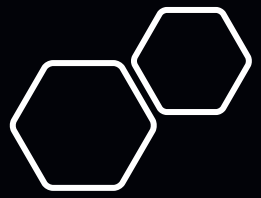


Privacy friendly search

Searching in encrypted databases

Polymorphic encryption

Privacy in databases

Privacy in machine learning

Privacy friendly revocation of credentials

Secure multiparty

Privacy friendly identity management

Revocable privacy

Obfuscation

Privacy in asynchronous messaging

Privacy friendly location based services

Anonymous cryptocurrency


Obfuscation

Agenda

- What is privacy and the problem?
- What is obfuscation?
- Going into depth
  - Network
  - First parties
  - Third parties
- Closing notes

What is privacy

- “***The right*** that someone has to keep their personal life or personal information ***secret*** or known only to a small group of people” – Cambridge dictionairy
- “the state of being alone and ***not watched*** or interrupted by other people” – Oxford dictionairy

https://dictionary.cambridge.org/dictionary/english/privacy
https://www.oxfordlearnersdictionaries.com/definition/english/privacy

The problem

- As a user of services you don’t want to be tracked and spied on
- Can you obfuscate your behaviour and identity to protect your privacy?
- Which methods and tools can be used to achieve this?

In one main question:

Can obfuscation and other methods of ‘resistance’ help to protect your privacy?

General Idea of obfuscation (Spartacus)

- Trying to find one individual person (the leader/Spartacus)
- Every soldier impersonates Spartacus
- Spartacus is thus "hidden" in the crowd

- -> The roman soldiers has to identify everyone as 'Spartacus', they cannot be sure who it actually is

Spartacus (Film), 1960 - directed by Stanley Kubrick

Obfuscation by animals

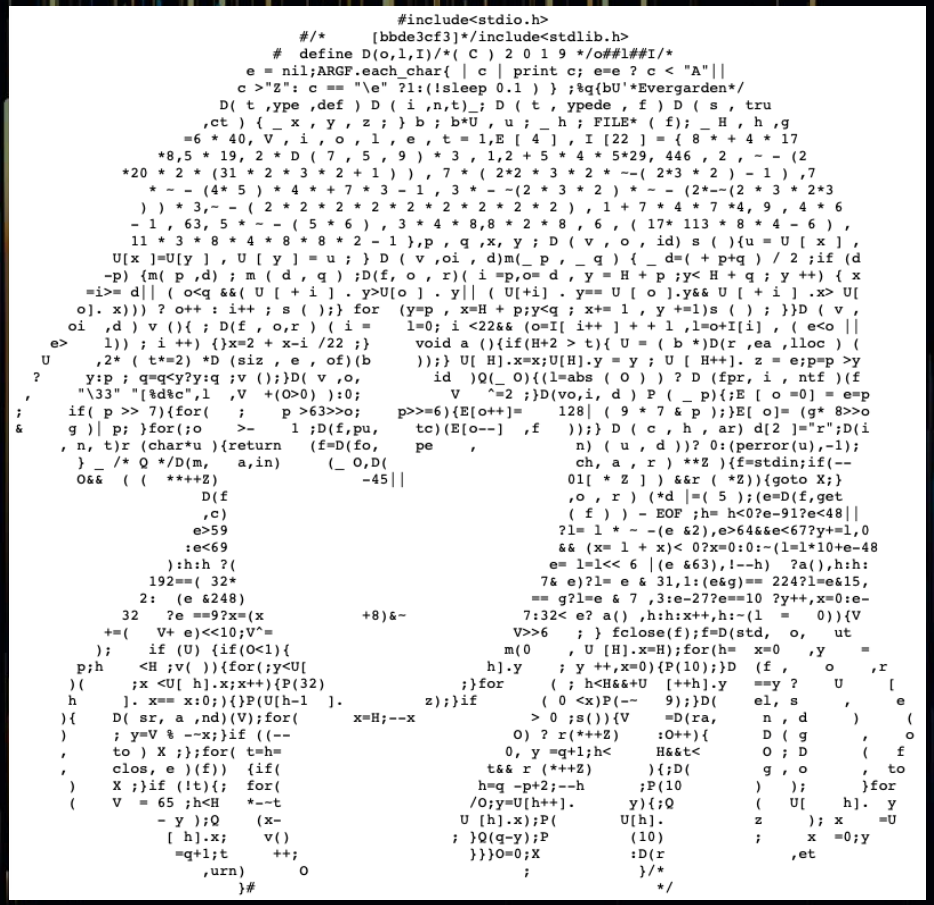
- Animals also use different forms of obfuscation
- "Passive" and "Active" obfuscation methods
- "Passive" obfuscation like the species Phasmida (Walking sticks)
- "Active" obfuscation like the Cyclosa (trashline orbweavers)

Obfuscation to attack rival businesses

- Obfuscation might also be used maliciously
- Uber vs. Gett case in New York
- Uber would create many false orders to obfuscate real orders, cancelling them again before arrival
  - Gett cannot distinguish anymore between real and fake orders
- Uber even sent job offers to the drivers
- -> Value of jobs at Gett are reduced by obfuscating real requests

Obfuscation in Programming

- International obfuscated C-code contest (ioccc.org)
- Reverse engineering gets harder
- Impossible to read at first glance
- Does not secure privacy



https://www.ioccc.org/2019/yang/violet.c

What is obfuscation

- Obfuscation can usefully be compared to camouflage
- Privacy based obfuscation
  - Using obfuscation methods and techniques to protect your privacy
- Anonymity based obfuscation
  - Using obfuscation methods and techiques to protect your identity/stay anonymous
- There is an overlapping area

What is obfuscation

Overlapping area

- While using obfuscation techniques to protect your privacy, you use networks and tools that hide your identity
- For example: hiding yourself in a group so you can not be tracked, you can use Tor
- But how you use the techniques, networks and tools define if you are protecting your privacy or identity

What is obfuscation

Some base techniques

- Encryption
- Anonymous communication networks
- Virtual private networks
- Steganography
- Pseudonymization

What is obfuscation

Limitations of the techniques

- **Encryption** – vulnerable to attacks
- **Anonymous communication networks** – can be slow, may not provide complete anonymity
- **Virtual private networks** – vulnerable to attacks, restricted in some countries, security depends on provider and implementation
- **Steganography** – vulnerable to detection, quality may be affected
- **Pseudonymization** – can be linked back to the original identity

What is obfuscation

Some basic use cases

- Online communication
- Data storage
- Online transactions
- Internet browsing
- Location privacy
- Personal information protection

