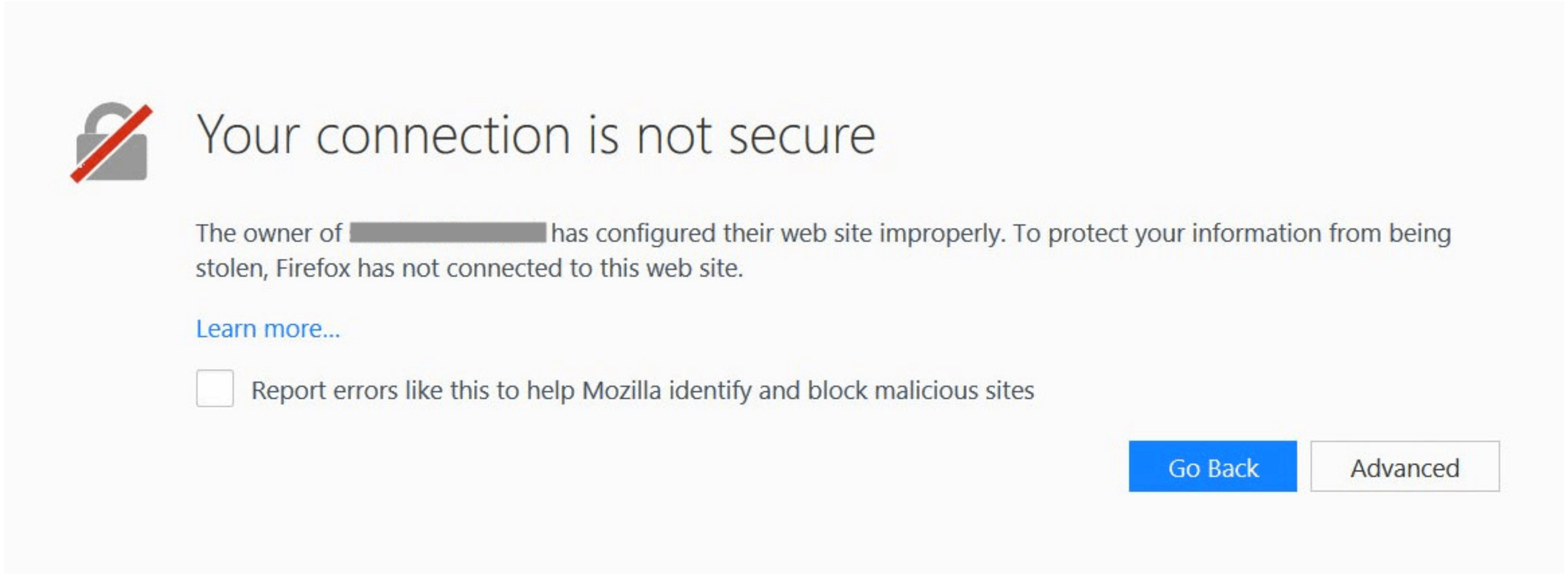
Common uses:

- Processes of transferring data.
- HTTPS
- Messenger apps
- Modern Email TLS*.

NOTE: This does not make something end to end encrypted by default.

*The email provider can still read your email unless you use PGP which is not covered tonight.

