DS 593: Privacy in Practice

Surveillance Cont’d

Instructor: Alishah Chator

News?

Last time

- End to End Encryption
- Defining Surveillance

Today

- Exploring targeted and mass surveillance by the state, corporations and other actors

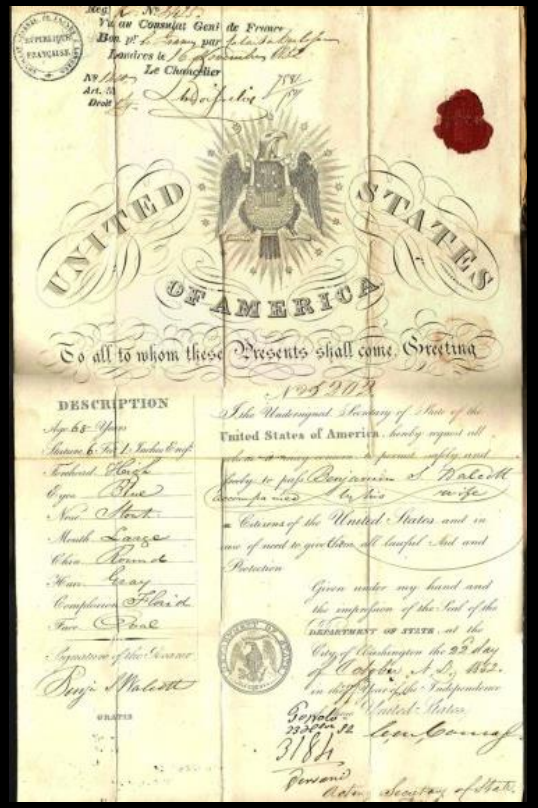
Brief History of Surveillance

- Targeted surveillance as a concept dates back to prehistory
  - Tactics have evolved over time

- Mass surveillance is a relatively newer phenomenon
  - As is mass *targeted* surveillance

