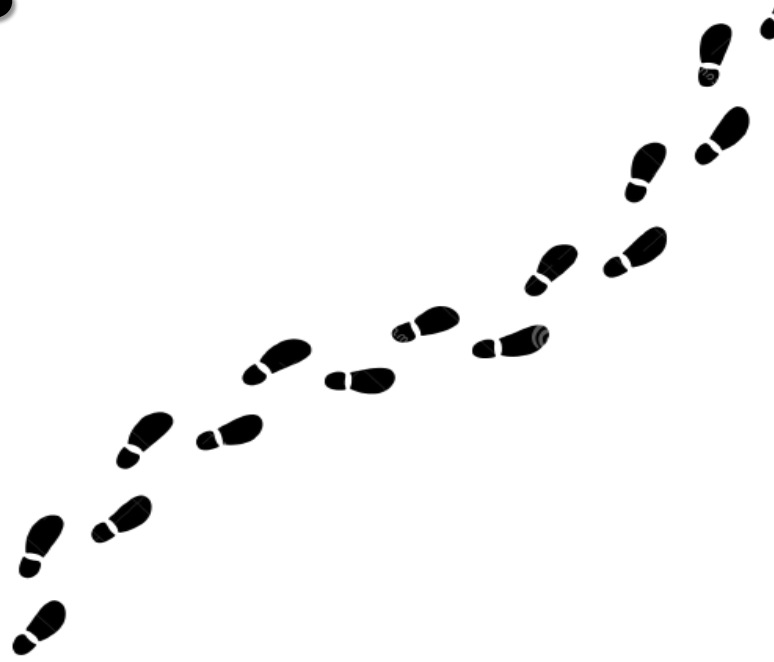
Tracking

Dr. Balázs Pejó

www.crysys.hu



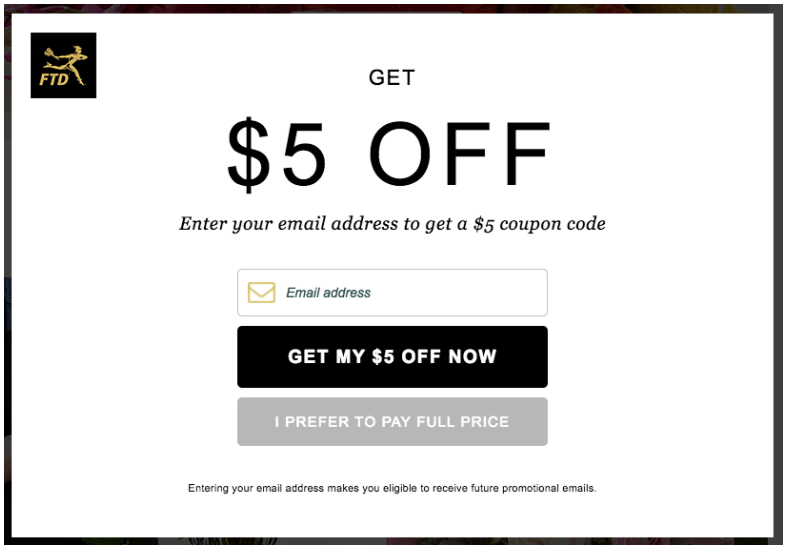
Agenda

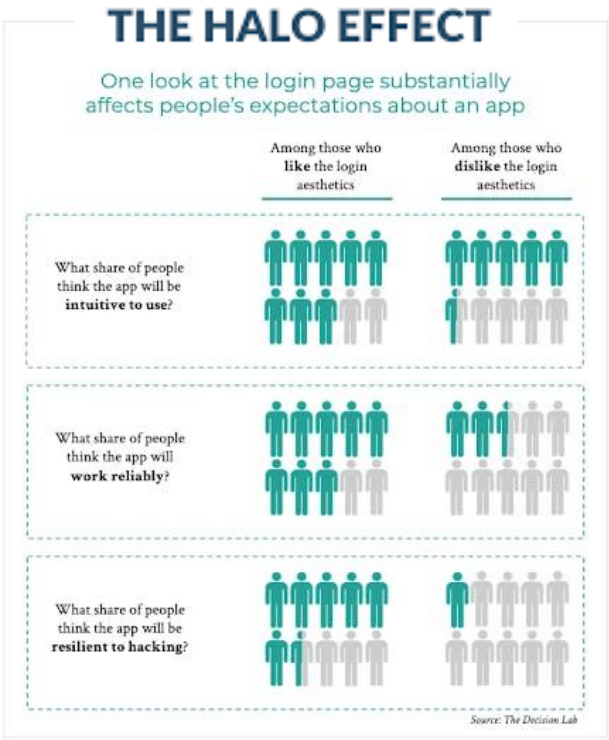
- Dark Patterns
- Tracking
- GDPR
- Deidentification
- Machine Learning
- Anonymization
- Cryptography

- Profiling
  - Manipulation
- Online Data
  - Data Brokers
- Tracking
  - Storage based
  - Cache based
  - Fingerprinting
  - Defense

Recap

- Dark Patterns nudge customers towards behaving in the company's desired way.
- Most of them are corresponding to well-known Cognitive Biases.





Profiling

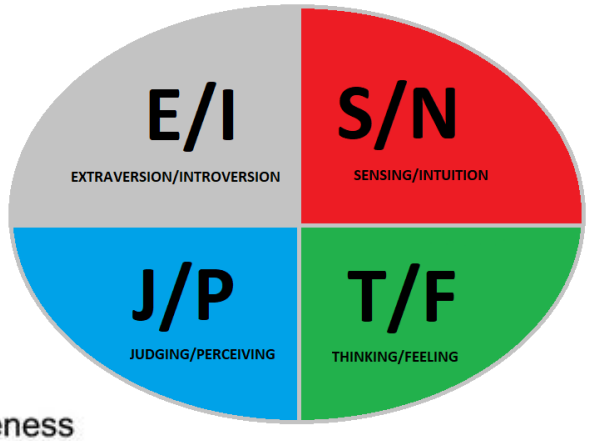
Individual Differences

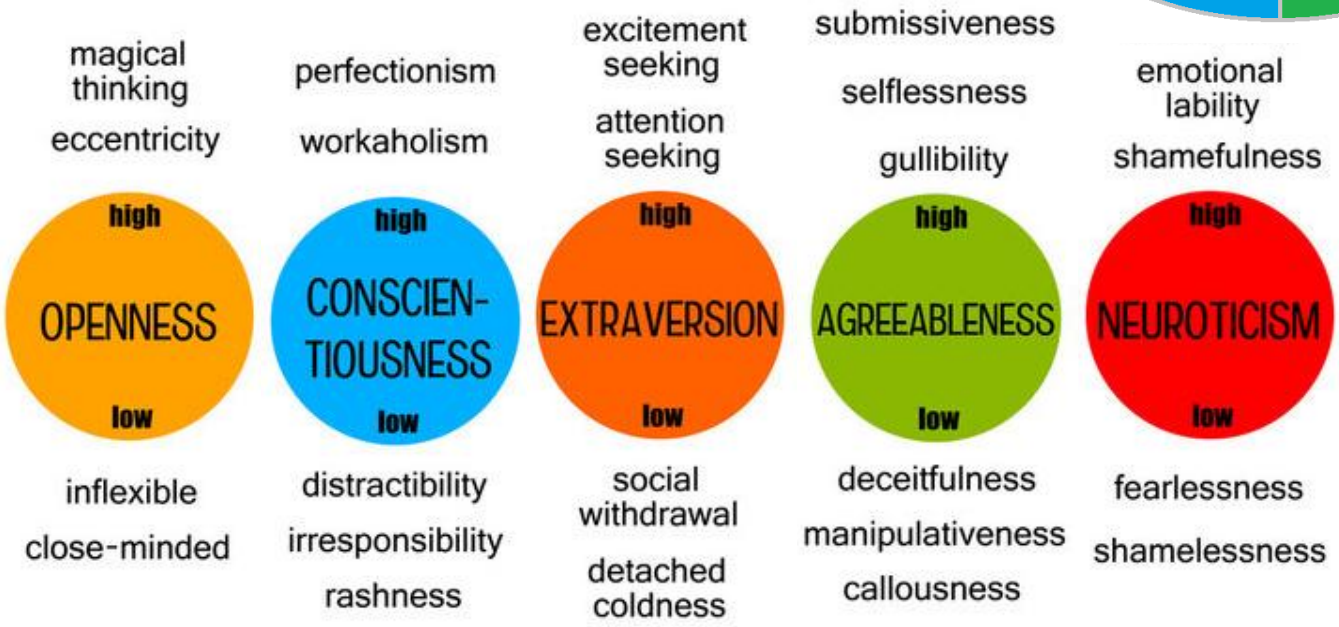
- People are different, with different level of susceptibility of different kind of Cognitive Biases.
- The effect of manipulations such as Dark Patterns could be increased with personalization.