What is obfuscation

Some examples of obfuscation

- Filling a channel with noise
- Location services without location tracking
- Blending genuine and artificial search queries
- Making patterns to trick a trained observer
- Many people under one name or in one outfit
- Changing "identities" periodically

Obfuscation

First party

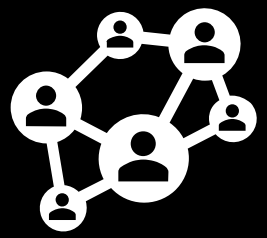
Social media

Network

Tor network

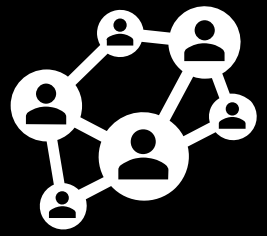
Third party

- Tracking by 3rd parties by e.g. cookies or the "Facebook-Pixel"
  - Cookies, which are present on multiple websites and thus can track a single users browsing history
  - Tracking may also be done with a .png imagine and the corresponding GET-request
- A user may block 3rd-party-cookies by the browser, preventing this kind of tracking
- Browser fingerprinting might be used instead of cross-site-cookies
  - The user does not need to give conscent to that
  - -> More convenient for tracking services

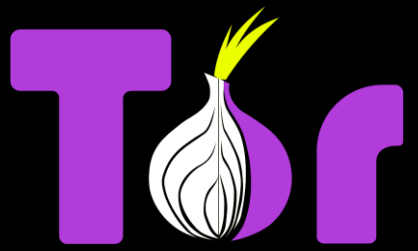


Network

Tor network



Tor network

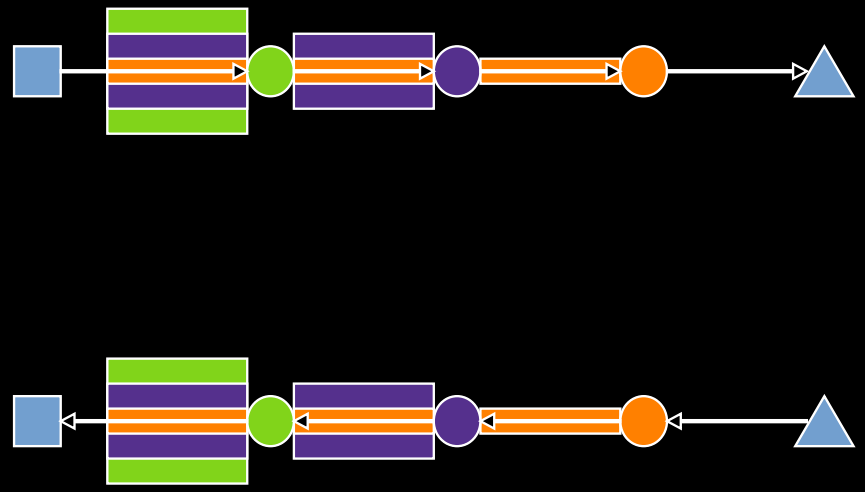


- Open-source privacy network that enables anonymous web browsing (Originally developed by the U.S. government)
- Who uses it?
  - **Government agencies**
  - **For-profit enterprises**
  - **Illicit organizations**
  - **Private individuals**

Tor network

How it works

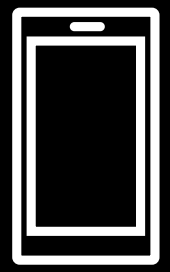
- The more people use it, the better
- Tor network does not directly connect your computer to the website
- Highly tangled network that frequently changes
- It uses layered encryption



Network

What does Tor have to do with obfuscation?

- *Can ensure privacy for data and communication on the web*
- *Helps with hiding yourself*
- *Being used by other tools*
- *Methods being used*
  - *Encryption*
  - *Data minimization*