City Watches and Patrols

Papers and Documentation



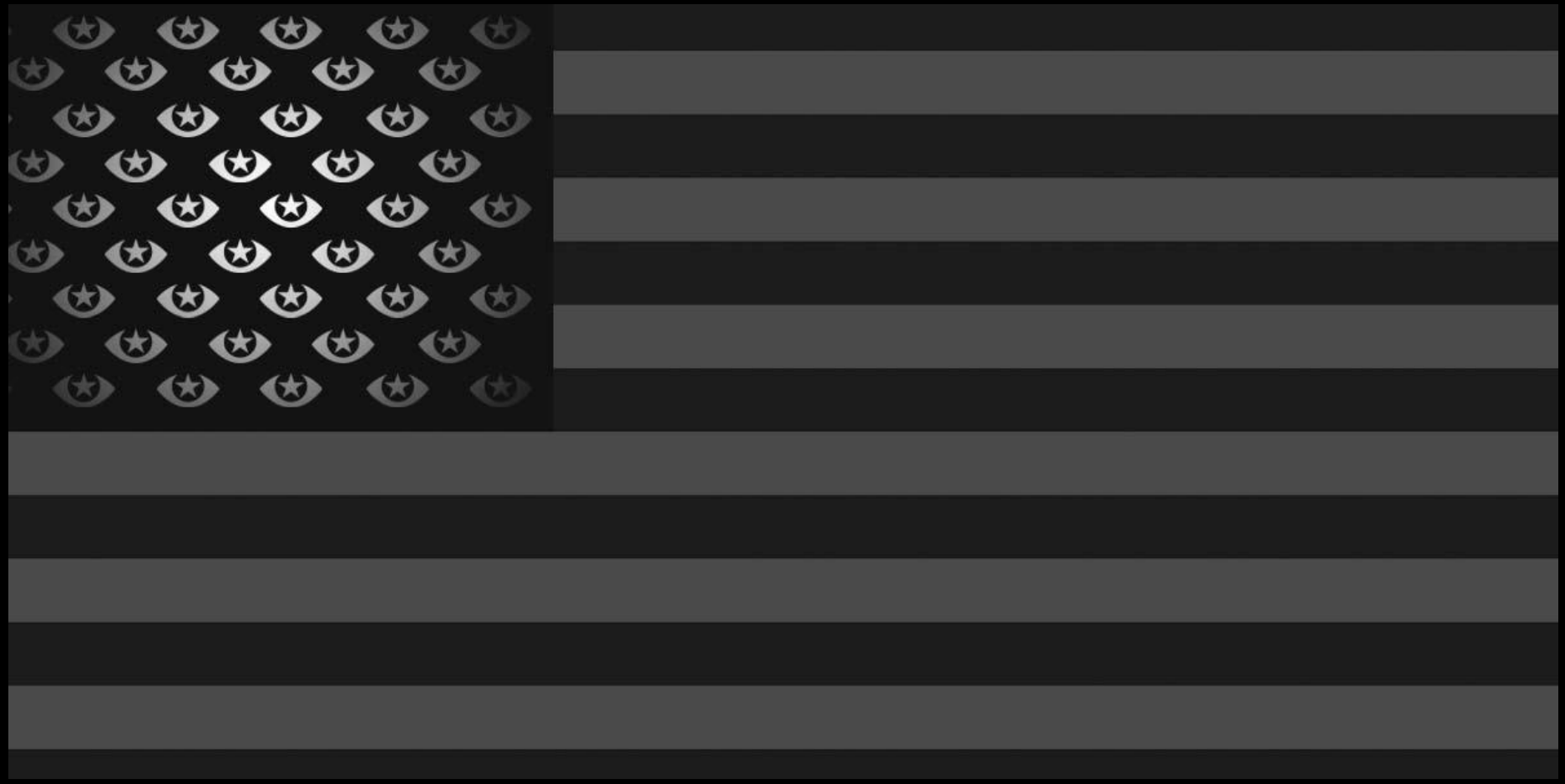
Red Scare and COINTELPRO

COINTELPRO

The FBI's Covert Action Programs Against American Citizens

Church Committee: Book III, Vol. 1

The PATRIOT act

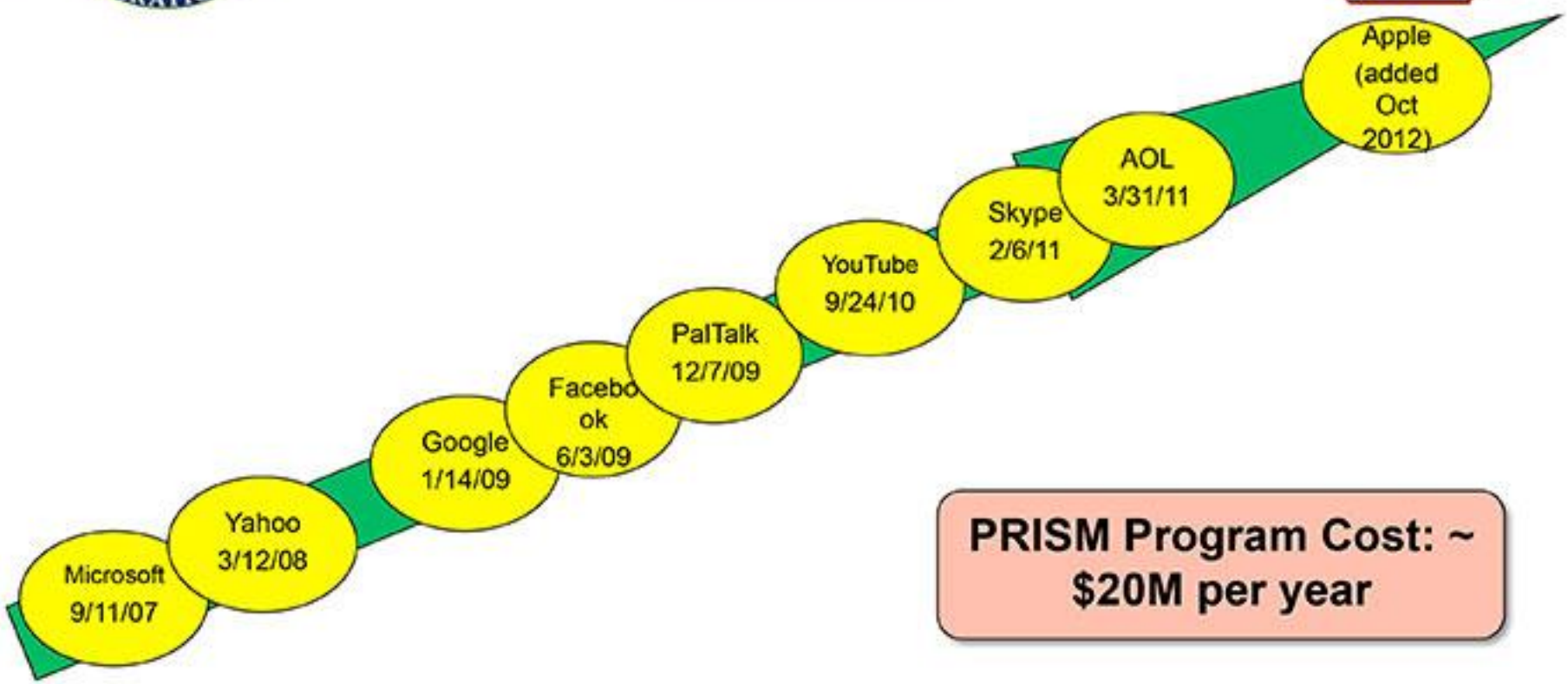


PRISM

The Snowden Revelations

- Given this history, why where these revelations such a big deal?