Psychometric Profiling

- The Big 5 (OCEAN)
  - **Openness**: Outgoing vs. Solitary
  - **Conscientiousness**: Organized vs. Careless
  - **Extraversion**: Curious vs. Cautious
  - **Agreeableness**: Compassionate vs. Critical
  - **Neuroticism**: Nervous vs. Confident

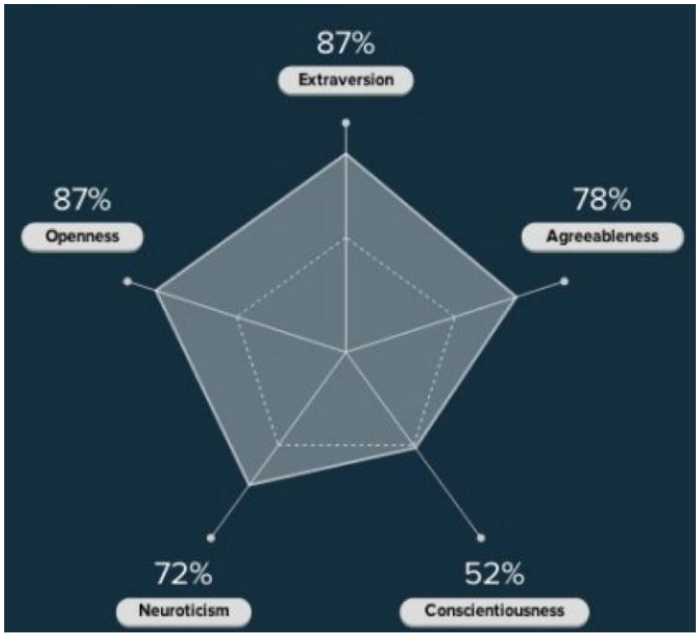
Myers–Brigg





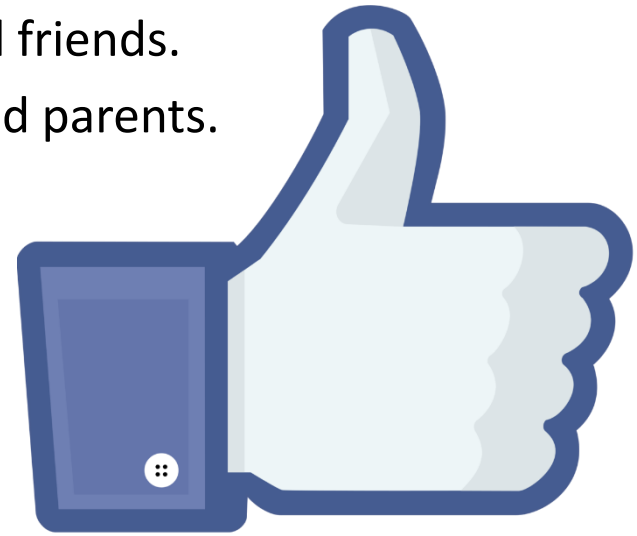
Personalized Ads

- Ads that were matched to people's extraversion or openness-to-experience-level resulted in up to 40% more clicks and up to 50% more purchases.
  - Introvert: "Stay safe and secure with the new Iphone".
  - Extrovert: "Be where excitement is with the new Iphone".



Personality from Likes

- In 2015 86.220 volunteers shared their Facebook Likes and completed a 100-question personality survey that determined where they stood on the Big Five traits.
- Researchers trained a Machine Learning model to predict the personality based on Likes.
  - After 10 Likes the ML model outperformed colleagues.
  - After 70 Likes the ML model outperformed friends.
  - After 150 Likes the ML model outperformed parents.
  - After 300 Likes the ML model outperformed partners.
- (That time) on average, people on Facebook had 227 Likes.

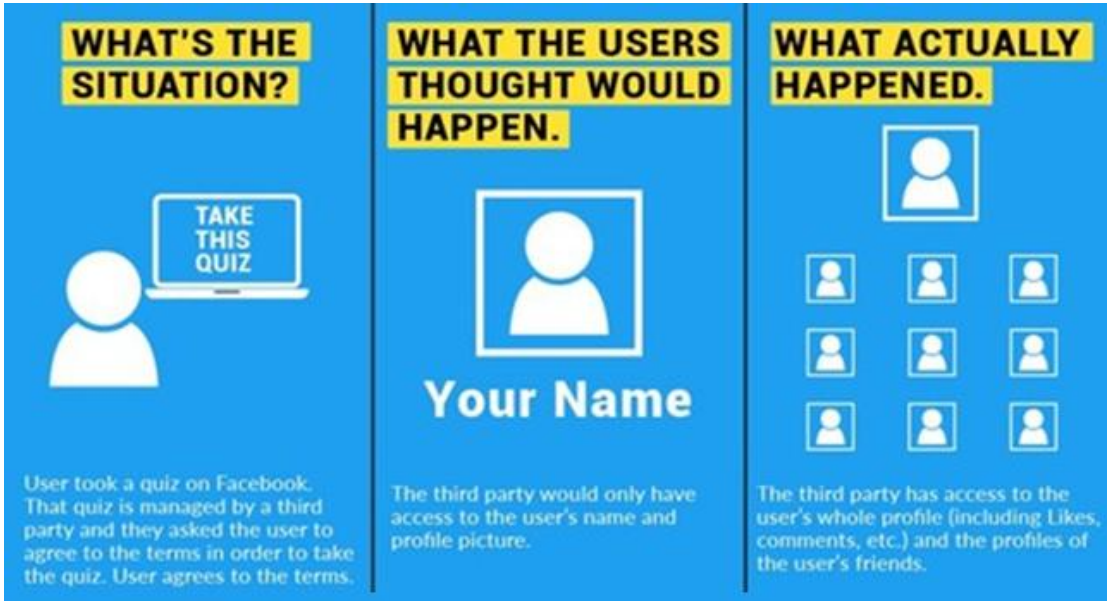


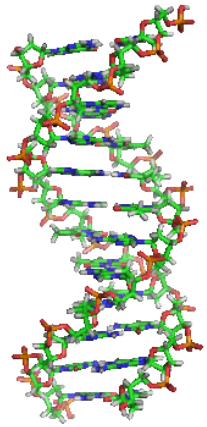
Demographics from Likes & Tweets

- In 2013 58.000 volunteers shared their Facebook Likes and provided their detailed demographic profiles.
- Researchers trained a Machine Learning model to predict various demographic attributes based on Likes.
  - The model determined the ethnicity with 95% accuracy.
  - The model determined the sexual orientation with 88% accuracy.
  - The model determined the political views with 85% accuracy.
- In 2016, researchers trained a machine learning model based on the tweets and the followers of the users, and find, that these features could be used to predict demographic features such as age, gender, and income) with an averaged F1 score of 81%.

Interdependent Privacy

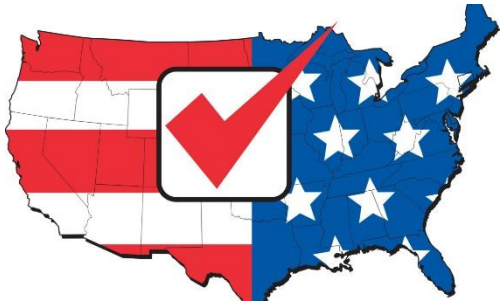
- In today's interconnected setting, the privacy of individual users is bound to be affected by the decisions of others.
  - For instance, a friend share a photo of you or tag you on a picture.
- Prior to 2017 the Facebook API allowed third party apps access data of the friends of a users.
  - For instance, a quiz could obtain information of its users' friends.

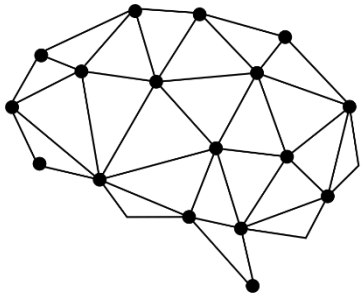




Cambridge Analytica

- GSR (specialized for research) harvested and processed Facebook data in a commercial deal with SCL (specialized for elections).
  - 270.000 App users lead to 50.000.000 profiles.
  - On average one App user revealed data of 160 other non-App users.
- Data was allegedly used to sway elections.
  - US Election 2016
  - Brexit vote





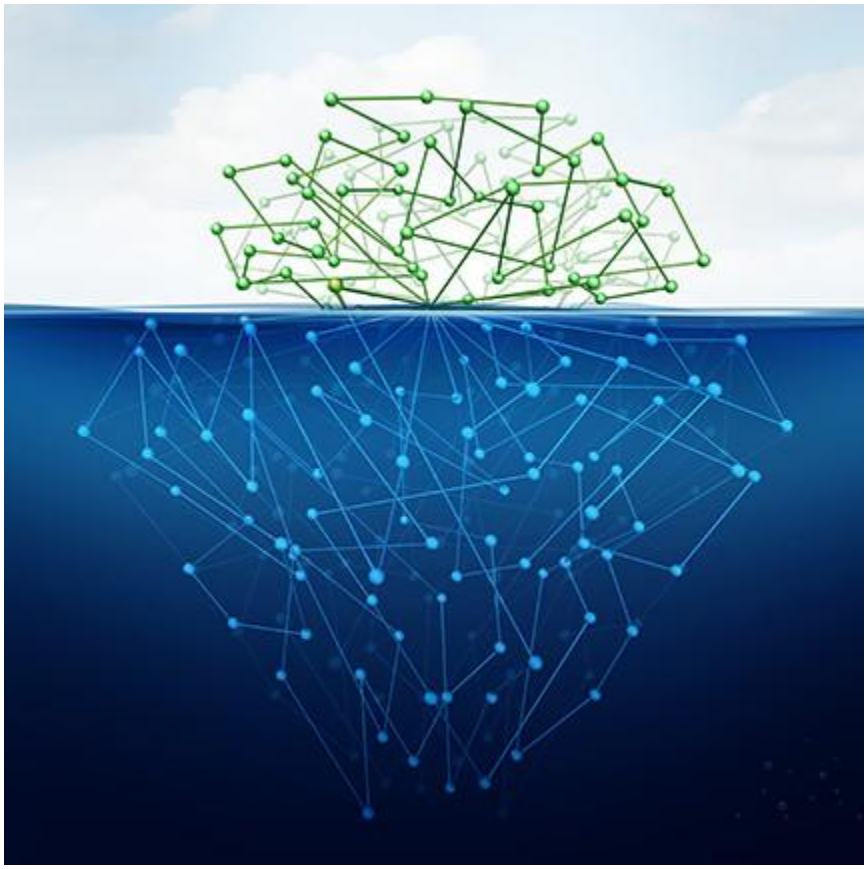
Cambridge Analytica

Microtargeting

- Social Networks know us, so they can offer targeted advertisement.
  - People high in neocriticism and conscientiousness tend to worry a lot and prefer order.
  - Extrovert and agreeable people put other people's needs before theirs, and don't enjoy new experiences.

