Personal Privacy

I don’t have anything to hide, right?

Who Are We?

Jack Norman

Jack Norman is an information security leader and consultant with over 20 years of software development and information security experience in the defense, public, and private sectors. In his role as Chief Information Security Officer Jack has supported dozens of acquisitions, an IPO, implemented multiple compliance projects, and architected numerous information security programs.

Jack is also a professor at Full Sail University, and holds a Master’s Degree in Information Assurance and Cyber Security from the Florida Institute of Technology, an Executive MBA from the University of Central Florida, and a CISSP certification.

Joe Tegg

- Husband
- Father
- 25yr+ Security guy
- Recovering BOFH
- Covert Technologist

Agenda

0830 - Welcome / Breakfast

0900 - Introduction - What is Privacy?

0930 - Digital and Physical Breadcrumbs

1100 - Threat Modeling

1200 - Lunch

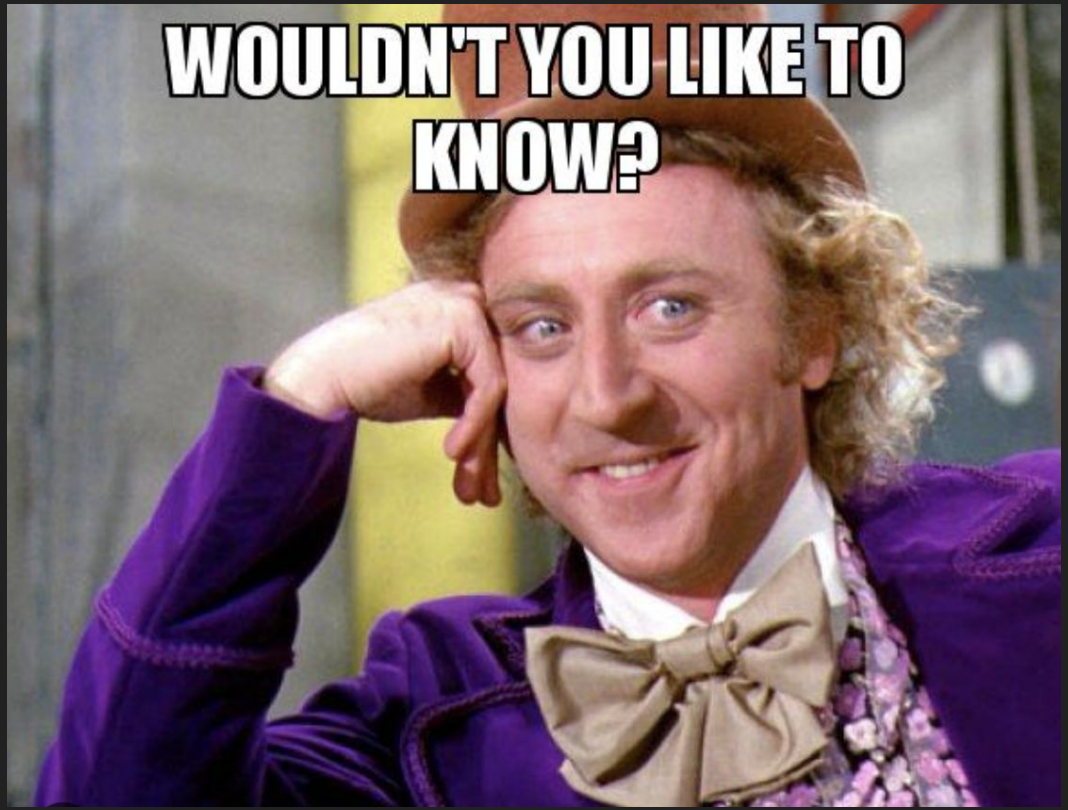
1230 - Digital Privacy

1500 - Physical Privacy

1630 - Peeling the Privacy Onion

INTRODUCTION - WHAT IS PRIVACY?

What Are You Looking To Get Out Of This Training?