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider



PRISM Program Cost: ~ $20M per year

Aggregation and Analysis

- Machine Learning!
  - XKEYSCORE
  - Dataminr
  - Palatir
  - EMBERS

Surveillance Tools and Tactics

- Street-level or physical surveillance tools

- Surveillance of digital communications

Stingrays

Drones

Recording Devices

Automated License Plate Readers

Gunshot Detection

Warrants and Gag orders

Zero Day Attack

A successful exploit using zero-day vulnerability to damage the system

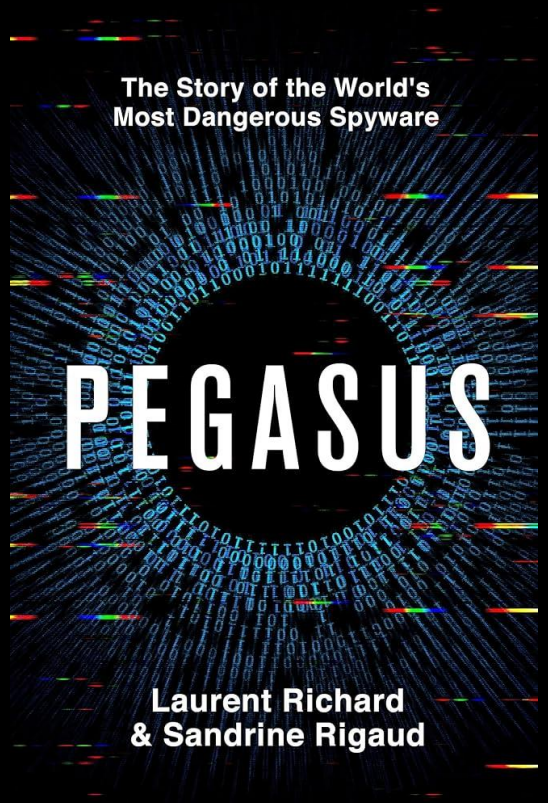
Zero Day Exploit

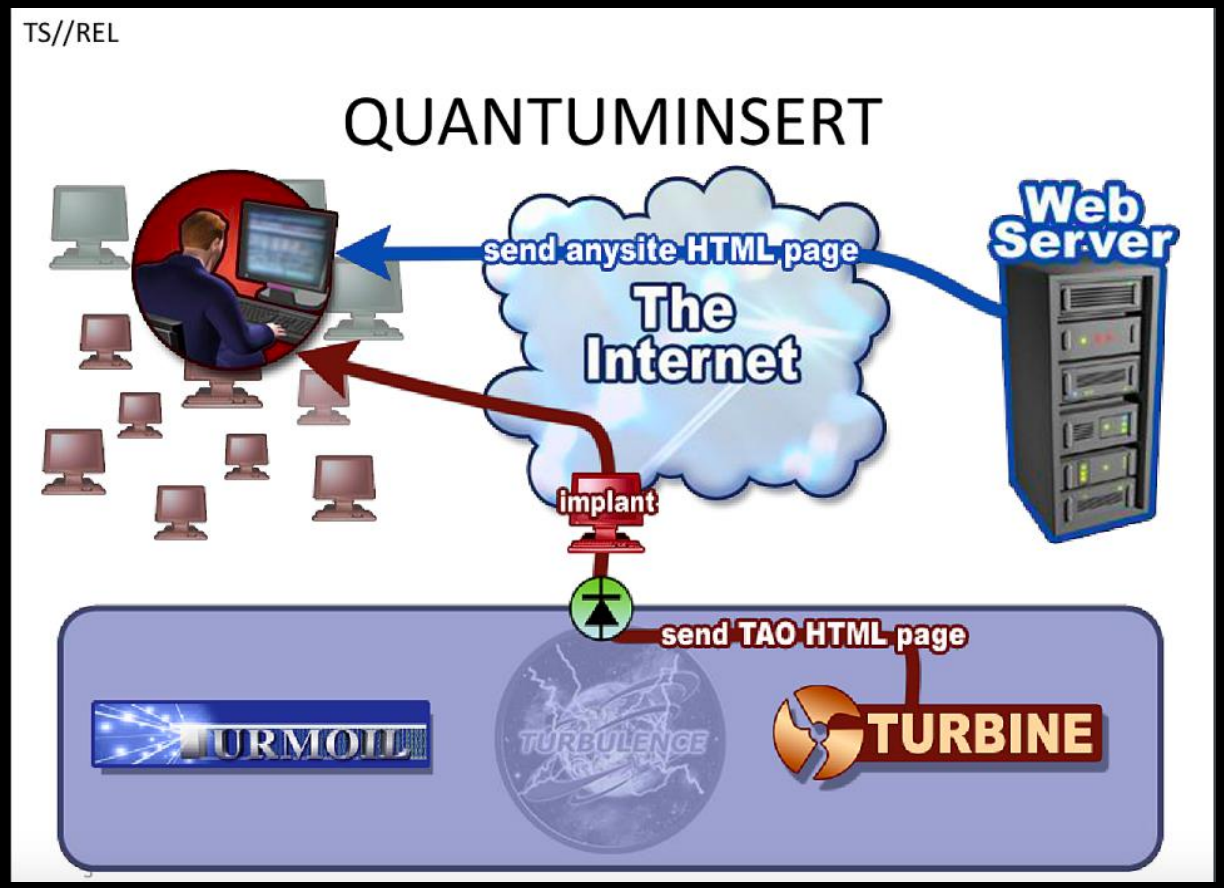
Technique used by hackers/crackers to escalate privileges using zero-day vulnerability

Zero Day Vulnerability

A software bug unknown to the vendor or parties interested in fixing it

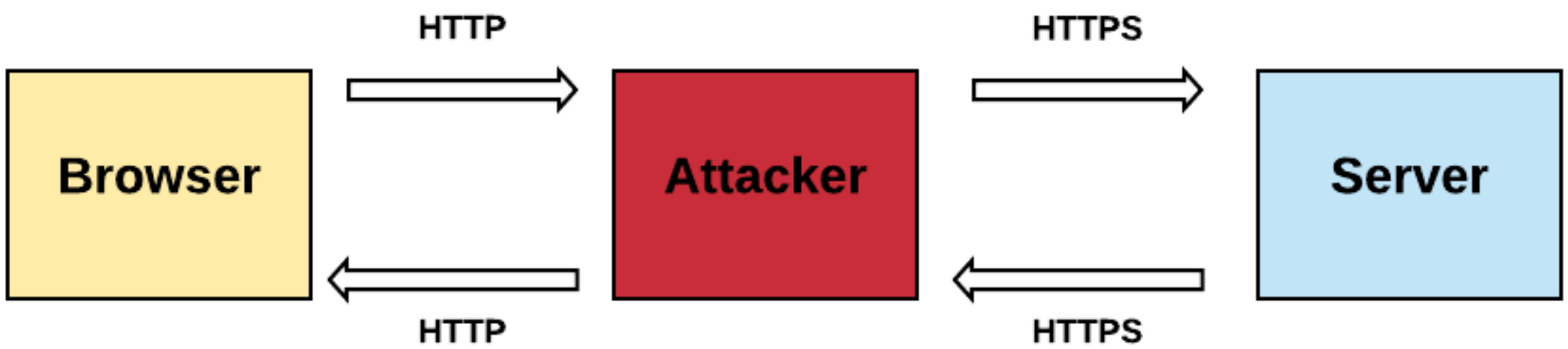
Spyware


The Story of the World's
Most Dangerous Spyware
PEGASUS
Laurent Richard
& Sandrine Rigaud


TS//REL
QUANTUMINSERT
send anysite HTML page
The Internet
Web Server
implant
send TAO HTML page
TURMOIL
TURBULENCE
TURBINE

Extraction tools

Downgrade attacks

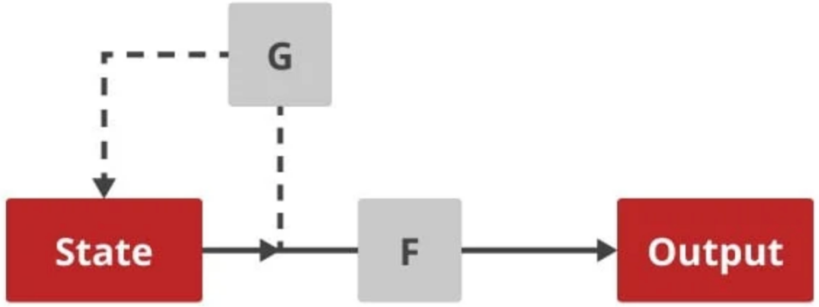


How the NSA (may have) put a backdoor in RSA's cryptography: A technical primer

2014-01-06

Nick Sullivan

9 min read



https://blog.cloudflare.com/how-the-nsa-may-have-put-a-backdoor-in-rsas-cryptography-a-technical-primer/

Who else is interested in monitoring you?