Players

- Online advertising plays a crucial role in keeping online content free.
- Advertiser: a party that has an online ad it wants to embed in web pages across the web. The advertiser is willing to pay for this service.
  - E.g., Adidas, Nike
- Publisher: a party who owns a web page (or web site) and is willing to place ads from others on its pages. The publisher expects to be payed for this service.
  - E.g., nytimes.com, washingtonpost.com
- Ad-network: a party who collects ads (and payment) from advertiser and places them on publisher pages (along with paying the publisher).
  - E.g., Google, Facebook



Hidden Data

PIN/Password from Sensors

Inferring user input through smartphone gyroscope
S Huang, R Wu, Y Wang, Y Sun, J Zhang, X Li
2022 2nd International Conference on Consumer Electronics and …, 2022 • ieeexplore.ieee.org

Accessory: password inference using accelerometers on smartphones
E Owusu, J Han, S Das, A Perrig, J Zhang
proceedings of the twelfth workshop on mobile computing systems & applications, 2012 • dl.acm.org

Pin skimmer: Inferring pins through the camera and microphone
L Simon, R Anderson
Proceedings of the Third ACM workshop on Security and privacy in smartphones …, 2013 • dl.acm.org

Your PIN sounds good! on the feasibility of PIN inference through audio leakage
M Cardaioli, M Conti, K Balagani, P Gasti - arXiv preprint arXiv …, 2019 - arxiv.org

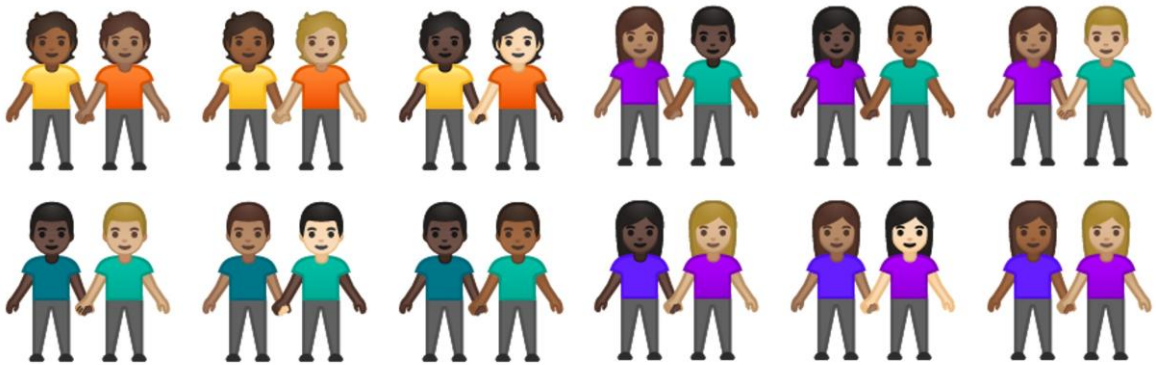
ArmSpy++: Enhanced PIN Inference through Video-based Fine-grained Arm Posture Analysis
H Dai, Y Chen, Y Du, L Wang, Z Shao, H Liu, Y Ren, J Yu, B Liu
ACM Transactions on Privacy and Security, 2024 • dl.acm.org

Sexuality from Selfie

Track 1

More Example

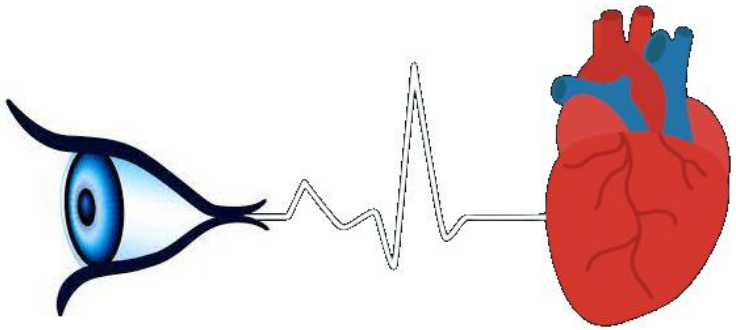
- Faces contain much more information than can be perceived and interpreted by the human brain.
- In 2018 a Machine Learning model was trained on 35.326 facial images with given sexuality.
  - Given a single (five) facial image, the model could correctly distinguish between gay and heterosexual men in 81% (91%) of cases, and in 74% (83%) of cases for women.
  - Human judges achieved much lower accuracy: 61% for men and 54% for women.



Health Status from Selfie

- Blood Pressure prediction: optical sensors in smartphones penetrate the skin to create an image of blood flow patterns.
  - In 2019 1.300 participants made a two-minute video records; the model predicted the blood pressure with almost 95% accuracy.

- Hearth Diseases prediction: the retina contains millions of cells, relying on a network of blood vessels, which also serve as a window into the hearth.
  - In 2022 using eye images from 95.000 people, a ML model trained to estimating heart disease risk outperformed the FRS score (a tool for the same task using age, gender, cholesterol level, blood pressure, and smoking habits).



Fitness Apps

- Religious belief
  - Location data could reveal attending services.
  - Accelerometer & Gyroscope could reveal praying. Five prescribed times a day. / Sunday mornings.
  - Heart rate could reveal user is inactive on Saturdays.

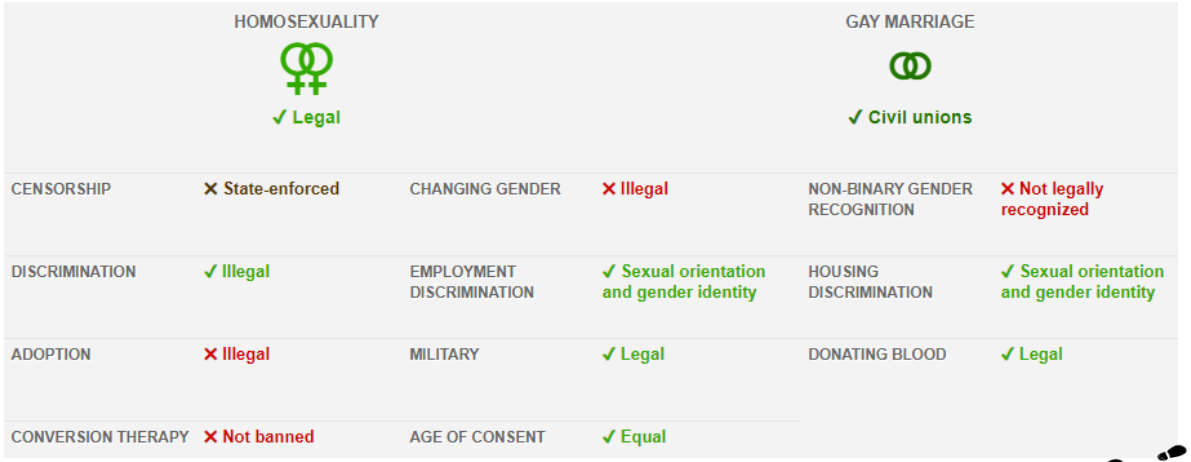
- Sexual activity: as long as your active energy is above your resting energy, your movements get logged.

- These are not proofs, but evidences.

Medium
https://medium.com › themergeofficial
Does your Smartwatch Track your Sexual Activity?

Problem

- People cannot anticipate the future misuse of their data.
  - Tomorrow, one can develop a new ML model to infer sensitive details from seemingly harmless data that you share today.
  - Innocent details from different sources could be combined which might reveal undesired secrets.
- You can be stigmatized based on your religion, political affiliation, sexual orientation, etcetera.
  - Consequences range from mere annoyance to even physical disability or death.



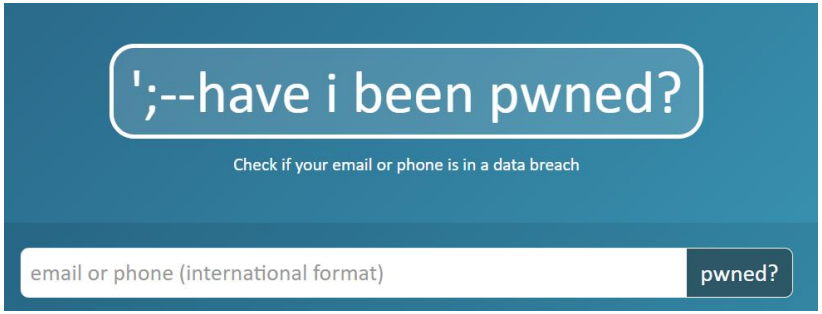
HOMOSEXUALITY ✓ Legal				GAY MARRIAGE ✓ Civil unions	
CENSORSHIP	✕ State-enforced	CHANGING GENDER	✕ Illegal	NON-BINARY GENDER RECOGNITION	✕ Not legally recognized
DISCRIMINATION	✓ Illegal	EMPLOYMENT DISCRIMINATION	✓ Sexual orientation and gender identity	HOUSING DISCRIMINATION	✓ Sexual orientation and gender identity
ADOPTION	✕ Illegal	MILITARY	✓ Legal	DONATING BLOOD	✓ Legal
CONVERSION THERAPY	✕ Not banned	AGE OF CONSENT	✓ Equal		

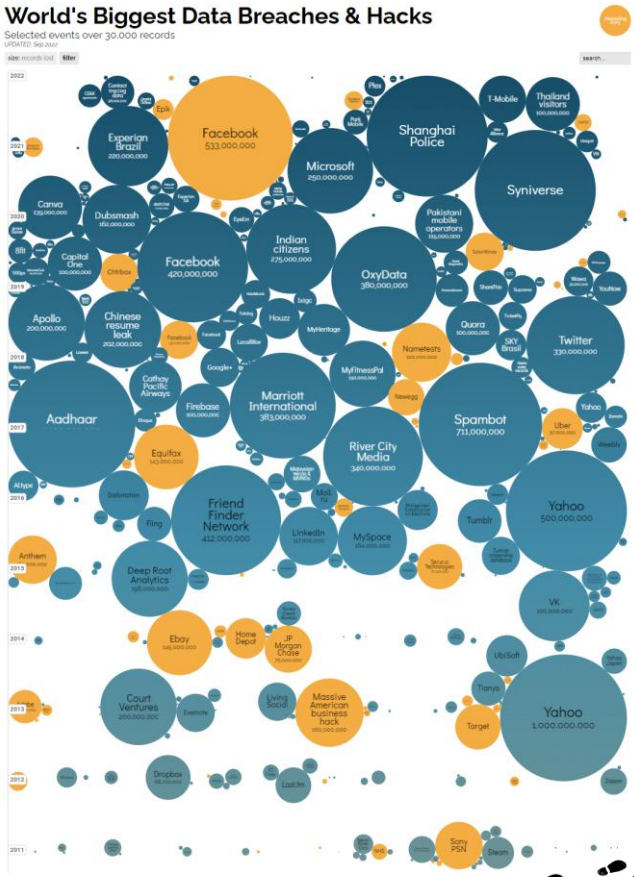
Data Breaches

- Even if you trust the company, they can have security incidents when your data can be stolen and sold in the black market.