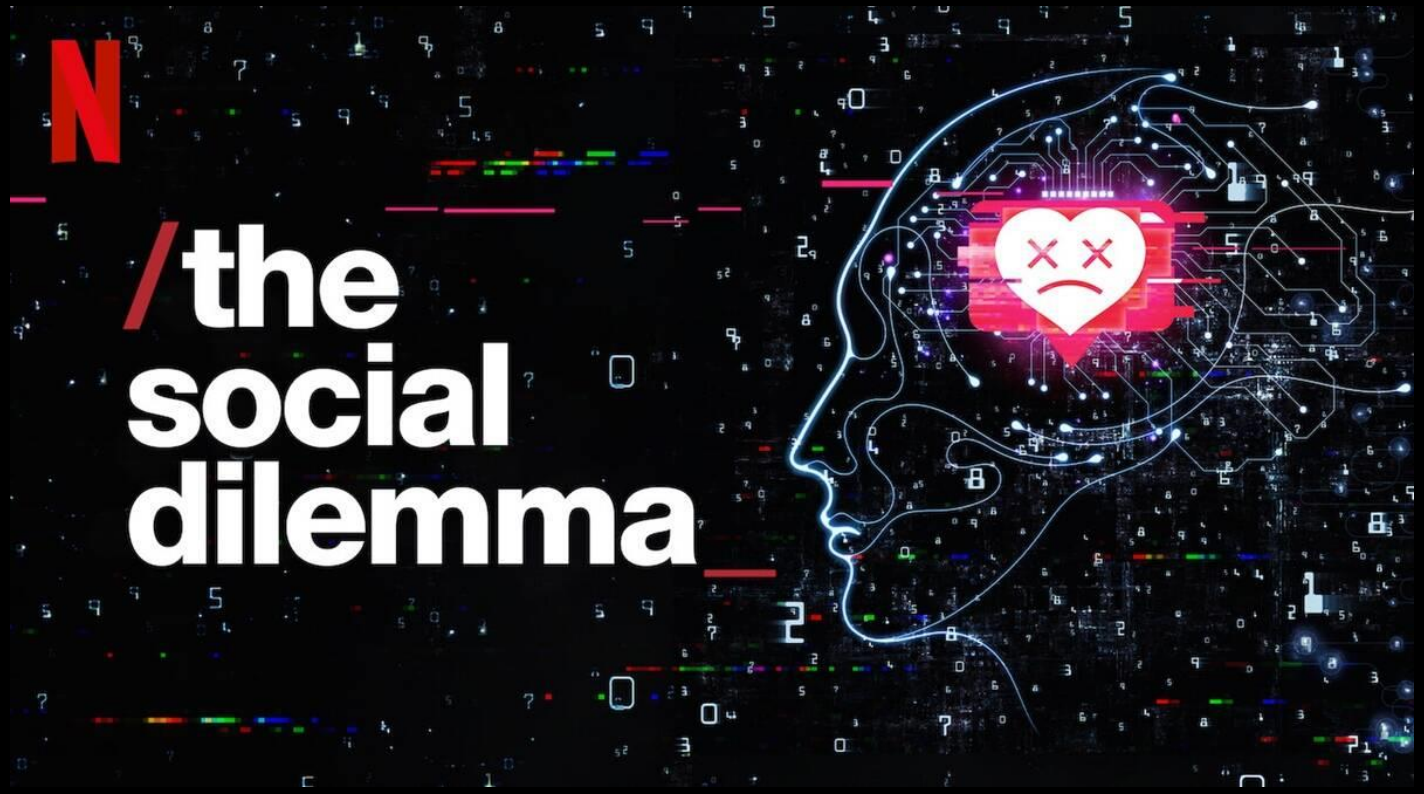


First party

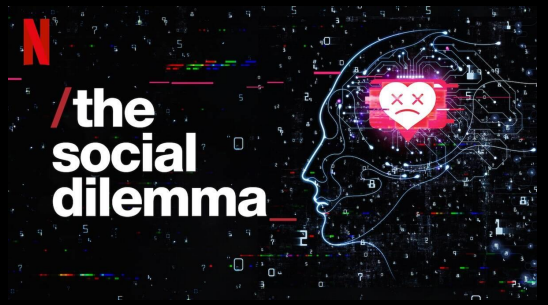
Social media

Social media

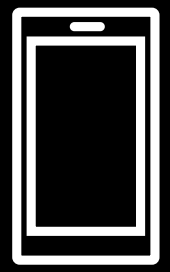
Social dilemma on Netflix
Did you see it?



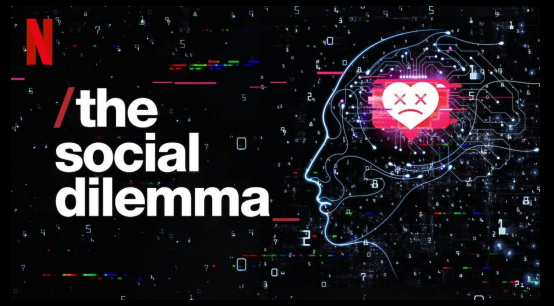
Social media



- “*Nothing vast enters the life of mortals without a curse*” - Sophocles
- “*We were naive about the flip side of that coin*” – Former president Pinterest
- “*If you are not paying for the product, then you are the product*”



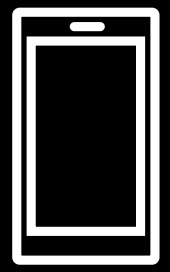
Social media



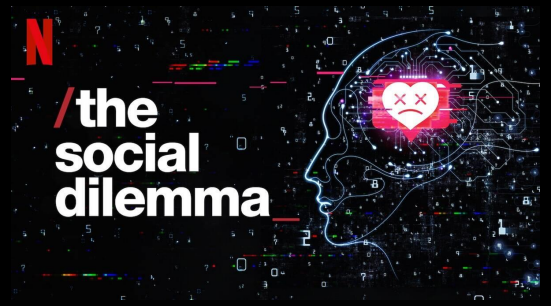
What is their goal?

- Engagement goal: drive up your usage, to keep you scrolling
- Growth goal: keep you coming back and invite as many friends
- Advertising goal: make as much money as possible from advertising

Do you recognize this pattern in your daily life?



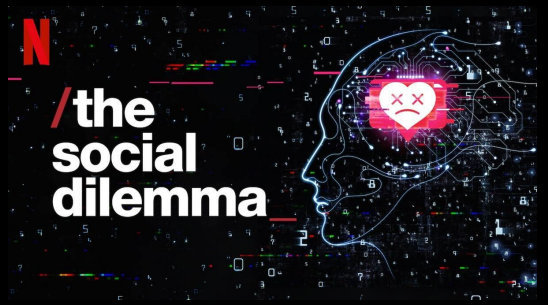
Social media



What do they use to track you?

- Cookies & fingerprinting
- Your location
- Your activities on the platform
  - What you watch and for how long
  - What you like
  - Which hashtags you use
  - Who you interact with

Social media



Do they know EVERYTHING about you?

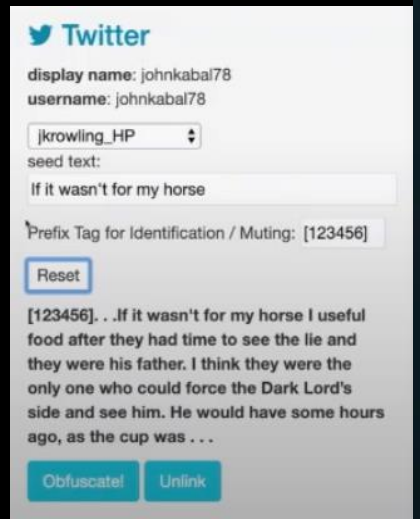
- Depressed?
- Lonely?
- Your ex?
- Stalking your ex?
- Thinking about your ex?
- What you do late at night?
- Introvert or extrovert?
- What kind of neuroses you have?
- Your personality?

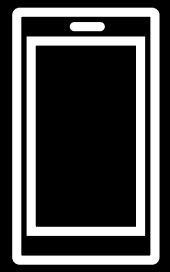
Invasion on your privacy?

Social media

Spartacus-as-a-service

- Obfuscation tool for 25 different social media platforms
- Floods account with random posts/events (mariages, job change etc.)
- Will change the "known behavior" of the obfuscated user drastically

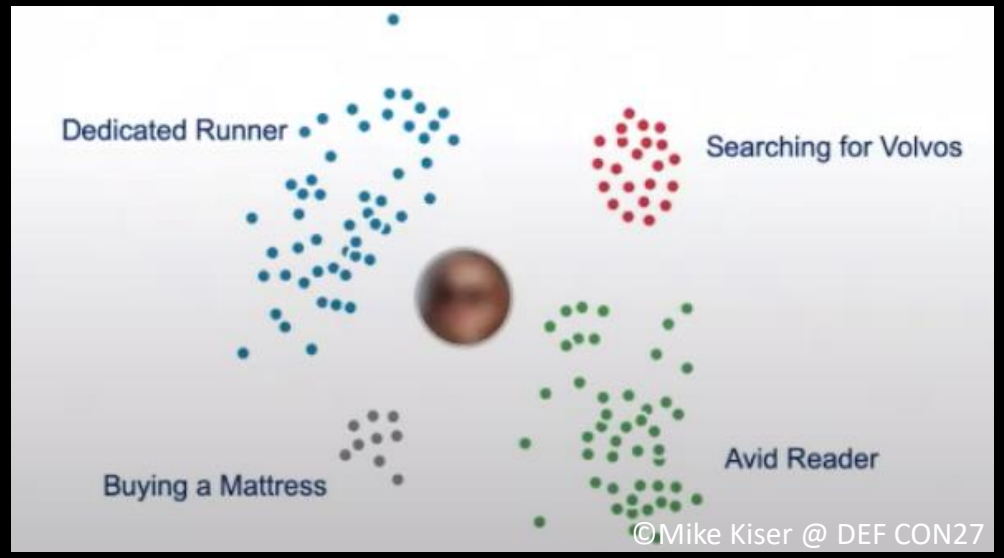


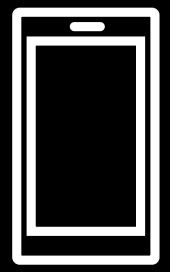


Spartacus-as-a-service

Does it help?