How do companies track everything we do?

- Identification is the name of the game

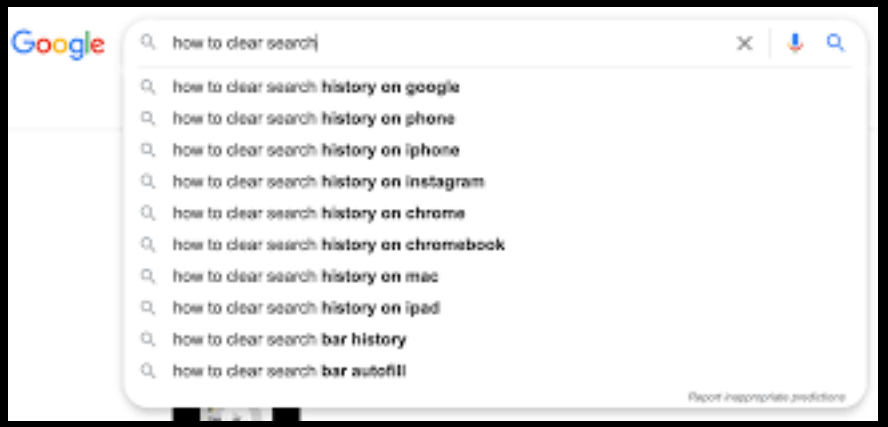
Our digital footprints

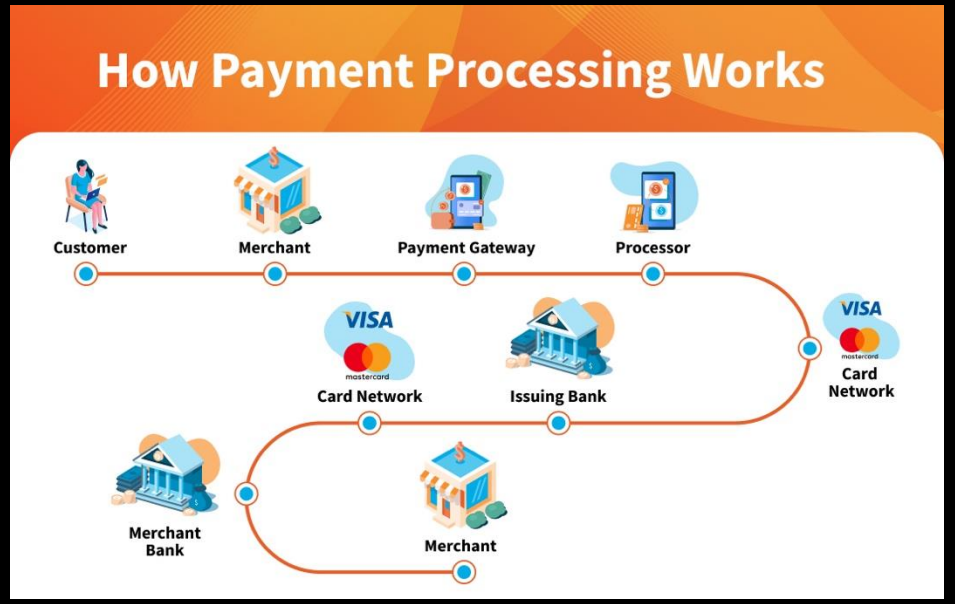
- The information and access we explicitly give
- IP Address
- Third-party cookies
- Browser fingerprinting
- Third-party scripts
- The “AI Blender”

Social Media Information

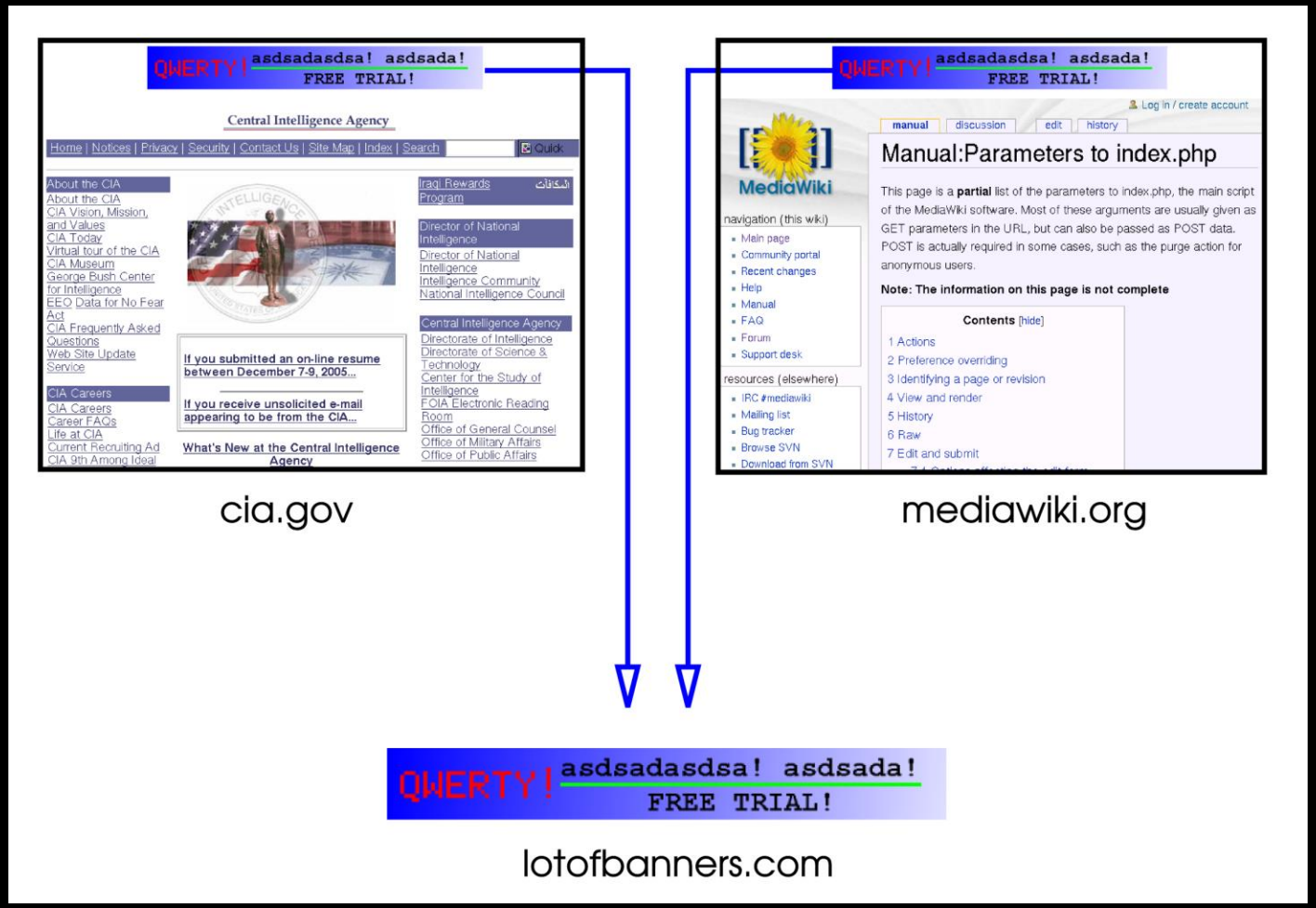
“Snitches”