- https://haveibeenpwned.com

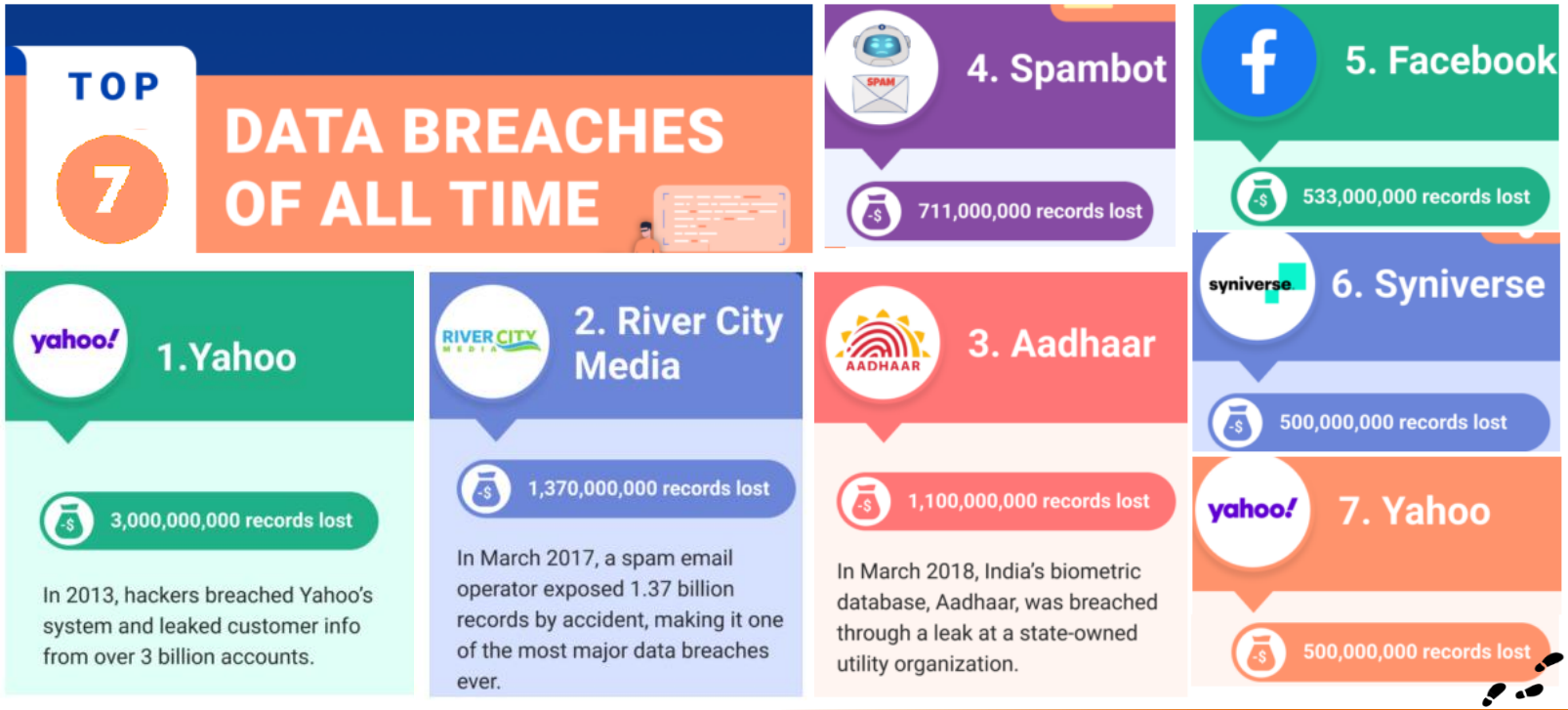
- https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/





Biggest Breaches

- Who & Why: by mistake an employee or intentionally an inside attacker, a cyberpunk hacker, a government agency.
- How: via Social Engineering like Phishing,
  using Brute Force Attacks on Passwords,
  or even by injecting Malware into the System.



Data Brokers

No Free Lunch

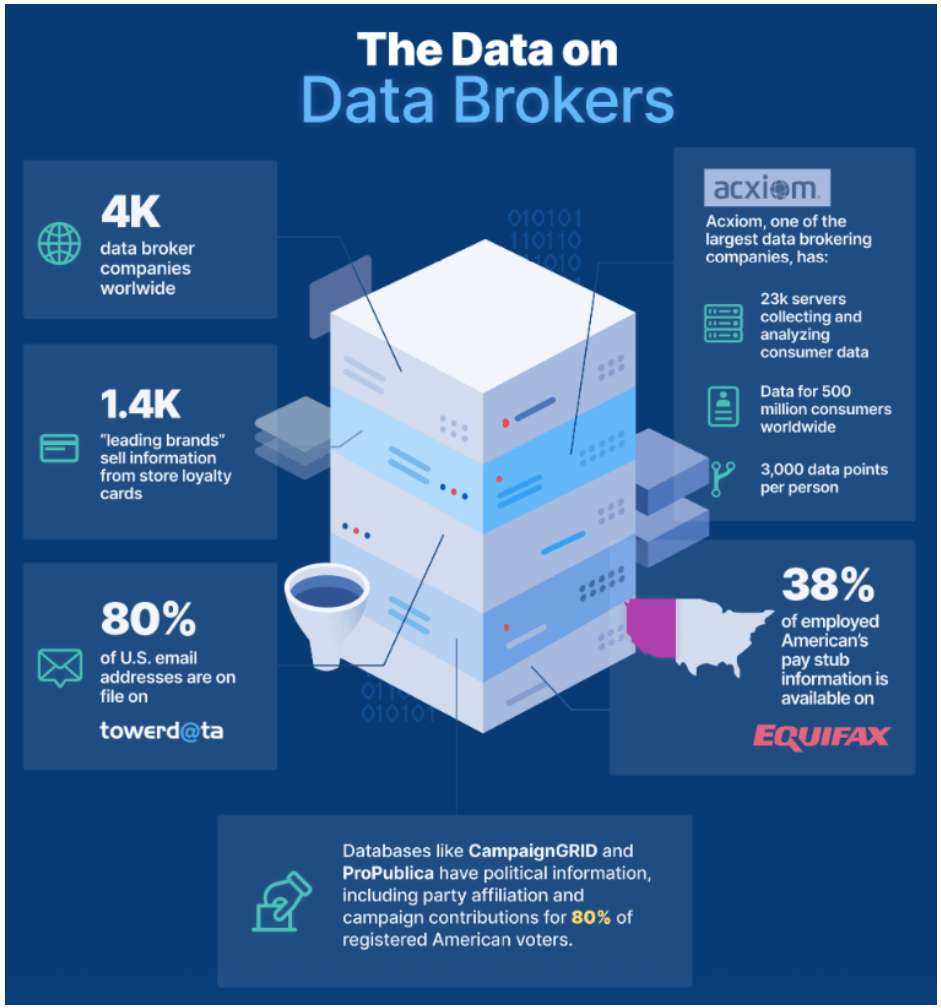
- The entire economy of the internet is basically built on advertisement.
  - All the stuff online is free, because you (and your data) is the product.
- Companies know more about you than you would like, and they do more about it than you would think.
- Download your Facebook dump.
  - Search shared media, for instance voice messages or photos and videos in chats from several years ago.
- Check your timeline on Google Maps.
  - Select a random day in the past.
- They know what you have done better than you do!

Data as Commodity

- Even without a Data Breach your data could leave the thrusted company's server, as services regularly trade and sell information to one another usually via Data Brokers.
  - This could lead to undesired privacy leakage.
- Microtargeting is highly effective, so it is a desire of every web-based service.
- Most companies do not have enough data about users in-house, so they buy it.

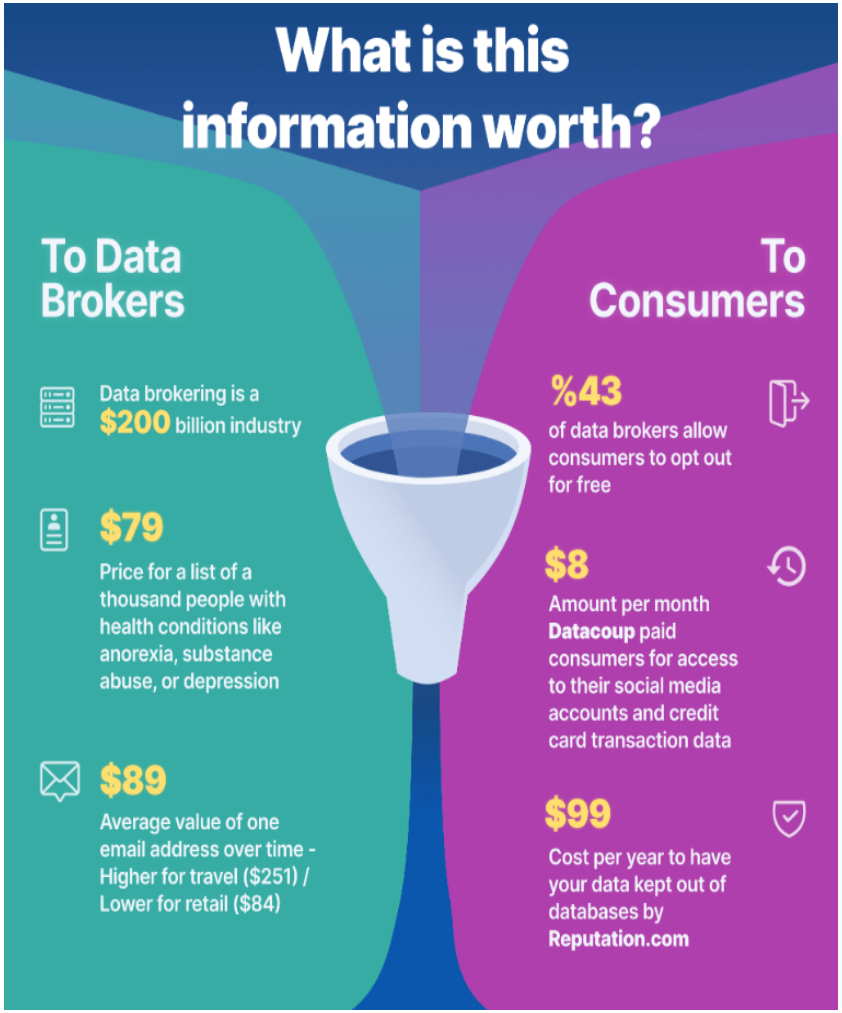
Data Brokers

- Data Brokers gather information from publicly available sources as well as buy information to supplement what they already have.
- They process, clean, and structure the collected data and license it for businesses.
  - For instance, data is sorted by user interests and characteristics for marketing companies.