- Using an obfuscated twitter profile to share information to an invited group, by muting the fake posts
- The user will have an obfuscated advertisement profile

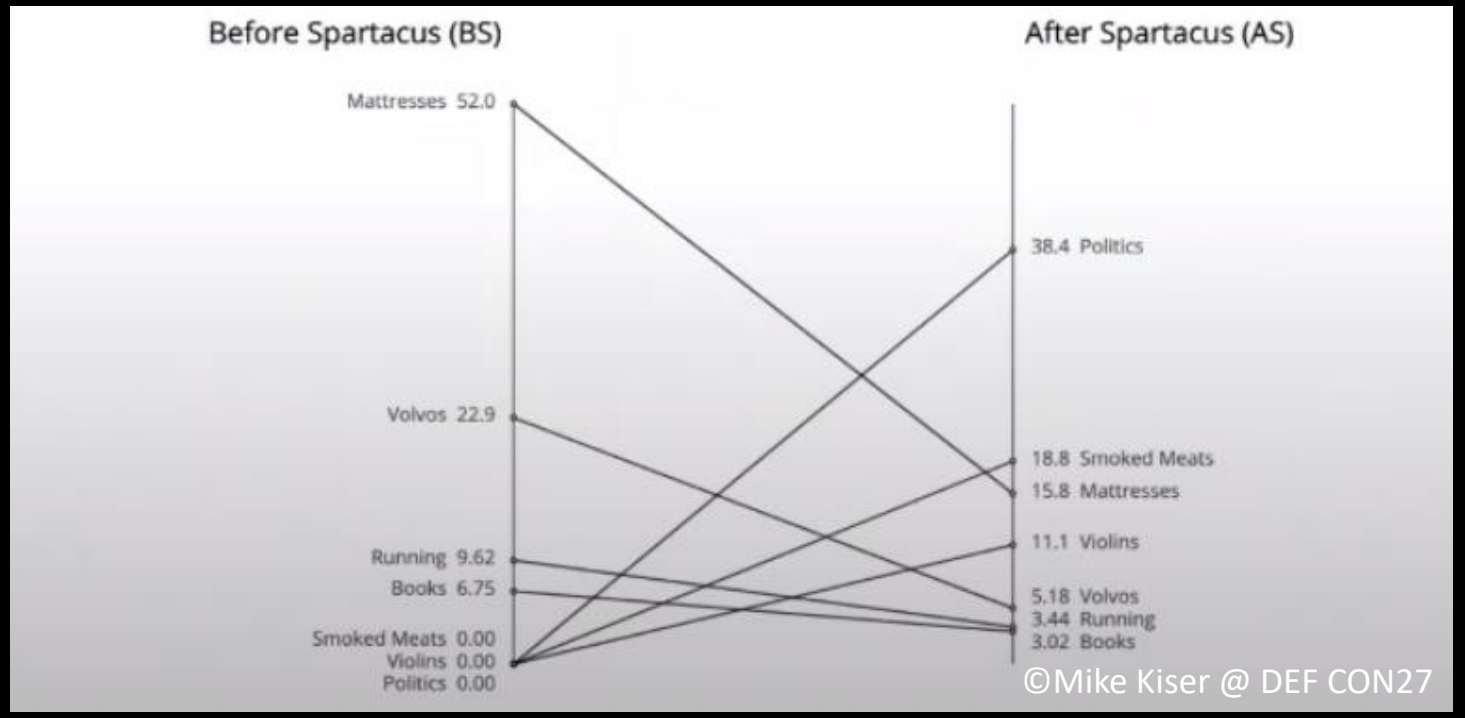




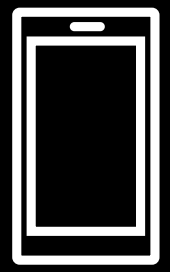
Spartacus-as-a-service

Does it help?

- Did change the ads served drastically over 4 weeks



- But do we really want this?