All-new
Ring Battery Doorbell
See more with Head-to-Toe Video
ring


Google
how to clear search
how to clear search history on google
how to clear search history on phone
how to clear search history on iphone
how to clear search history on instagram
how to clear search history on chrome
how to clear search history on chromebook
how to clear search history on mac
how to clear search history on ipad
how to clear search bar history
how to clear search bar autofill
Report inappropriate predictions


How Payment Processing Works
Customer
Merchant
Payment Gateway
Processor
VISA
mastercard
Card Network
Issuing Bank
VISA
mastercard
Card Network
Merchant Bank
Merchant

Third-party cookies

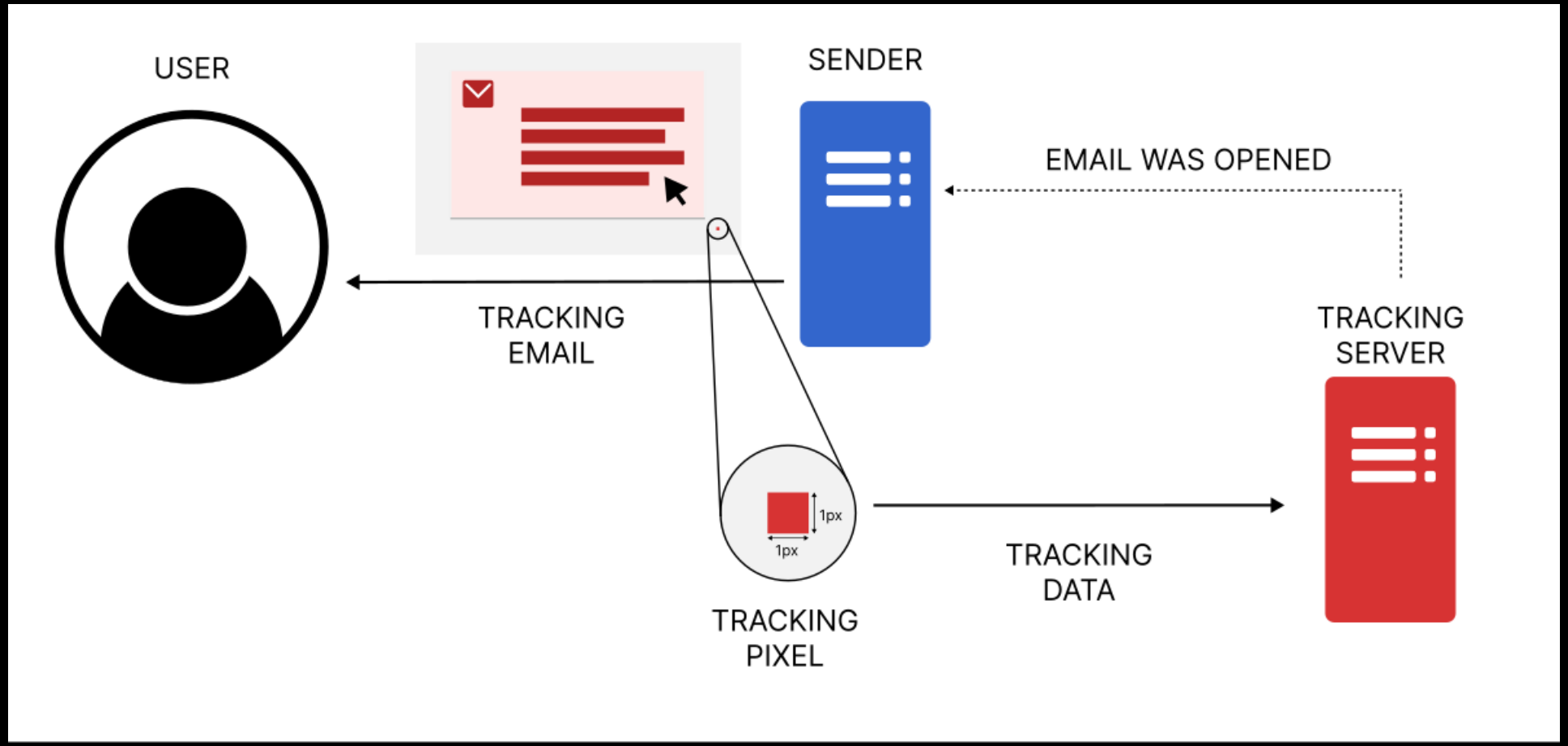


Browser Fingerprinting

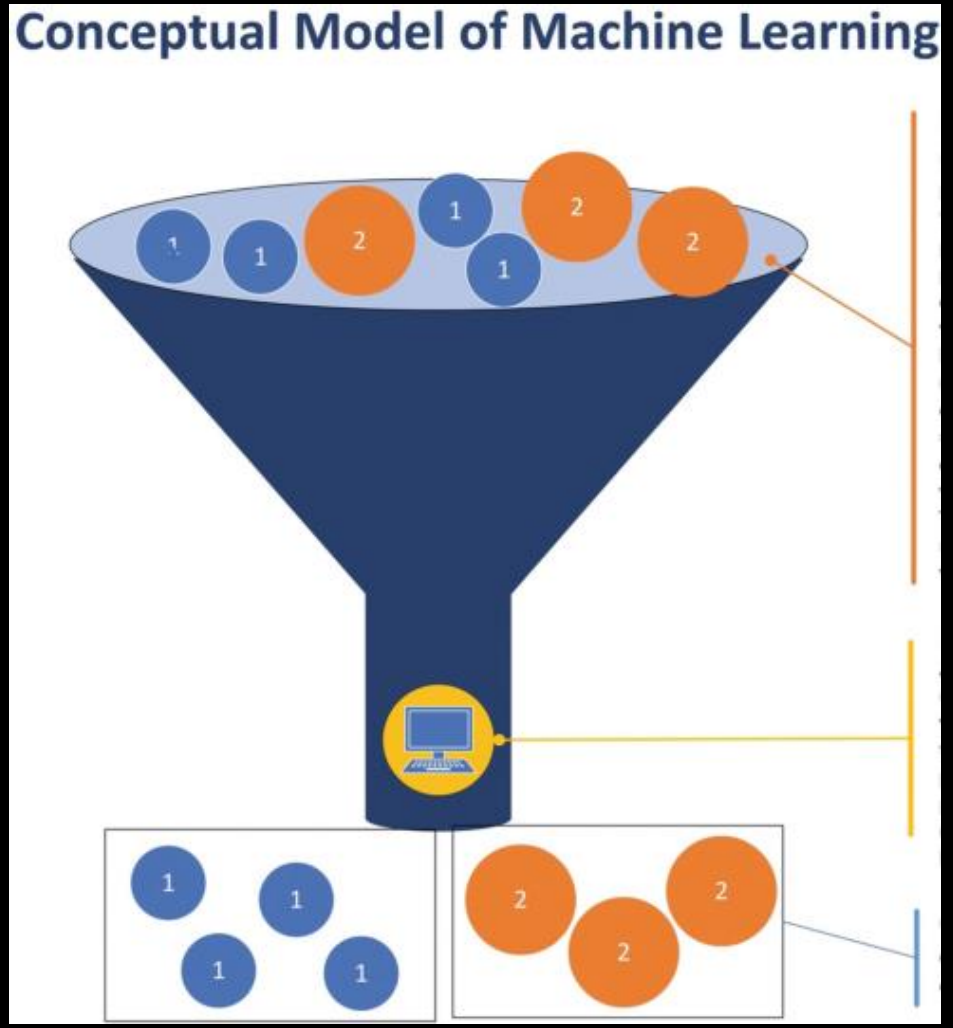
Environment

Variable	Value
PATH	/usr/local/bin:/usr/bin:/bin
CTK_ERROR_DOCUMENT	404.html
DOCUMENT_ROOT	/www
HTTP_ACCEPT	text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
HTTP_ACCEPT_CHARSET	ISO-8859-1,*,utf-8
HTTP_ACCEPT_ENCODING	gzip,deflate,bzip2
HTTP_ACCEPT_LANGUAGE	en-US,en
HTTP_REFERER	http://www.google.com/search?q=phpinfo+HTTP_USER_AGENT
HTTP_USER_AGENT	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/525.13 (KHTML, like Gecko) Chrome/0.2.149.27 Safari/525.13
REDIRECT_STATUS	200
REDIRECT_URL	/identifiant/info.php