Collected Data

- Name & Address & SSN
- Date of birth & Gender
- Marital & Family status
- Education levels & Assets
- Occupation & Income
- Phone & Email & Location
- Buying habits & CCN
- Hobbies & Political views
- Health related data
- Web searches and activities
- …



(Not) Sensitive Data

- The medical information you relate to your physician is highly protected, but if you go to a medical website and search for terms like “HIV” or “abortion”, that information is not protected at all.
- Apps on your phone can sell your exact locations to third parties.
  - Claim to be anonymized, but we know better!
- Researcher visited a broker’s website and left without doing anything. Later got an email:
  - *“… We also offer a pretty cool service called Website Visitor Identification which helps brands identify who’s browsing their website. … In fact, it’s how we knew to send you this quick email!”*

Used For

- Marketing and advertising
  - Businesses purchase data so they can tailor marketing or political messages, customer offers, etc.

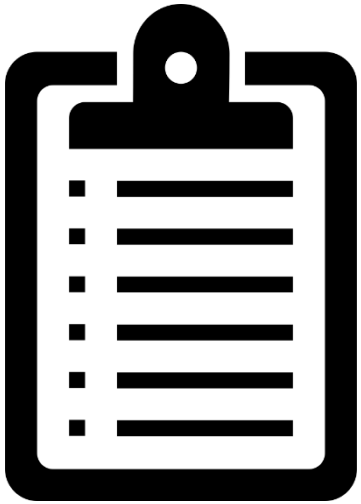
- Risk mitigation
  - Businesses use the data to help crack down on fraud, e.g., calculate a consumer's likelihood to default on a loan.

- Health insurance
  - Businesses use the data to work out what insurance rates you should be charged for cover based on your data profile.

- People search sites
  - Companies (e.g., Spokeo, PeekYou, PeopleSmart, Pipl) allow you to search for a person by name and receive information about them such as address, phone & email, date of birth and so on.

Lists to Sell

- Most Data Brokers target mainstream advertising companies and focus on common categories.
  - New Parents & Impulse Buyer
  - Sports Enthusiast & Music Lover
- Some sell list which are sensitive in nature.
  - Alcoholics
  - Rape Victims
  - Erectile Dysfunction Sufferers
- Few even cross lines
  - Suffering Seniors
  - Pay-day loan Hispanics



JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Wednesday, January 27, 2021

Marketing Company Agrees to Pay $150 Million for Facilitating Elder Fraud Schemes

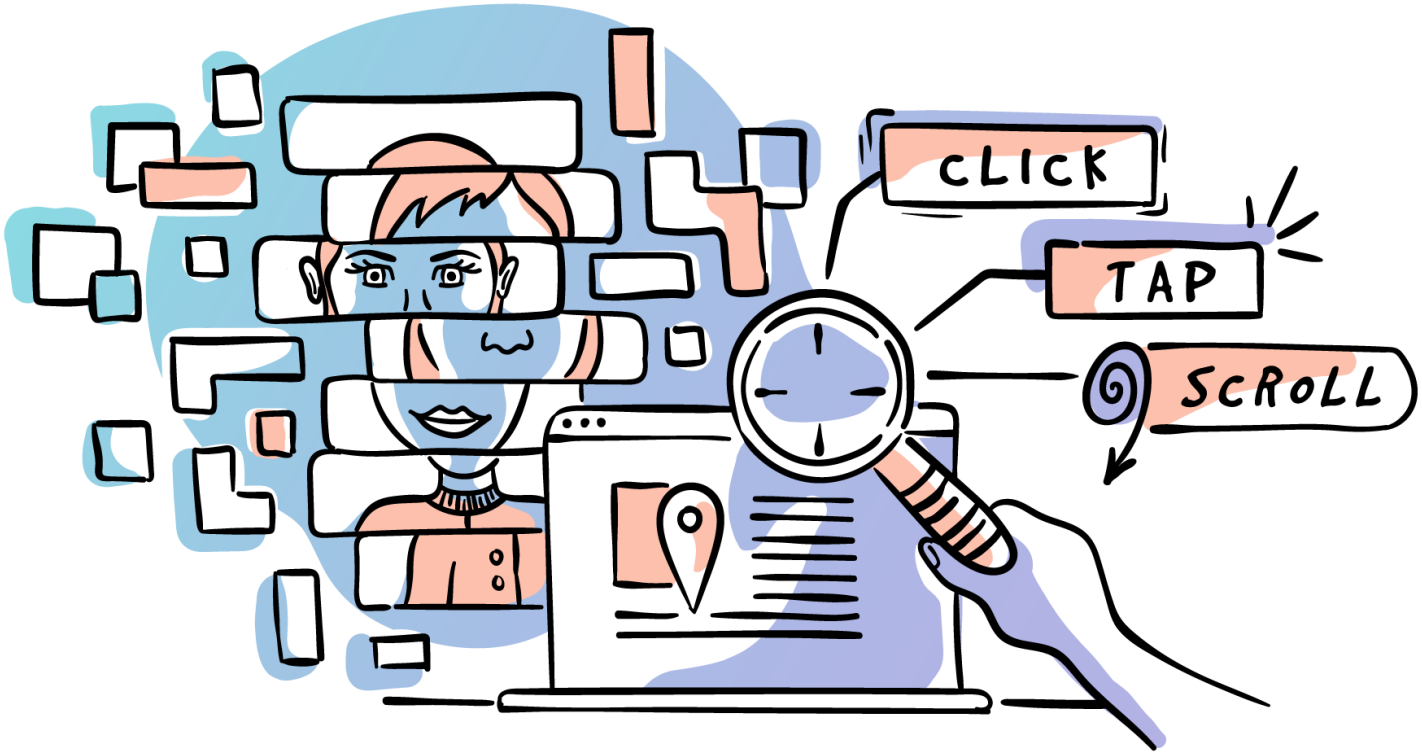
Victims of Schemes to Receive $127.5 Million

The Middleman of Surveillance Capitalism

- When you open a website and agree to give permission to share your consumer data with third-party partners, chances are that your personal data will end up being sold to a data broker.
  - Especially in the United States, where data-privacy law is not very restrictive.
- Under GDPR, in order to process a person's data, one of the six legal bases for data processing must apply.
  - One of these bases is legitimate interest, which is relatively vague and possibly the most abused and misinterpreted legal basis.
  - Another is consent, which is usually obtained by exploiting the inattention of internet users who do not read what they consent to.
- Consent was given for a specific purpose, which might blur after numerous data reselling.

Opting Out

- Privacy Rights Clearinghouse has a comprehensive data broker list. This includes a link to their privacy policies and details on how you can opt-out from each broker.
- Brand Yourself scans for your data in the databases of major data brokers and gives you a report on where your data has been found.
- PrivacyDuck and DeleteMe are examples of companies that will help keep your data private for a fee for their services.

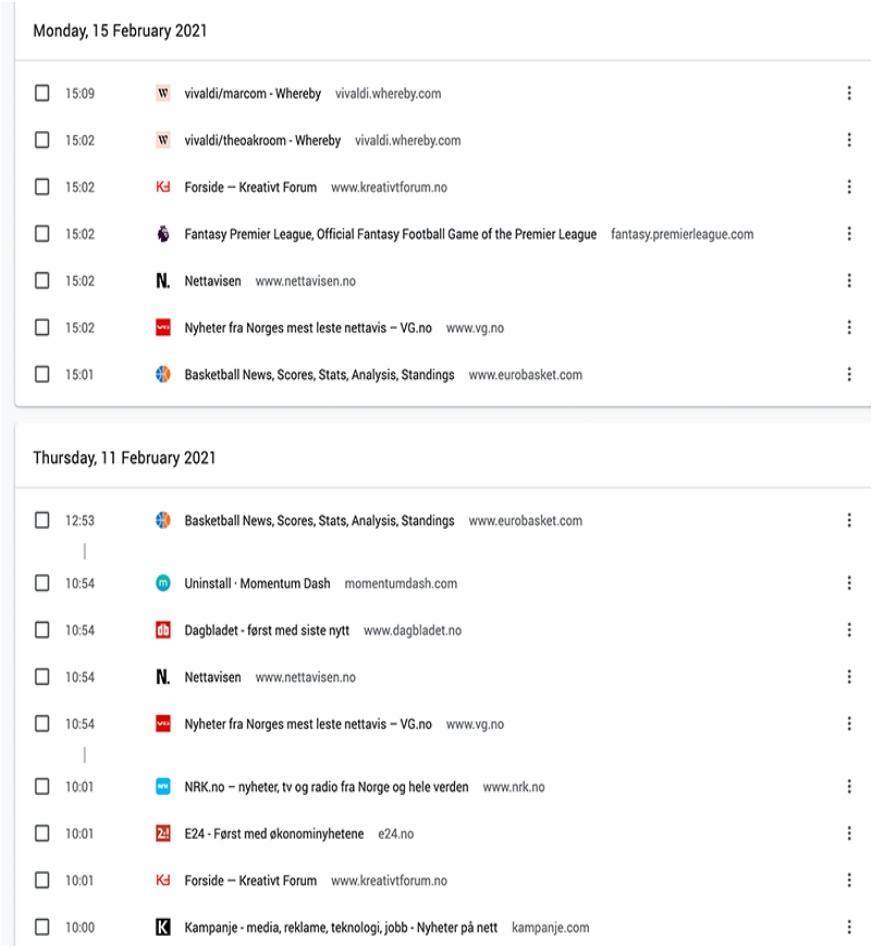


Web Tracking

Tracked Data

- Visit data
- On-site behavior
  - Clickstream
  - Copy-paste actions and content
  - Mouse activities
- Site content
- …