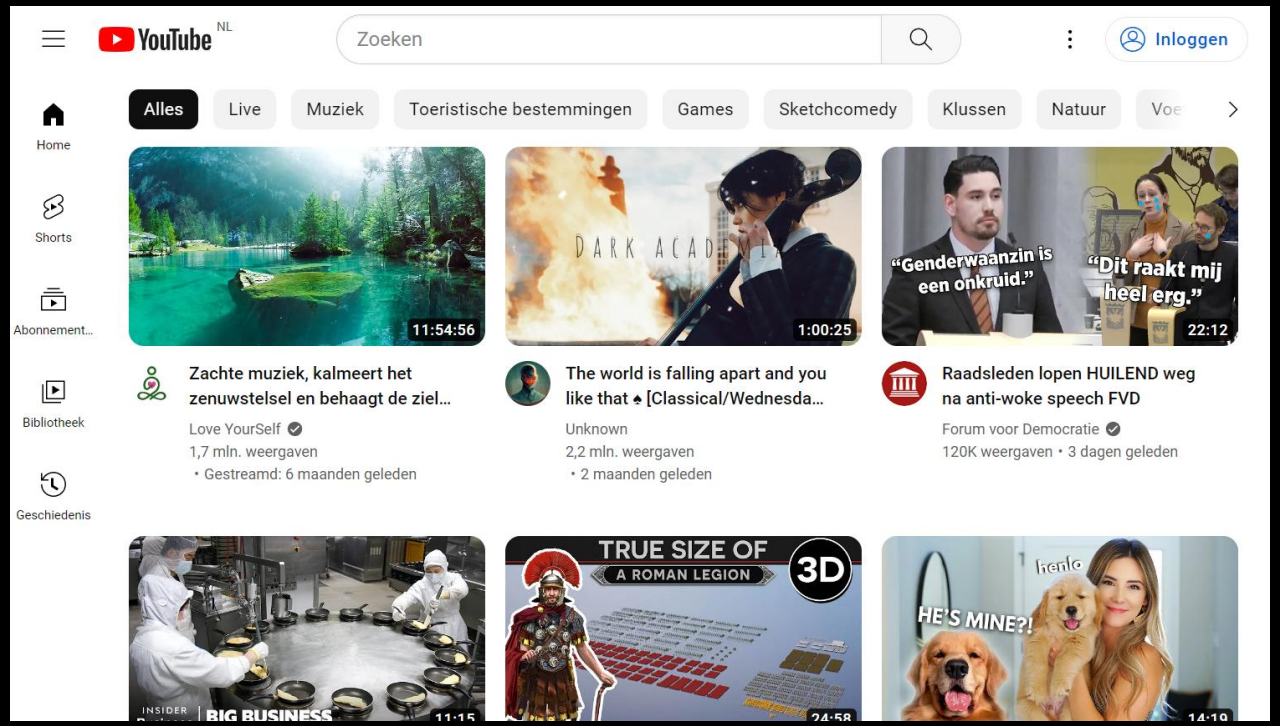


Social media

- Would this be useful?
- Would you use it?

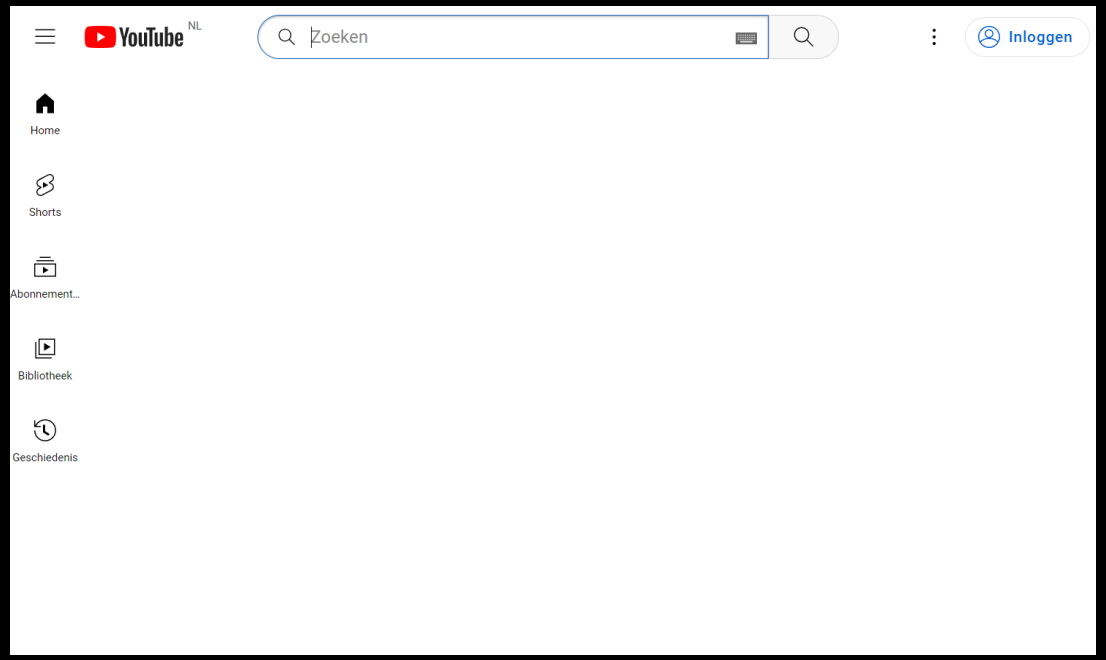
Social media

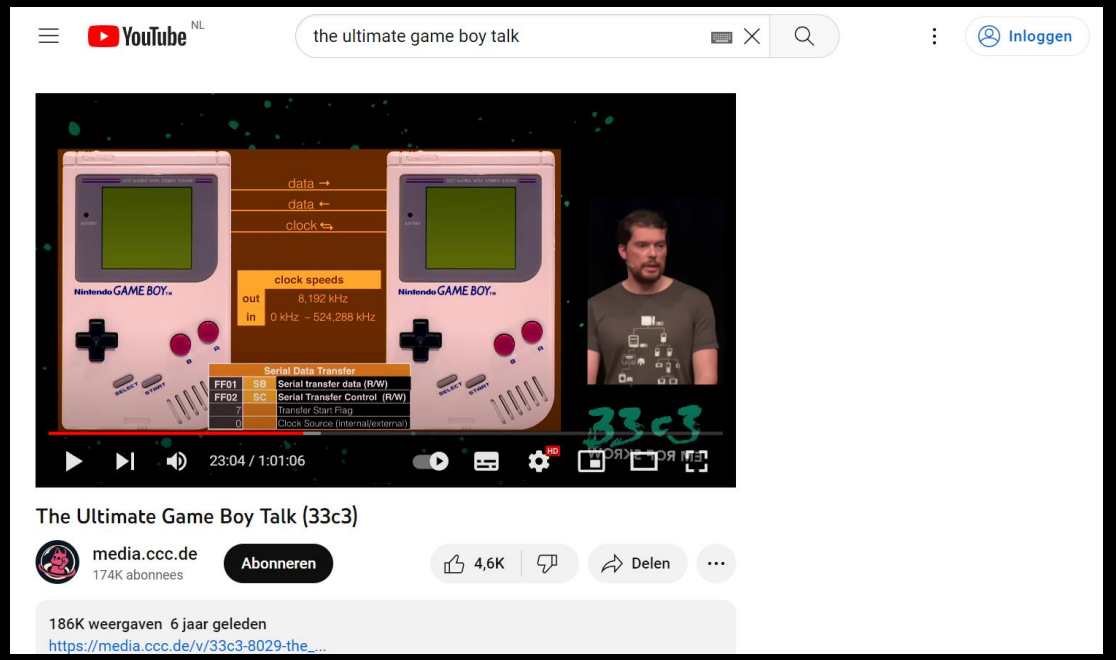
- Fighting the symptoms! with YouTube as case study