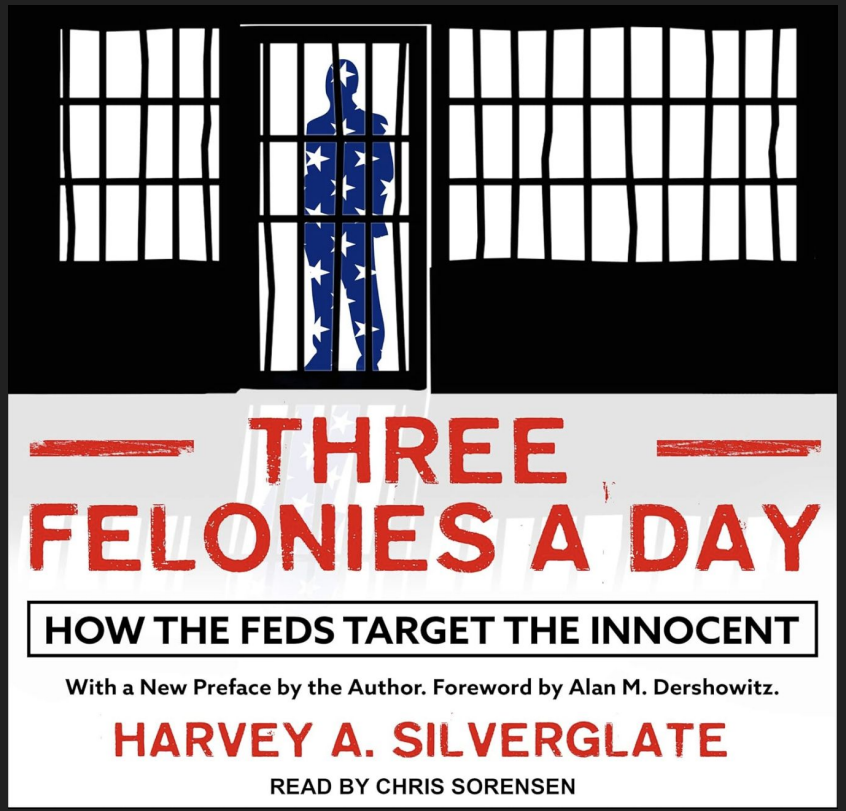


What is Privacy?