- Is browsing history unique?
  - Success probability
- What background knowledge is needed to re-identify an individual?
  - Plausibility



Monday, 15 February 2021

15:09	vivaldi/marcom - Whereby	vivaldi.whereby.com	
15:02	vivaldi/theoakroom - Whereby	vivaldi.whereby.com	
15:02	Forside – Kreativt Forum	www.kreativtforum.no	
15:02	Fantasy Premier League, Official Fantasy Football Game of the Premier League	fantasy.premierleague.com	
15:02	Nettavisen	www.nettavisen.no	
15:02	Nyheter fra Norges mest leste nettavis – VG.no	www.vg.no	
15:01	Basketball News, Scores, Stats, Analysis, Standings	www.eurobasket.com	

Thursday, 11 February 2021

12:53	Basketball News, Scores, Stats, Analysis, Standings	www.eurobasket.com
10:54	Uninstall · Momentum Dash	momentumdash.com
10:54	Dagbladet - først med siste nytt	www.dagbladet.no
10:54	Nettavisen	www.nettavisen.no
10:54	Nyheter fra Norges mest leste nettavis – VG.no	www.vg.no
10:01	NRK.no – nyheter, tv og radio fra Norge og hele verden	www.nrk.no
10:01	E24 - Først med økonominyhetene	e24.no
10:01	Forside – Kreativt Forum	www.kreativtforum.no
10:00	Kampanje - media, reklame, teknologi, jobb - Nyheter på nett	kampanje.com

De-identification

- Success probability
  - In 2017 researchers find that 50 links are sufficient to uniquely fingerprint 42% of users in a sample of about 370.000 users.
- Plausibility
  - 374 twitter users were asked for 30 day browsing data.
  - They tried to find the public twitter profile of these users.
  - 268 users (72%) with 25-50 links on Twitter were de-identified.

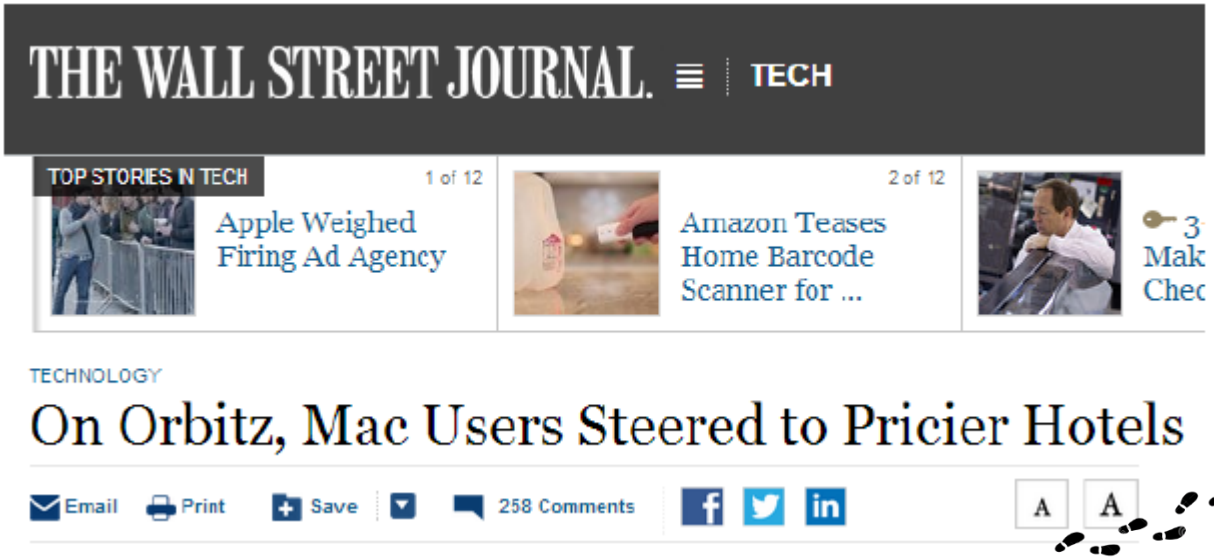
- Two German collected the browsing history of 3 million people by creating a fake company.
  - Asked clickstream data from data brokers.
  - Got it for FREE!

'Anonymous' browsing data can be easily exposed, researchers reveal

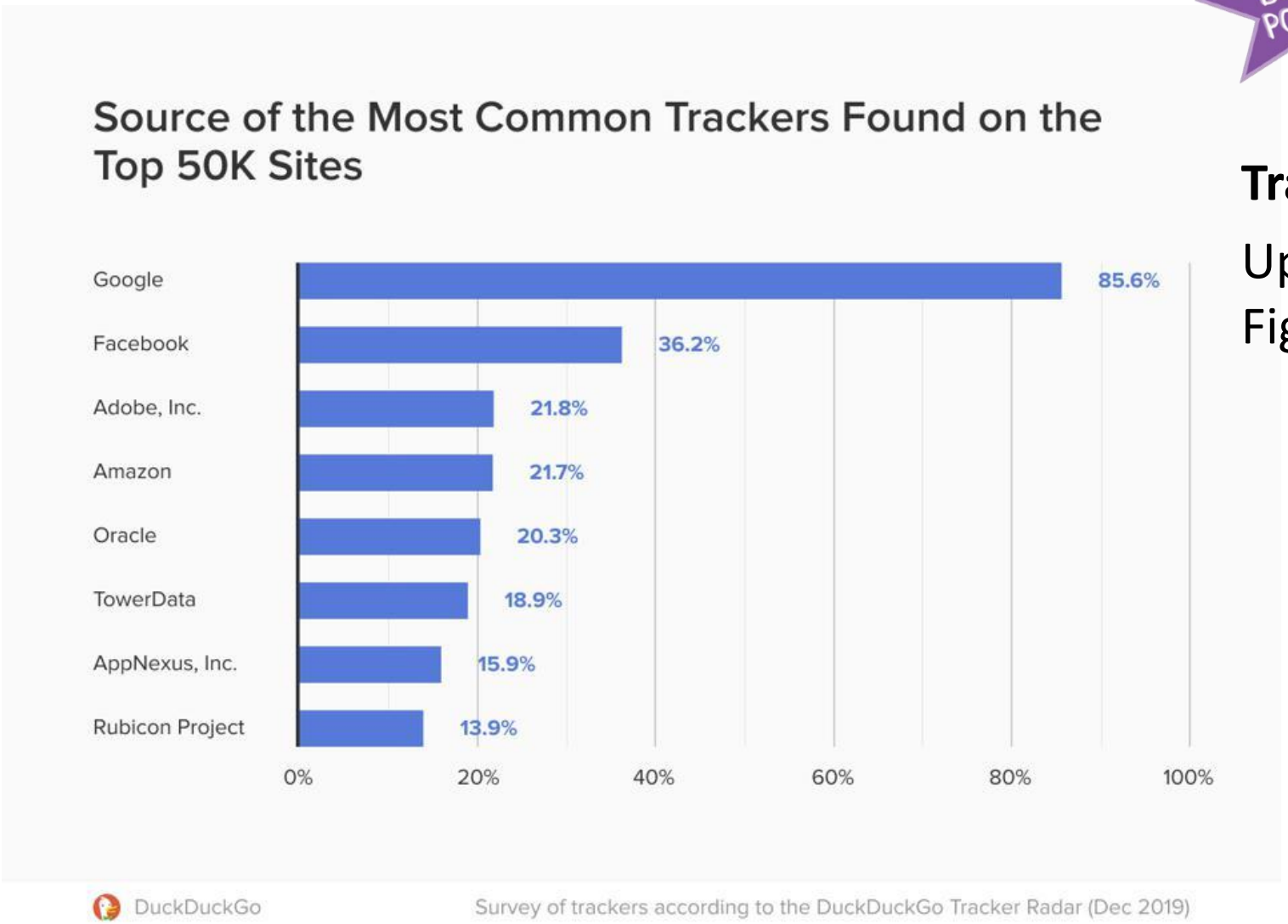
A journalist and a data scientist secured data from three million users easily by creating a fake marketing company, and were able to de-anonymise many users

Issues

- No transparency
  - What information is inferred and used for targeted ads?
- Unfair, discriminatory decisions
  - Price discrimination, financial credibility, government surveillance.
- Heavyweight scripts that bog down browsers
  - Slow down the web by 55% on average.
- Manipulation
  - E.g., political ads (Trump, Brexit)
- Malvertising
  - Malware in ads.