HTTPS

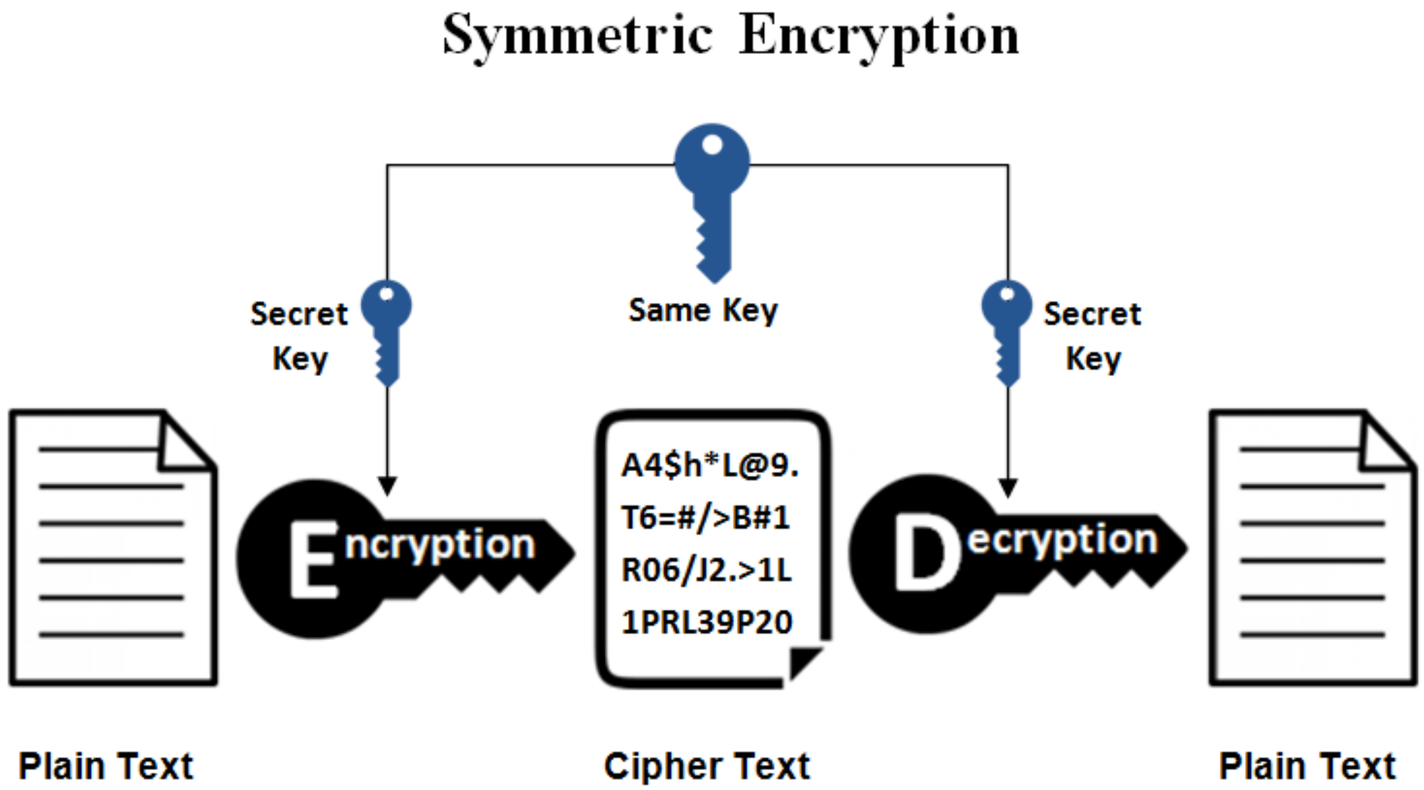


You can visit this site. BUT! DO NOT TYPE ANYTHING SENSITIVE!

Symmetric Encryption

Encryption involving one key used to “lock and unlock” the data.

The same key is used for both encryption and decryption. As a result, this key must be stored safely.



Symmetric Encryption

Encryption involving one key used to “lock and unlock” the data.

Common uses:

- **Drive encryption**
- Account data encryption.
- End-to-end encrypted data.

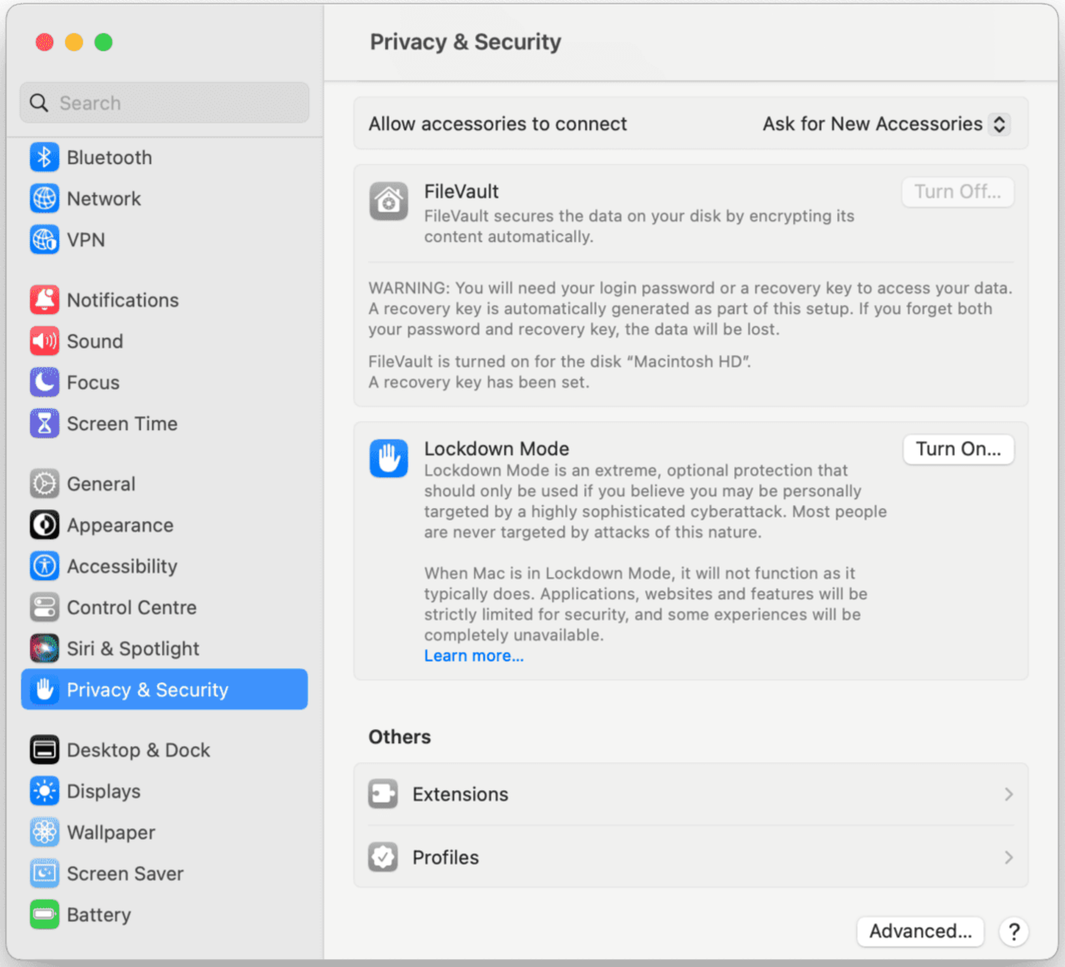
Drive Encryption (Full Disk Encryption (FDE))