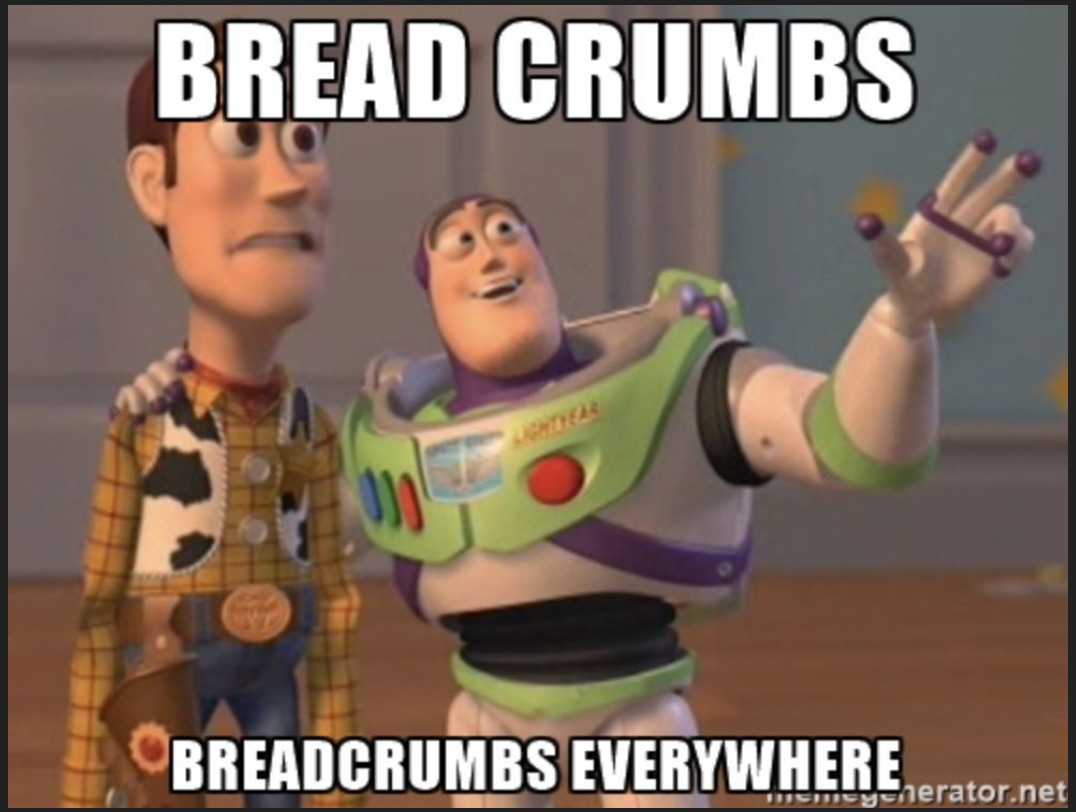
noun

- the state or condition of being free from being observed or disturbed by other people.
- the state of being free from public attention.

Why Should You Care About Privacy?



DIGITAL AND PHYSICAL BREADCRUMBS

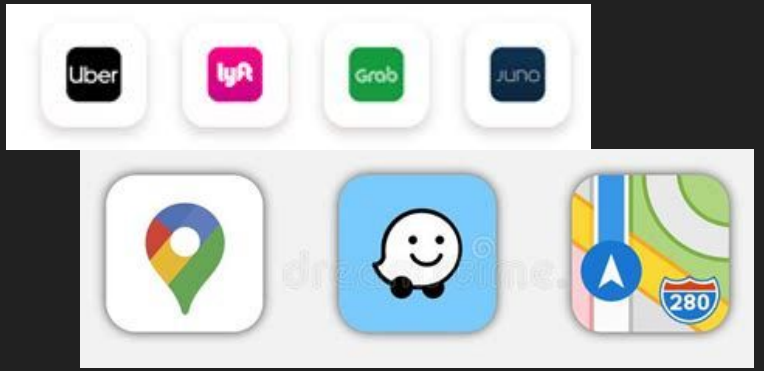


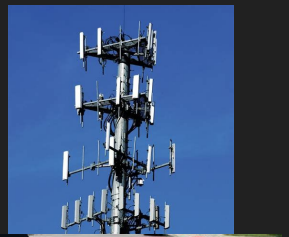
What is a digital breadcrumb?

: something (such as a hint or clue) that serves to lead or guide *(to a user identity or individual)*

What about these?

What about physical breadcrumbs?