The Unbearable Presence of Tracking



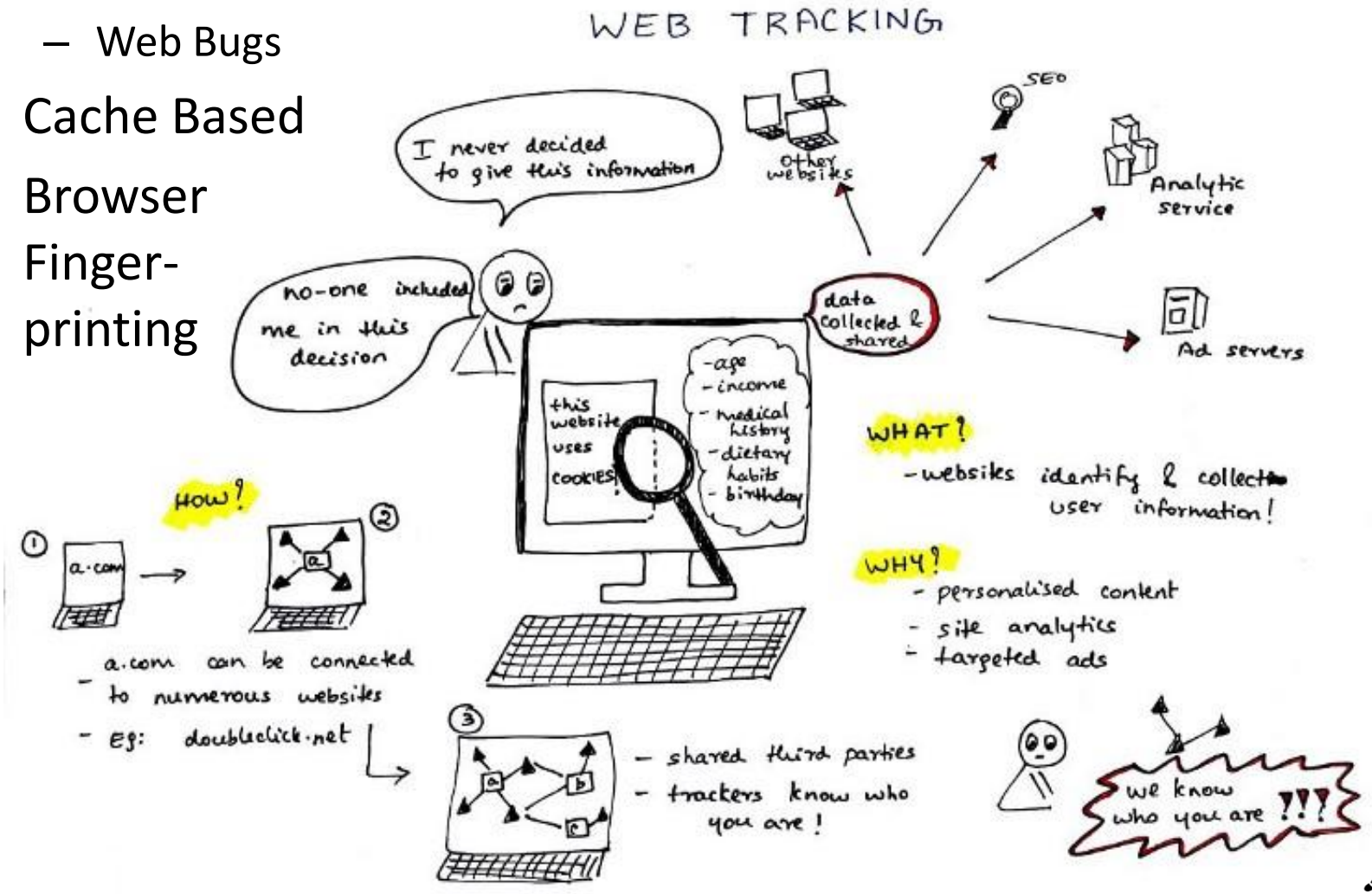
BONUS POINTS

Track 2

Update Figure

Tracking Types

- Storage Based
  - Web Bugs
- Cache Based
- Browser Finger-printing



Storage-based tracking

State Storing

- Web tracking relies fundamentally on a website's ability to store state on the user's machine.
  - Cookies
  - HTML5 uses LocalStorage
  - (Flash used Local Storage Objects (LSOs))

	HTTP Cookies	HTML5 storage	Flash cookies
Storage	4KB	5Mb by default	100KB by default
Expiration	Session by default	Permanent by default	Permanent by default
Location	In SQL file (Firefox)	In SQL file (Firefox)	Stored outside the browser
Access	Only by browser	Only by browser	By multiple browsers on same machine

OBSOLETE

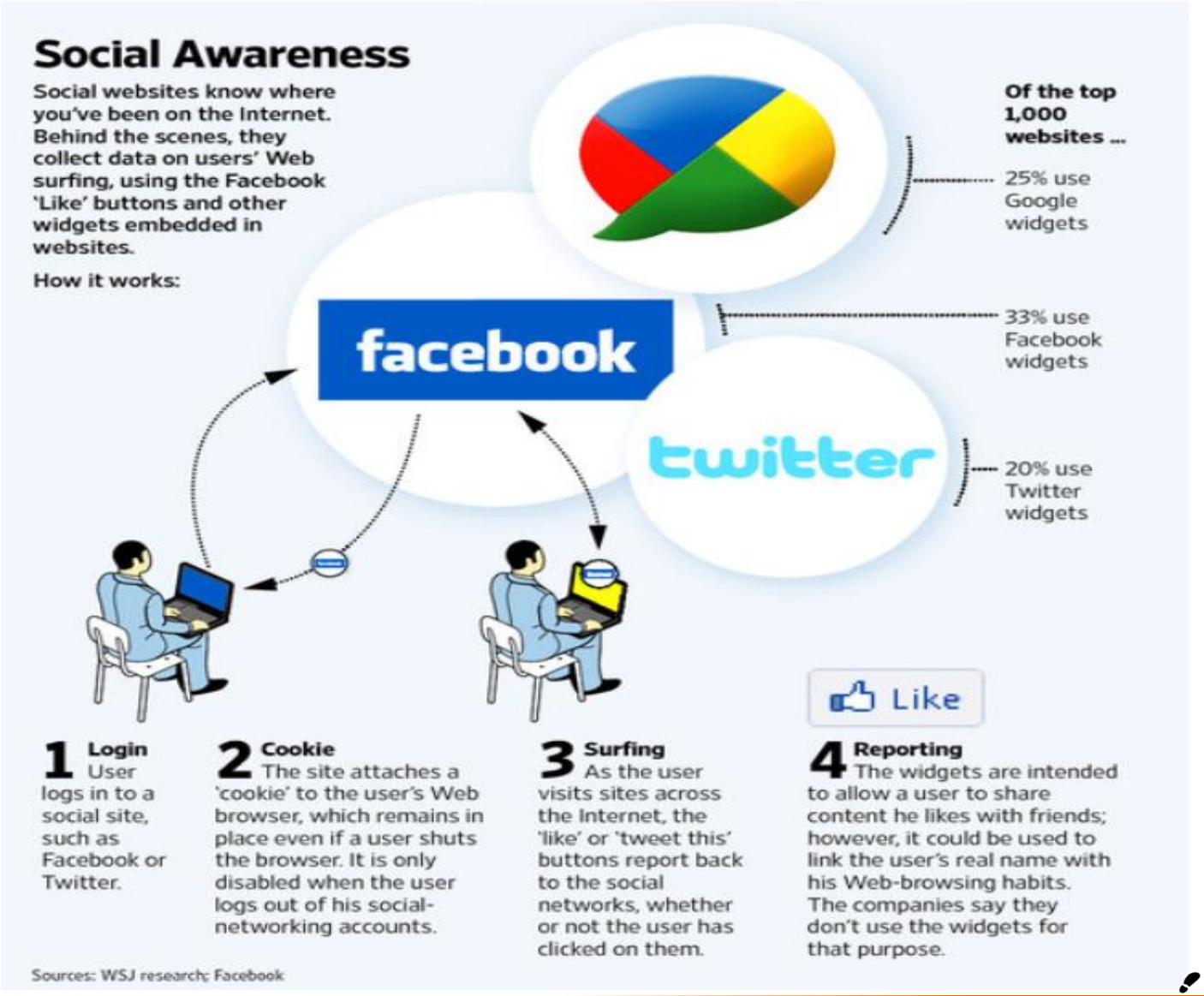
Cookies

- Originally (to make the Web „user-friendly”), it is used to store:
  - Login information (e.g., session Ids)
  - Shopping carts
  - User settings (e.g., default language)
  - …

- Then, for more privacy-invasive purposes: Behavioral profiling
  - Monitor the list of previously visited sites (Web-history)
  - Clicked ads
  - …

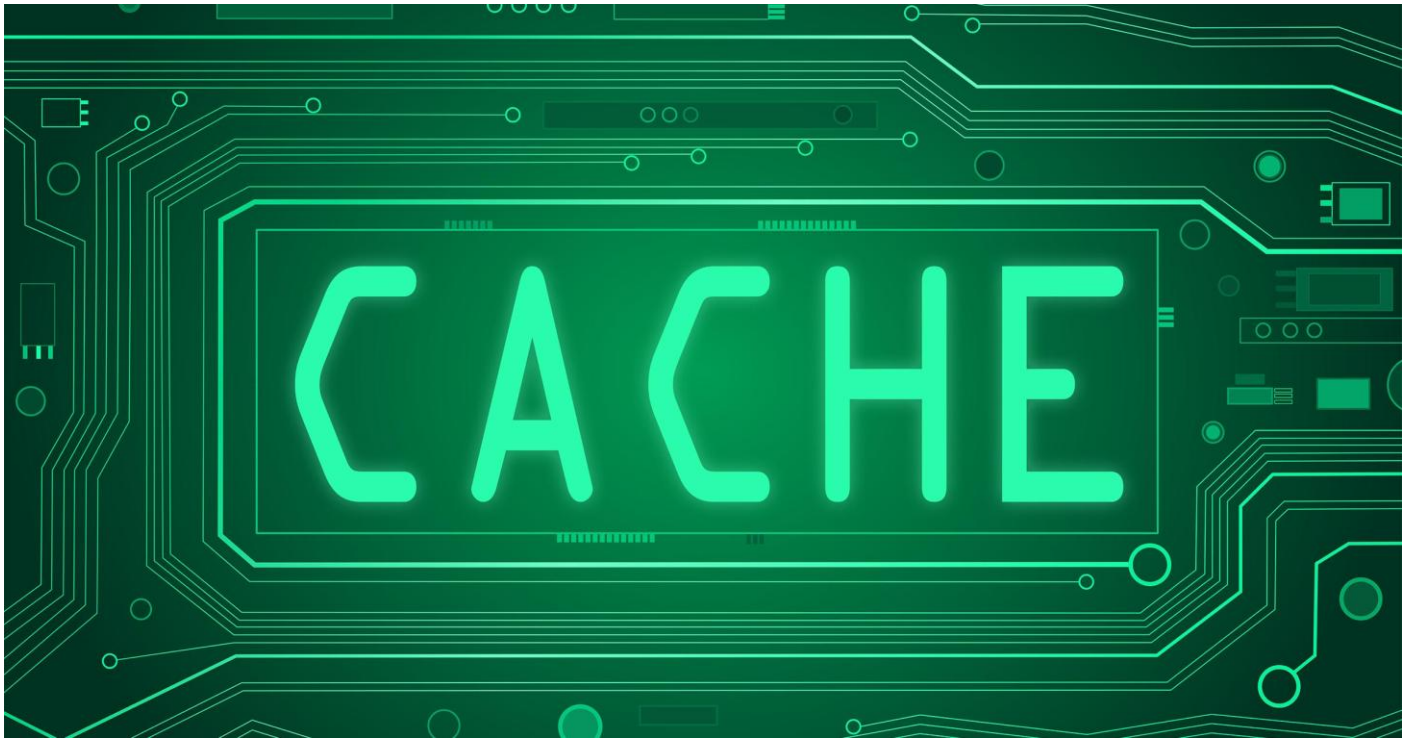
- First-party cookies: set by the domain visited.
- Third-party cookies: set by domains embedded in the page.
- Same-origin policy ensures that cookies (and other client-side state) set by one domain cannot be accessed by another.