Third-party scripts

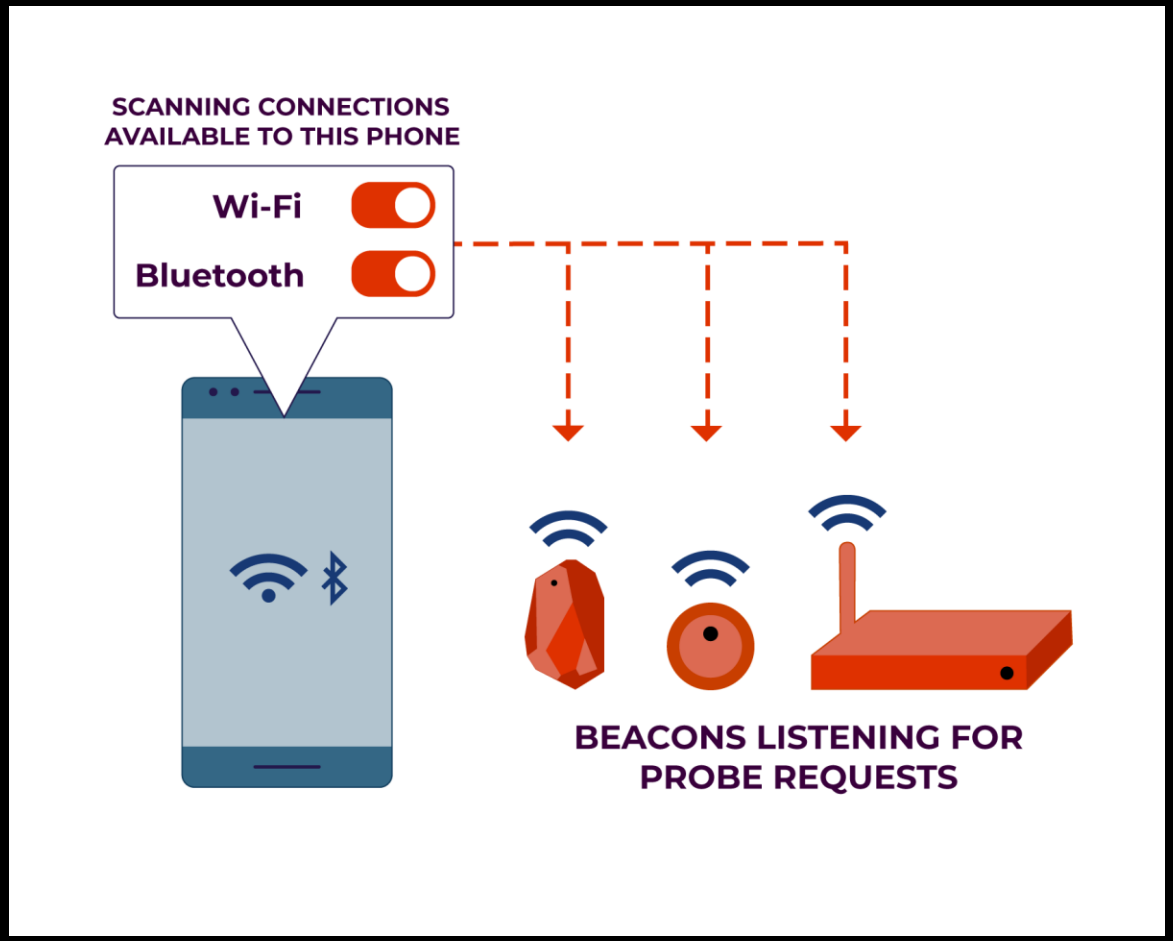


The “AI Blender”