Social media

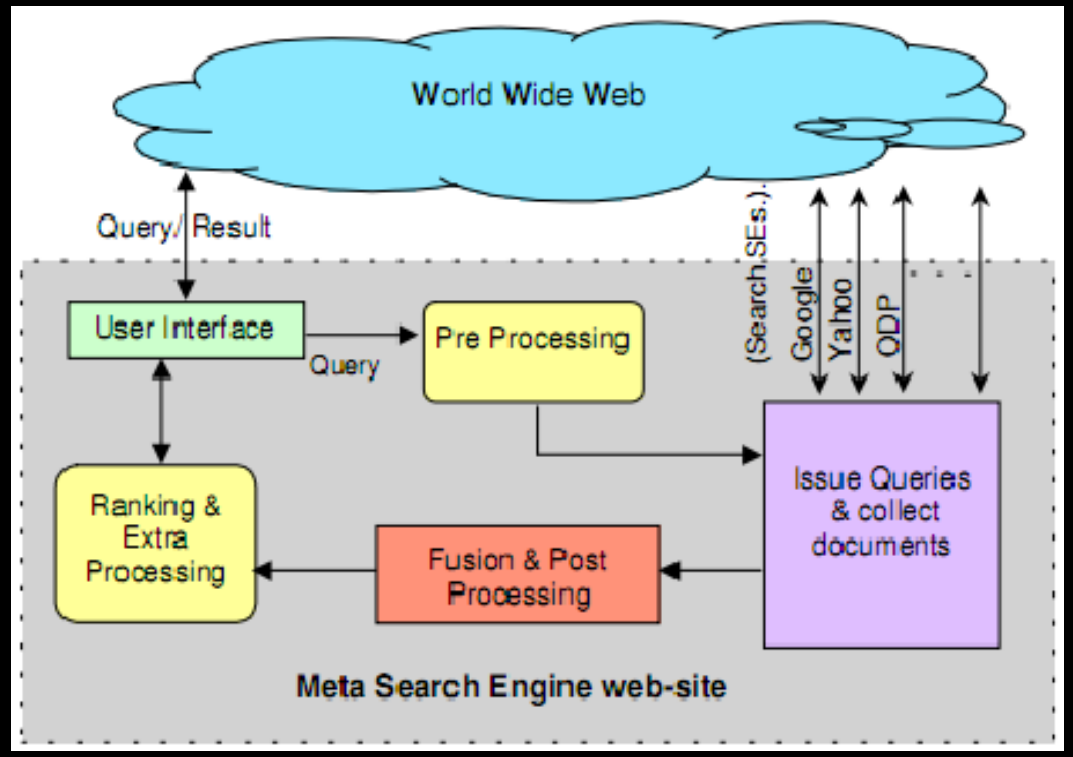
- Fighting the symptoms! with YouTube as case study