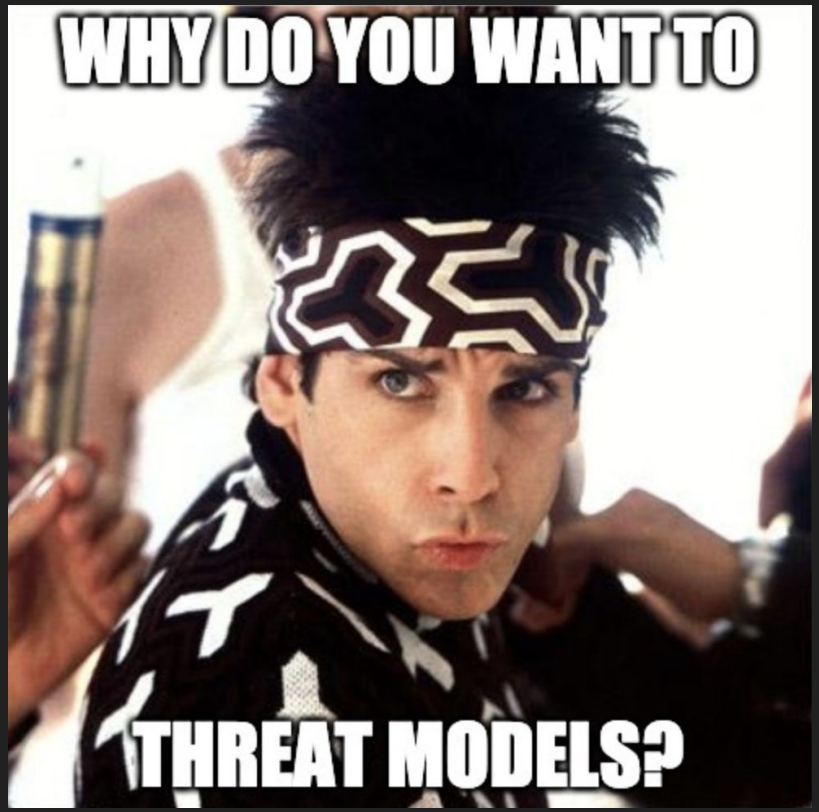




Field Trip!

Digital Footprint Activity

THREAT MODELING



What is Threat Modeling?

verb

a structured approach that aims to identify and prioritize potential threats and vulnerabilities. It involves identifying potential attackers, their motivations, and the methods they might use to exploit vulnerabilities of a subject.

Why YOU Need To Threat Model?

Who Are You?

Are you a public figure (e.g. politician, actor, priest)?

Do you own a lot of assets (e.g. wealth, jewelry)?

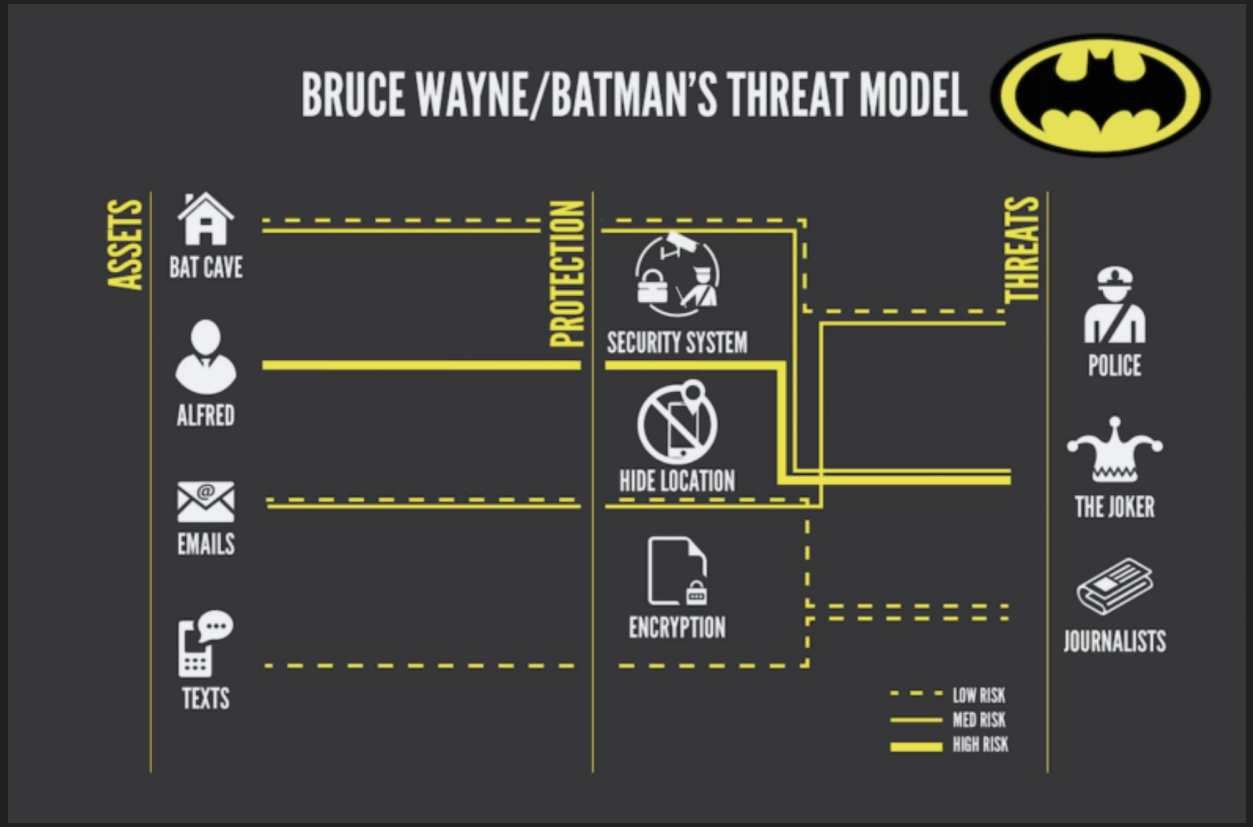
Are you a victim (e.g. domestic abuse, stalker)?