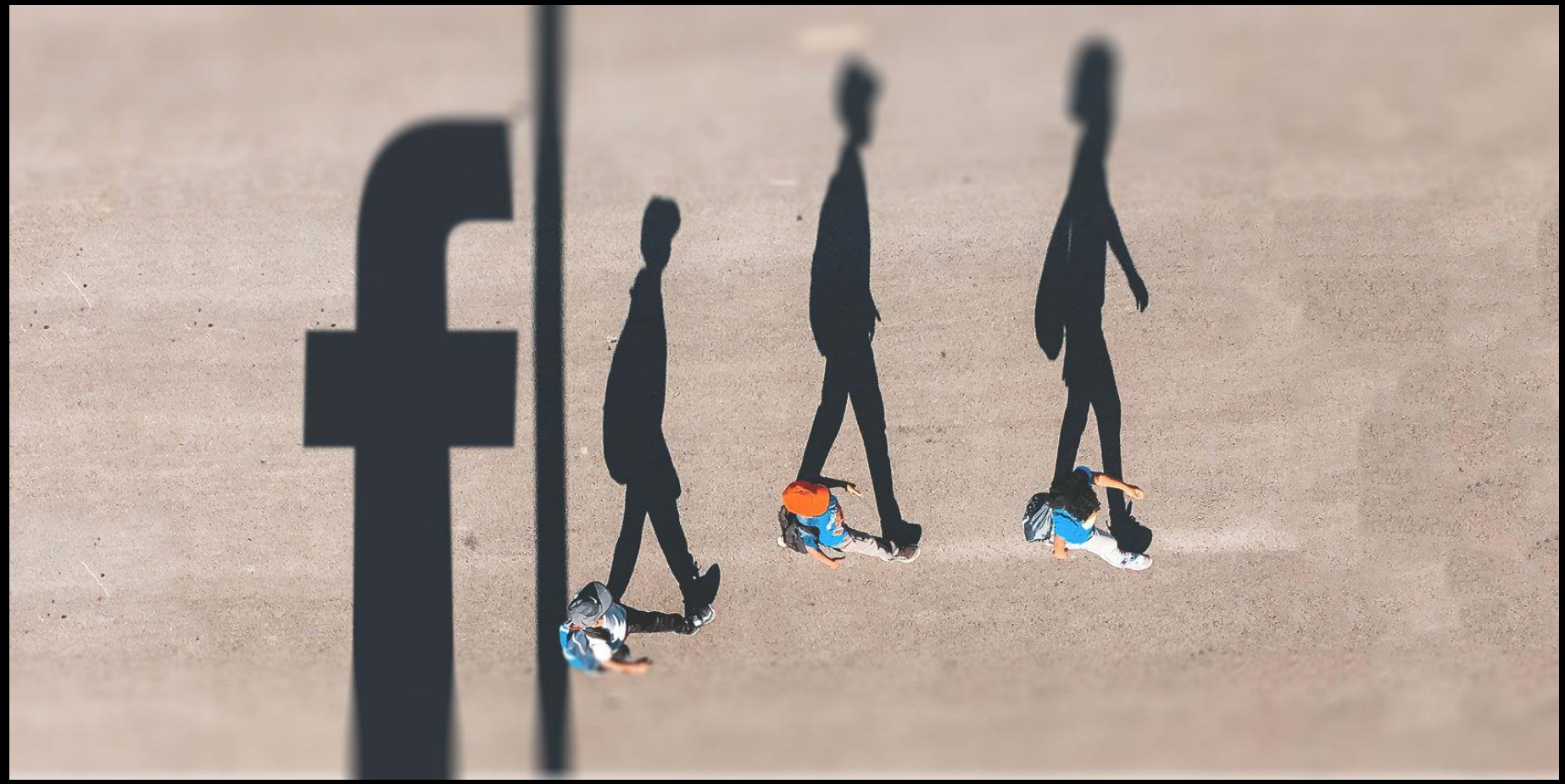


Vertical Integration

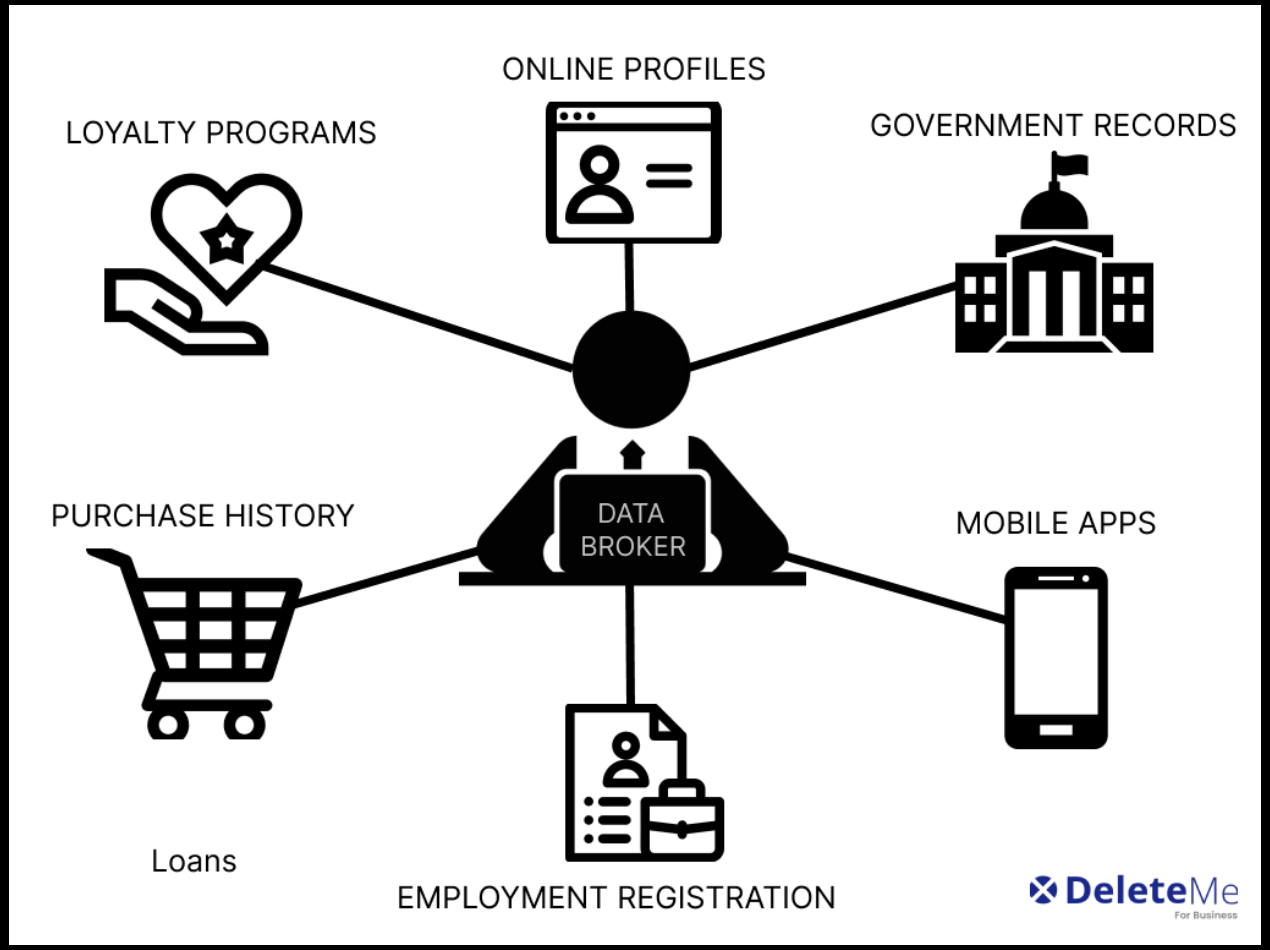
MAC Addresses



Shadow Profiles



Data Brokers

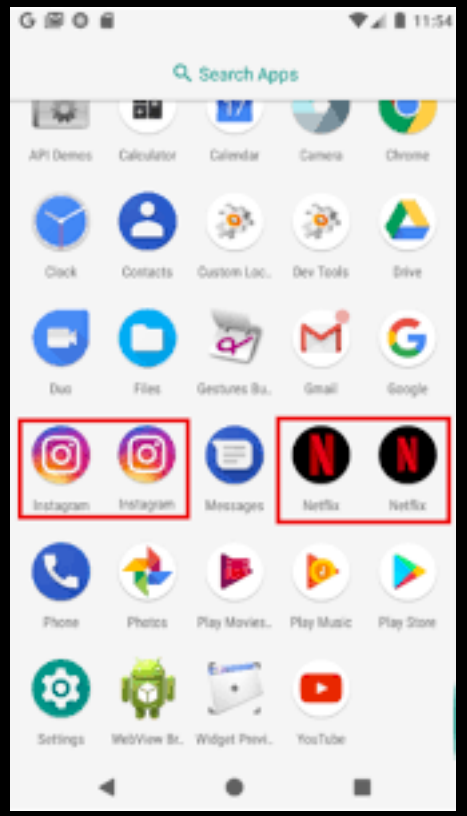


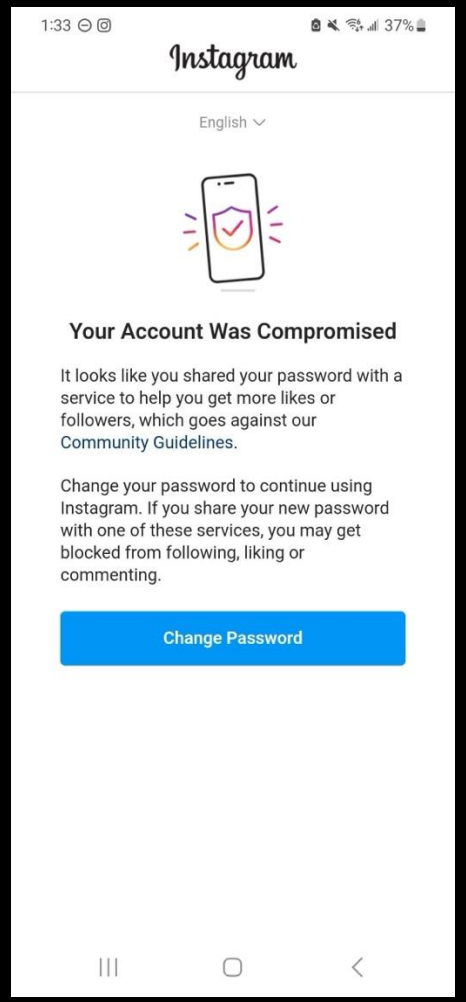
Why collect all of this

- $$$
  - Advertisers
  - Goverments/LE
  - Other brokers
  - Tech Companies
  - Insurance Providers
  - Political Campaigns

Are there other types of tracking to be aware of?

Intimate Partner Surveillance





Next Time

Privacy in Tension