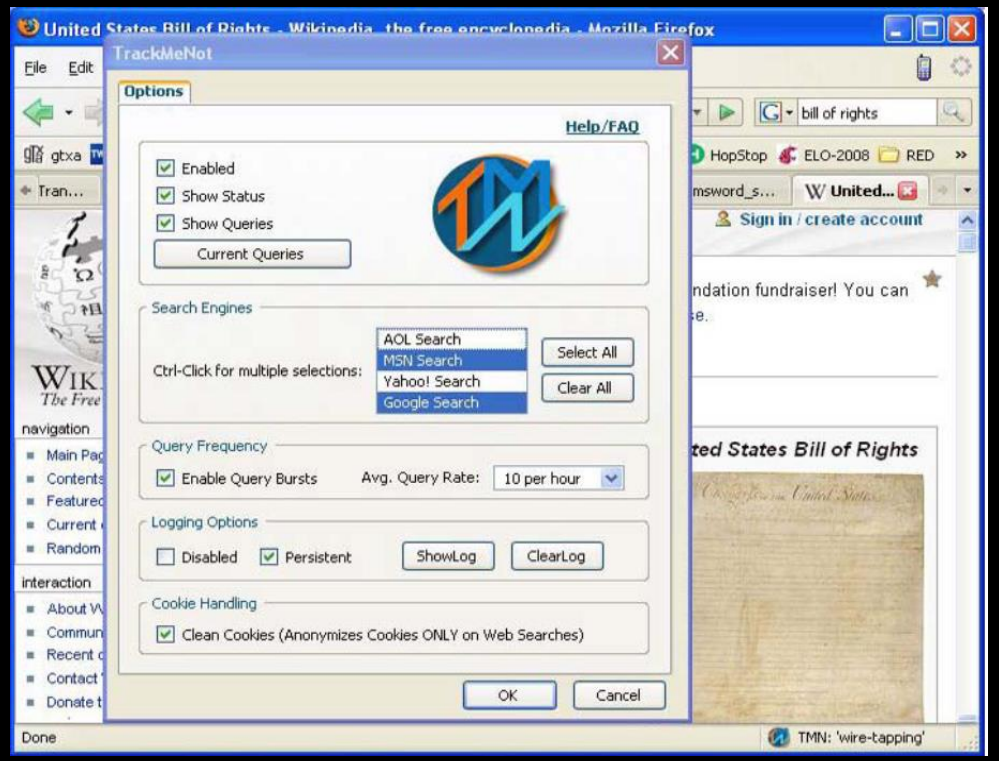


Search engines

- *Hiding Together*

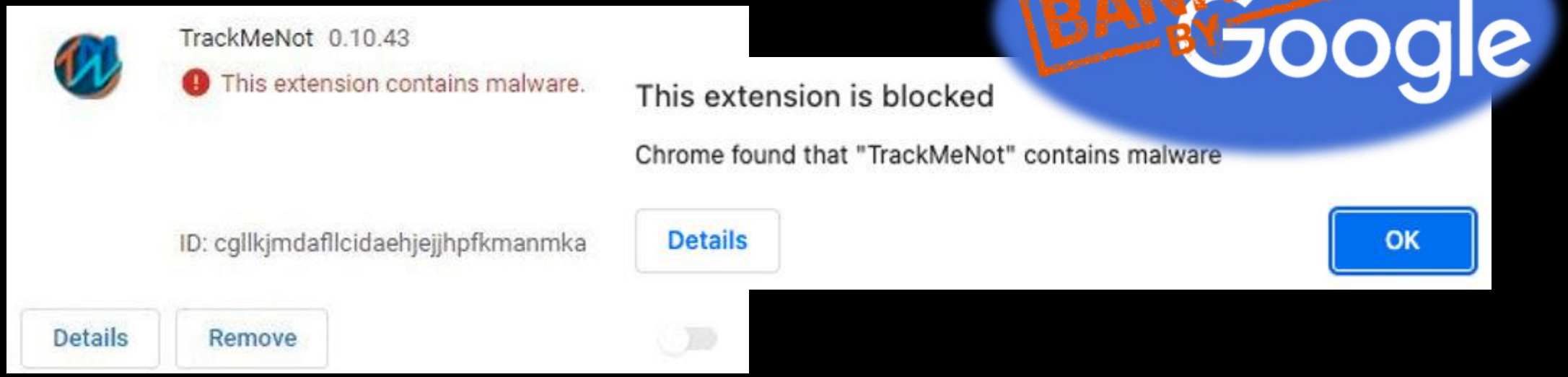


- *Generating Noice*



Search engines

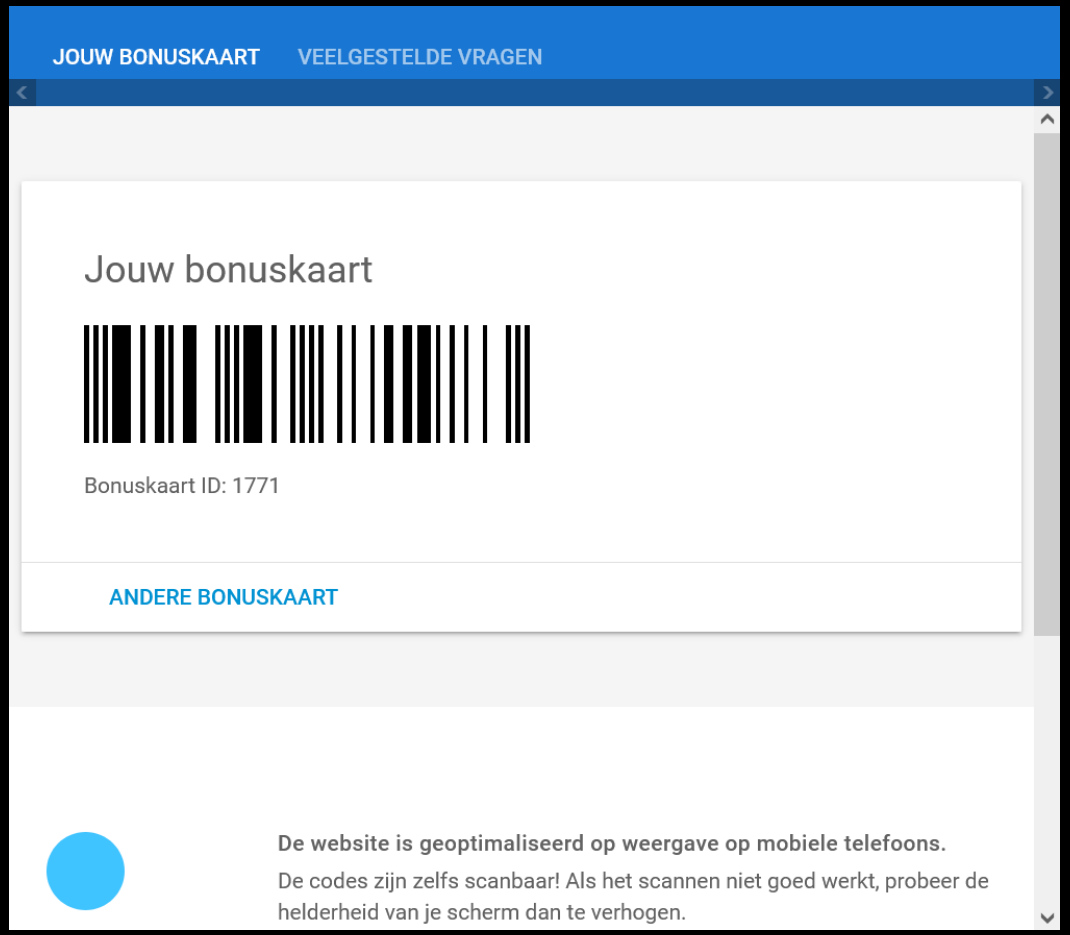
- *What Happened?*



"After further review of your item, we have confirmed that your item did not comply with our Program Policies and will not be allowed back in the store. However, your developer account will be reinstated."

Retail

- Albert Hein bonuskaart



(Online) retail

- Amazon, Bol, Coolblue, ect.

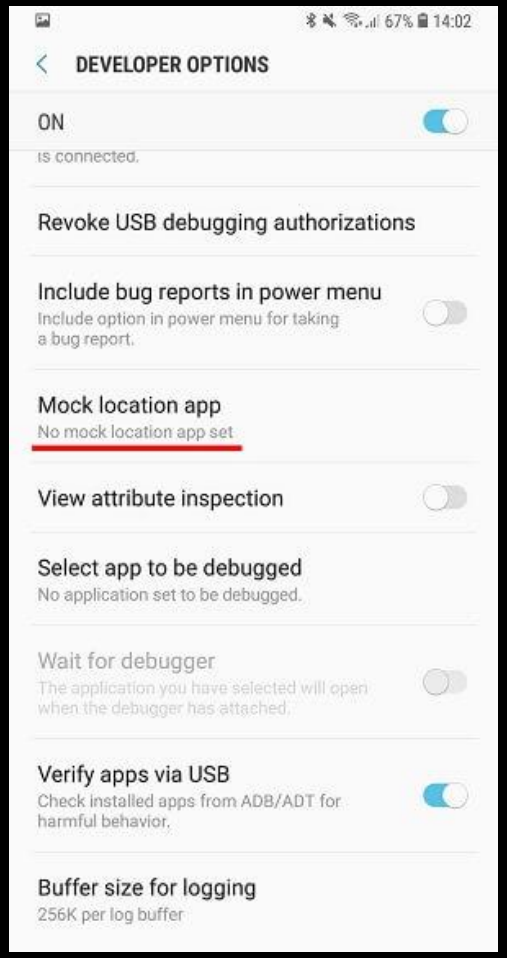
WEB / REPORT

Chaos theory: what happens when Amazon buys you random stuff? / 'Random Shopper' tries to outrun the recommendation engines

By RUSSELL BRANDOM
Source RANDOM SHOPPER
Dec 4, 2012, 10:47 PM GMT+1 | 0 Comments