What do you do (e.g. profession, clubs, hobbies)?

What is your public perception (e.g. liked, loved, hated)?

How much time do you have?

Are You ….Batman!



Source: arstechnica.com

Where Do I Start?

What do you want to protect (e.g. data, communications, physical possessions)?

Who do you want to protect it from (e.g. people, organizations, criminals)?

How likely is it that you will need to protect it (e.g. your level of responsibility)?

How bad are the consequences if you fail (e.g. death, financial ruin)?

How much trouble are you willing to go through in order to try to prevent these consequences (e.g. money, time, effort)?

Source: ssd.eff.org

LUNCH

DIGITAL PRIVACY

What Do the Pros Do?

Source:
arstechnica.com

Operating System Best Practices

DO…

- Use host-based firewall
- Disable location services / telemetry
- Use local accounts
- Minimize software
- Secure DNS (e.g. Cloudflare, PiHole)
- Delete your data securely (e.g. Bleachbit, DBAN)
- Use virtualization and containers (e.g. VirtualBox, Docker)
- Use Linux

DO NOT…

- Backup to the cloud
- Use “cracked”, untrusted software, or “free” software

Demo Time!

VBox w/ Tails
Secure DNS
Little Snitch / Windows Firewall

Browser Best Practices

DO…

- Use a modern browser, apply updates!
- Minimize browser plugins
- Use a pop-up blocker, understand what is tracking you!
- Use HTTPS (The “S” stands for secure)
- Use a Virtual Private Network (VPN)

DO NOT…

- Use public or free WiFi
- Let your browser store your passwords
- Enter any personal information into an unexpected pop-up

“Think of the internet as a public place. Do not leave your details lying around!”

Demo Time!

Firefox w/ Containers
Brave Tour
Privacy Badger / uBlock Origin

Email Best Practices

DO…

- Use a strong and unique password
- Use two-factor authentication
- Strategically use temporary email addresses
- Use secure email service
- Use encryption
- Unsubscribe from mailing lists
- Delete emails older than 180 days!

DO NOT…

- Use a simple password
- Click on suspicious attachments/links
- Enter any personal information into a pop-up screen
- Use real information for “Security Questions”

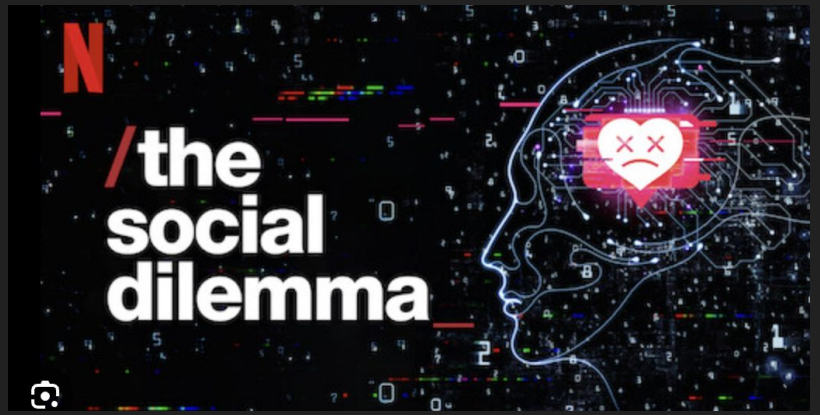
Demo Time!