Protect your phone and computer data from someone physically removing the drive for data extraction without your password

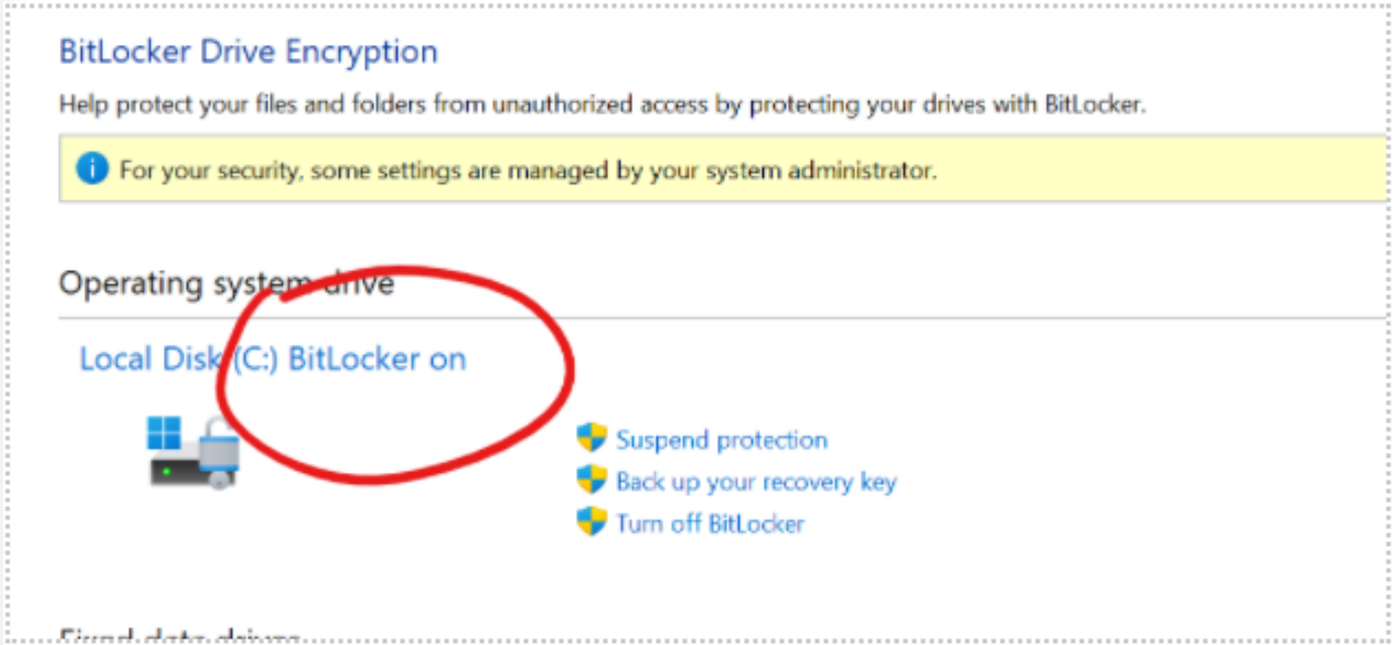
If you have an **iPhone** with a password, you already have FDE on! Ensure its a strong password!

Android users can check if theirs is on in settings security > Advanced settings > Encryption & credentials > Encrypt phone. Newer phones should have it on by default.

Drive Encryption (Full Disk Encryption (FDE))



FileVault: MacOS



BitLocker: Windows.

Only available on Windows 10 or 11 Pro

Tool: Veracrypt

Category: Drive Encryption Software

A free software that lets you use full disk encryption on many devices. Can also create hidden drives that support plausible deniability.

Great for Windows devices without BitLocker!

You can create invisible encrypted drives with VeraCrypt where you can essentially deny their existence (plausible deniability).

Tool: Monero (XMR)

Category: Anonymous purchasing

A cryptocurrency that allows for anonymous transactions without linking identities.

Pros:

- Allows for anonymous transactions
- Growing in popularity

Cons:

- Cryptocurrency is illegal in some countries.
- Difficult to purchase directly with real money due to government pressure (even in the US).
- Not widely accepted outside of the dark web.

Tool: Proton Mail

Category: Secure Email

A free swiss email service with a strong reputation for privacy and encrypted storage of users emails that is used by many activists.

Pros:

- Emails are end-end encrypted at rest so they cannot be accessed by anyone without your password.
- Allows for anonymous account setup (with a couple steps)

Cons:

- Email is fundamentally not secure.
- Emails with a non-Proton Mail user will not be encrypted on the recipients side.
- Some features are behind a paywall.