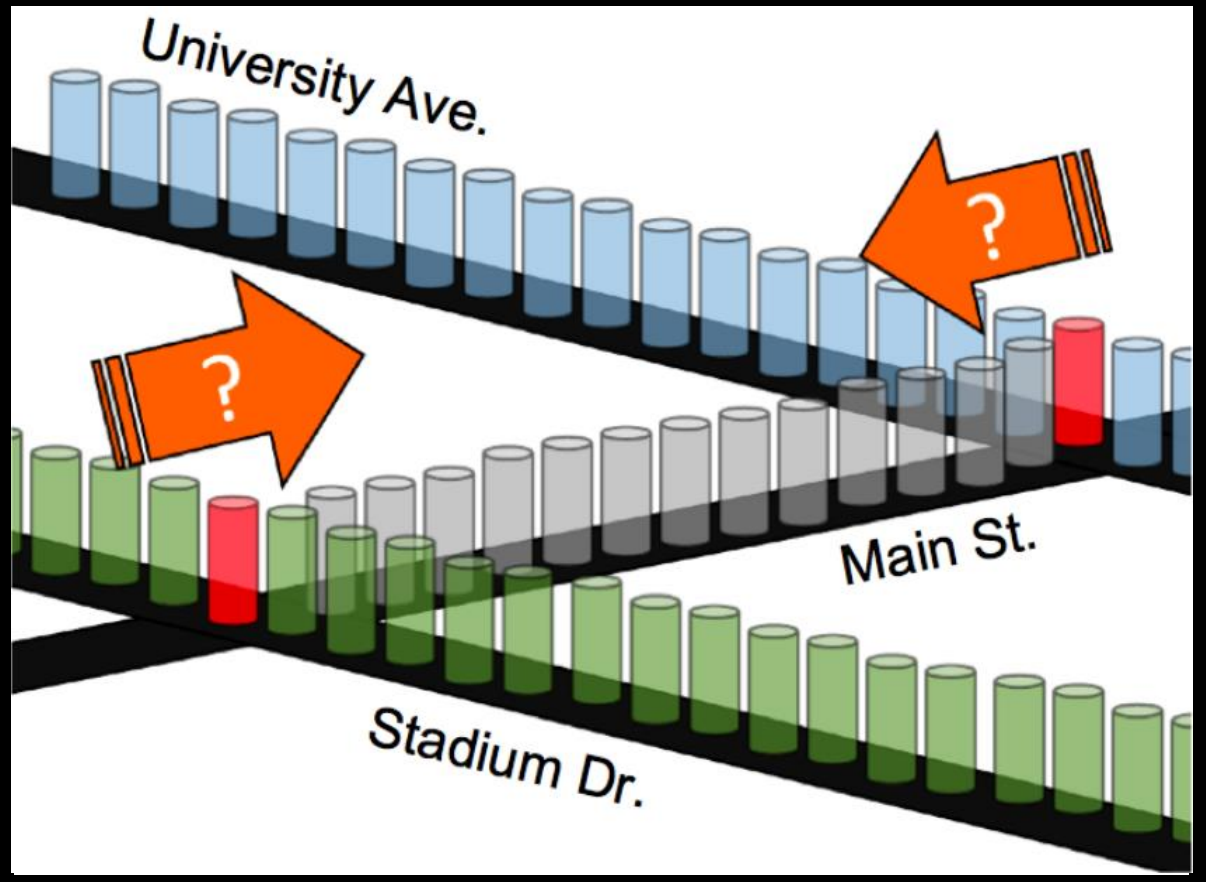
Location based tracking

- Location services
- *Spoofing*

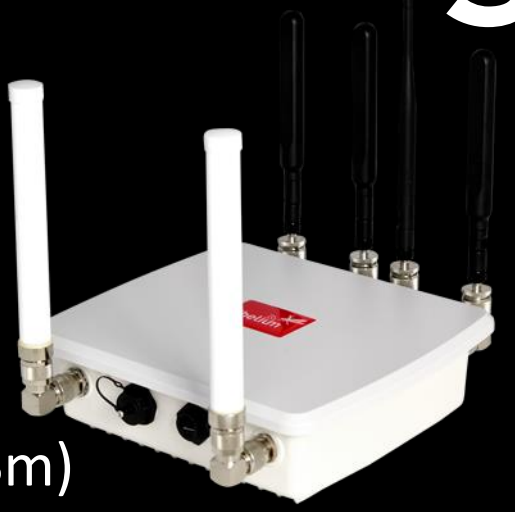


Location based tracking

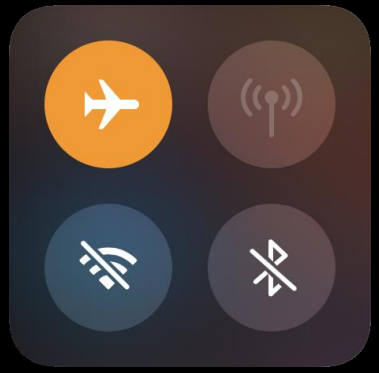
- CacheCloak

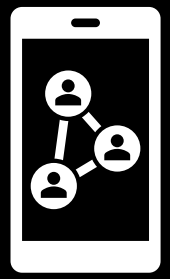


Location based tracking



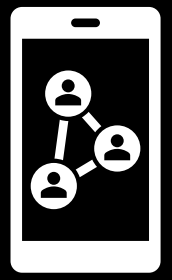
- **Unique ID** – Auto-generated numeric identifier.
- **Timestamp** – Time/date of the measurement.
- **MAC** – Source MAC address of the station
- **RSSI** – signal strength of the device from the scanner (measured in dBm)
- **Vendor** – Device vendor of the detected device (i.e. Apple, Samsung, etc.)
- **AP** – the SSID or network to which the device is associated





Third party

- Tracking by 3rd parties by e.g. cookies or the "Facebook-Pixel"
  - Cookies, which are present on multiple websites and thus can track a single users browsing history
  - Tracking may also be done with a .png imagine and the corresponding GET-request
- A user may block 3rd-party-cookies by the browser, preventing this kind of tracking
- Browser fingerprinting might be used instead of cross-site-cookies
  - The user does not need to give conscent to that
  - -> More convenient for tracking services



Third party

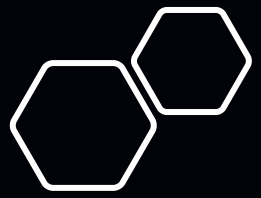
How to obfuscate against them

- Disable all cookies, however no impact on browser fingerprinting

- So many identifying factors often lead to a perfect match for a single user
- Possible to obfuscate the user agent, browser version etc.
  - However, this often detected by modern tracking tools and thus not very effective

Contrasting techniques

- Data minimisation:
  - Delete all social media
  - Not using app versions of services
  - Privacy settings in app
  - Using an addblocker
- Data Obfuscation
  - Spartacus-as-a-service
  - CacheCloak
  - GPS-spoofing
  - TrackMeNot
  - Adnauseum



Is Obfuscation by the user okay?

- The user is "lying", but only to avoid being exploited
- Waste of resources (bandwidth, computing power, electricity)
- "Griefing" non-obfuscated users
  - You might effect other users
- Against most Terms of Service
  - Google deleted/banned most obfuscation tools from the chrome app store =)

Problem solved?

Can obfuscation and other methods of 'resistance' help to protect your privacy?

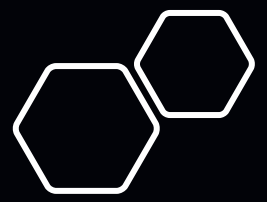
Yes it can but:

It depends!

You have to implement the right techniques

You might need to implement multiple techniques

It might buy you time, it might be circumvented easily



Thank you