- Proton Mail
- Temporary Email
  - 10 Minute Mail
  - Guerrilla Mail

Social Media Best Practices

DO…

- Use privacy settings
- Understand the terms and conditions
- Use false information strategically
- Use group shot for your profile picture
- Use caution before clicking links
- Minimize third party applications



DO NOT…

- Post ANYTHING that you would not want your employer to see!
- Interact with content
- Use your legal name as your profile name
- Post about future travel plans

"If you are not paying for it, **YOU** are the product!"

Story Time!

How PIs use social media
Documentary Review - The Social Dilemma

Mobile Device Best Practices

DO…

- Lock your device with a password or PIN
- Keep your software up-to-date
- Strategically use faraday bags
- Enable the ability to remotely wipe your device
- Use a secure phone (Purism, Unplugged)

DO NOT…

- Leave WiFi and Bluetooth on all the time
- Send any image/video that you do not want to be public!
- Jailbreak/Root your device

"If Beyonce's high-powered legal team cannot get pictures removed from the Internet …NEITHER CAN YOU!!!"

Demo Time!

iOS / Android privacy best practices

PHYSICAL PRIVACY

Home Privacy Best Practices

DO…

- Use physical security measures (e.g. door devils, quality locks)
- Disable devices that listen (e.g. Google Home, Alexa, Siri)
- “Roll-Your-Own” security surveillance
- Minimize WiFi connections
- Use _nomap at the end of your WiFi SSID name
- Talk to your neighbors

DO NOT…

- Make your home “smart”
- Make your home stand out

Field Trip!

Camera System (Unifi, Reolink)
Physical Security (Door Devil, Locks, privacy tint)

Vehicle Privacy Best Practices

DO…

- Use garage or back into your driveway
- Put visor down when going through tolls or areas with cameras
- Tint your windows
- Use vehicular trusts

DO NOT…

- Drive a vehicle that stands out
- Use automatic toll services (e.g. Sunpass, EZ Pass)
- Use vehicle manufacturer mobile apps
- Use OnStar / LoJack
- Drive erratically

Story Time!

Flock cameras
What “can” be done

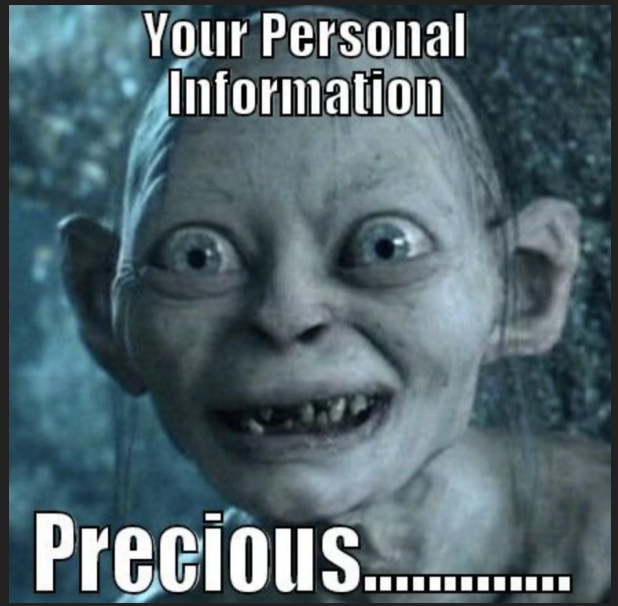
Personal Privacy Best Practices

DO…

- Leverage legal structures (e.g. LLCs, Trusts)
- Freeze your credit (and your loved ones)
- Opt out of marketing junk mail DMAchoice.org)
- Opt out of credit card and insurance offers (optoutprescreen.com)
- Use nomad residency
- Use PO Box or CMRA (Commercial Mail Receiving Agencies)
- Understand what data has been collected about you

DO NOT…

- Freely give away personal information
- Put utilities in your name
- Directly work for an employer



Demo Time!

Opt outs
Bazzell Guide Tour

Physical Privacy Best Practices

DO…

- Wear anti facial recognition clothing
- Leave primary phone at home (use burner)
- Adjust your daily routines / routes
- Walk in crowds
- Use cash

DO NOT…

- Look directly at public cameras with uncovered face
- Purposefully avoid cameras
- Use digital health monitors

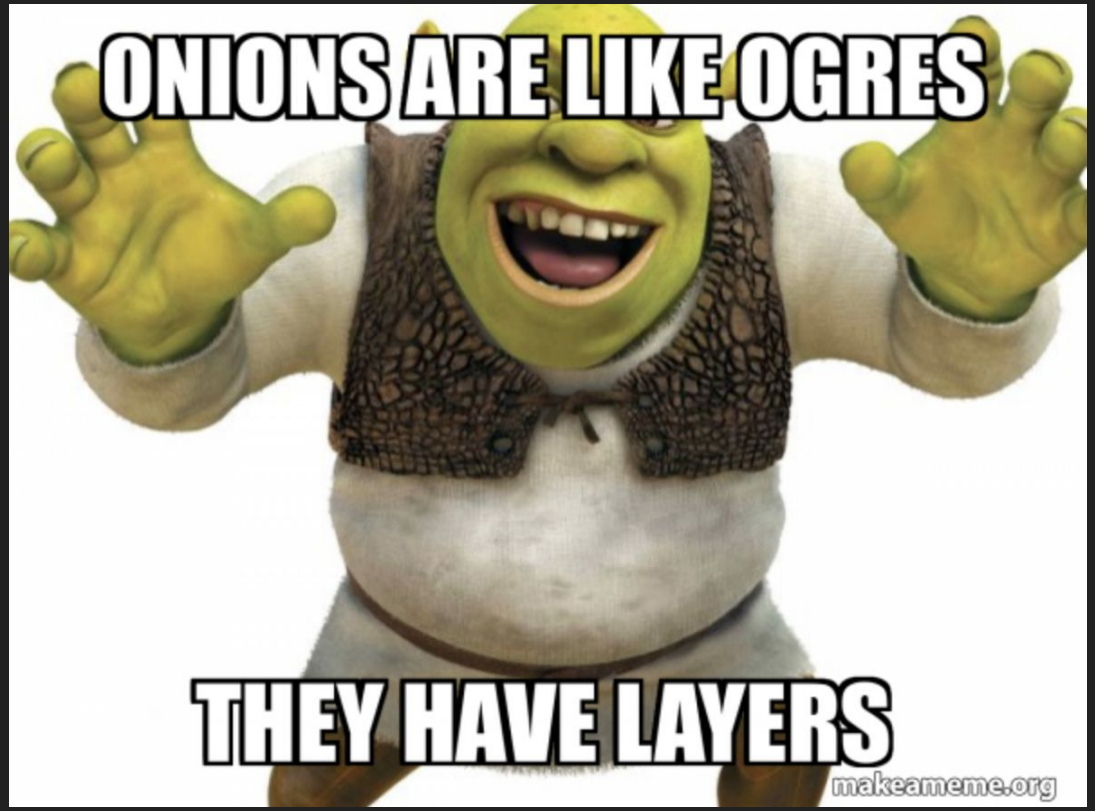
Story Time!

Police misuse of facial recognition

Clearview AI

Facial Recognition in Retail

PEELING THE PRIVACY ONION



Resources

FTC: How to Stop Junk Mail - https://consumer.ftc.gov/articles/how-stop-junk-mail

A Guide for Nomads - https://issuu.com/rootlessliving/docs/rootless_living_issue_22_may_june_2023/s/25470439

IntelTechniques (Michael Bazzell) - https://inteltechniques.com/index.html

EFF Surveillance Self-Defence - https://ssd.eff.org/