Social Buttons



Web Beacons (Bugs)

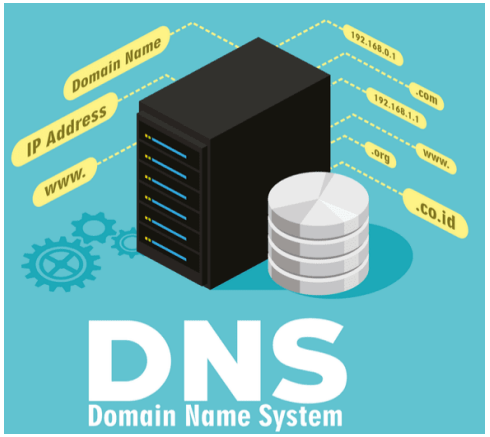
- A website can embed content from another domain by direct inclusion (<img src=...>) or using iframe.
- Web bugs are hidden or camouflaged,
  e.g., 1x1 pixels, transparent GIFs, etc.



Cache-based tracking

Time-based Tracking

- Is the requested content retrieved from the browser cache (visited site) or not (non-visited site)?
- Javascript can measure the loading time, hence it can be used to distinguish between cache and non-cached content.

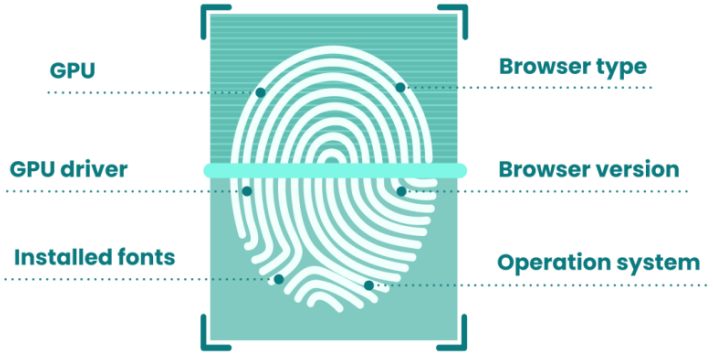


- DNS caching
  - JavaScript does a DNS lookup with the website address and measures the lookup time.
  - If entry exists in the DNS cache (i.e., visited site), the response is significantly faster.
- TLS caching
  - To avoid full TLS-handshake, TLS/SSL session ids are cached in the client's browser.
  - If entry exists in the resumption cache (i.e., visited site), the TLS-handshake is significantly faster.

Fingerprinting

Fingerprinting

- A fingerprint can consist of one or more values which can be read by the web service when the user browses its website.
  - A unique identifier of a device, operating system, browser version or instance, etc.



- These are more-or-less persistent properties which do not change much over time.
- These properties are queried commonly and transparently, the user does not recognize that (s)he is tracked.
  - Mostly implemented by JavaScript and Flash.

https://amiunique.org/

Are you unique ?

Yes! You are unique among the 1225575 fingerprints in our entire dataset.

The following informations reveal your OS, browser, browser version as well as your timezone and preferred language. Moreover, we show the proportion of users sharing the same elements.

50.82%

47.70%

v108

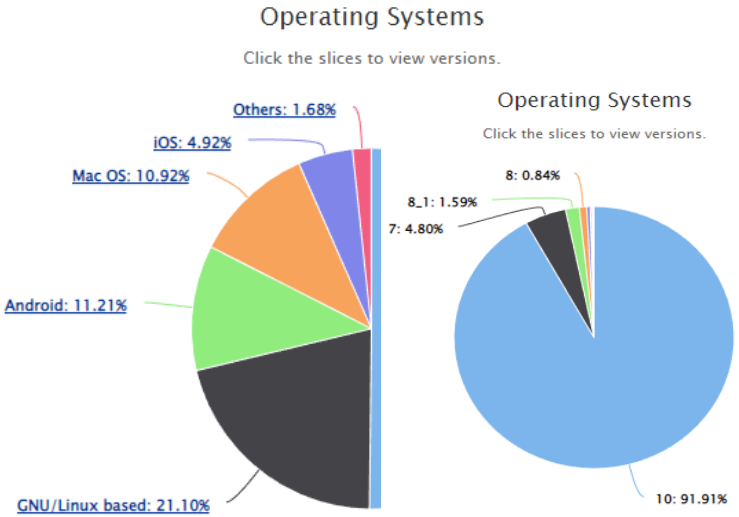
3.86%

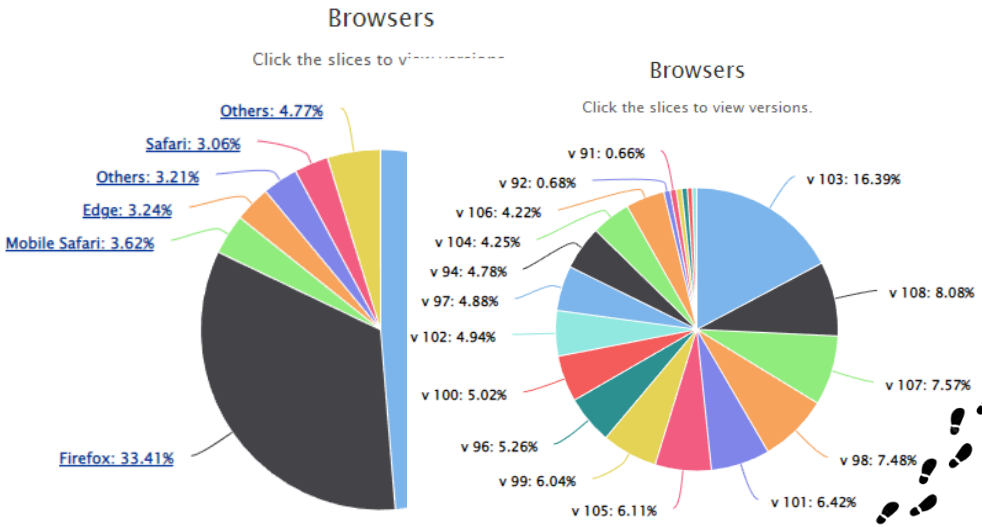
UTC+1

12.19%

en

76.67%





Canvas Fingerprinting

- Using the Canvas API of modern browsers, an adversary can exploit subtle differences in the rendering of the same text or WebGL scenes to extract a consistent fingerprint.
  - Rendering of text depend on operating system, font library, graphics card, graphics driver, and the browser.
  - The fingerprinting script first draws text with the font and size of its choice and adds background colors.
  - Then it calls the Canvas API's ToDataURL method to get the canvas pixel data and hashes it to obtain a fingerprint.

- Easy to obtain, fast, no user awareness.
- May be combined with other high-entropy browser properties such as the list of plugins, fonts, or extensions.

Browser Ext. Fingerprinting (via DOM)

- List of installed extensions cannot be retrieved in a browser, but they can be detected based on their changes made on the page's Document Object Model.
  - DOM: Representation of the structure and content of a website.
  - They add new or remove existing DOM elements.
  - These changes are usually unique to the extension.

```
1  <!DOCTYPE html>
2
3  <html>
4
5    <head>
6      <!-- Title -->
7      <title>Website Title Goes Here</title>
8      <!-- Meta content type -->
9      <meta charset="utf-8" />
10     <!-- Meta description -->
11     <meta name="description" content="Website desription can go here">
12     <!-- Viewport -->
13     <meta name=viewport content="width=device-width, initial-scale=1">
14   </head>
15
16   <body>
17     <!-- Content goes here... -->
18   </body>
19
20 </html>
```

Extension's change comes here

Stats (2016)

- On Chrome Store, 9% of all extensions (out of the 10.000 most popular) are fingerprintable based on their DOM changes.
- 70% of users (out of 854) have at least one fingerprintable extension.
- 14% of all users (out of 854) have unique combination of extensions which cause detectable DOM changes.

- More popular websites may invoke more plugins, hence they have larger fingerprinting power.

Track 3

Update Stats

Browser Ext. Fingerprinting (via Resources)

- Another method to detect extensions is through their Web accessible resources.
  - Extension resources that are referenced/accessible in a regular webpage are flagged as web accessible in the manifest files.
  - If a JavaScript injects some resources into webpage, it must be flagged as web accessible.
  - Resource is available as: chrome-extension://<extensionid>/<pathToFile>

- chrome-extension://cfhdojbkjhnklbpkdaibdccddilifddb/icons/abp-40.png

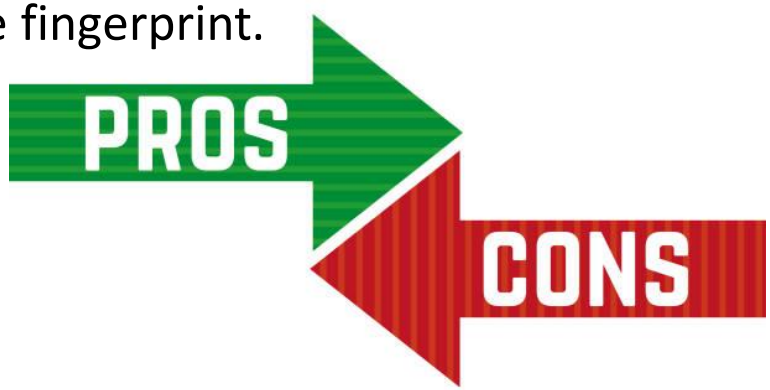
Browser Fingerprinting

Pros

- Fast and quite precise
- Passive (no data storage needed)
- Very hard to control by the users
  - Probably need special browser designed specifically to have no identifiable fingerprint.

Cons

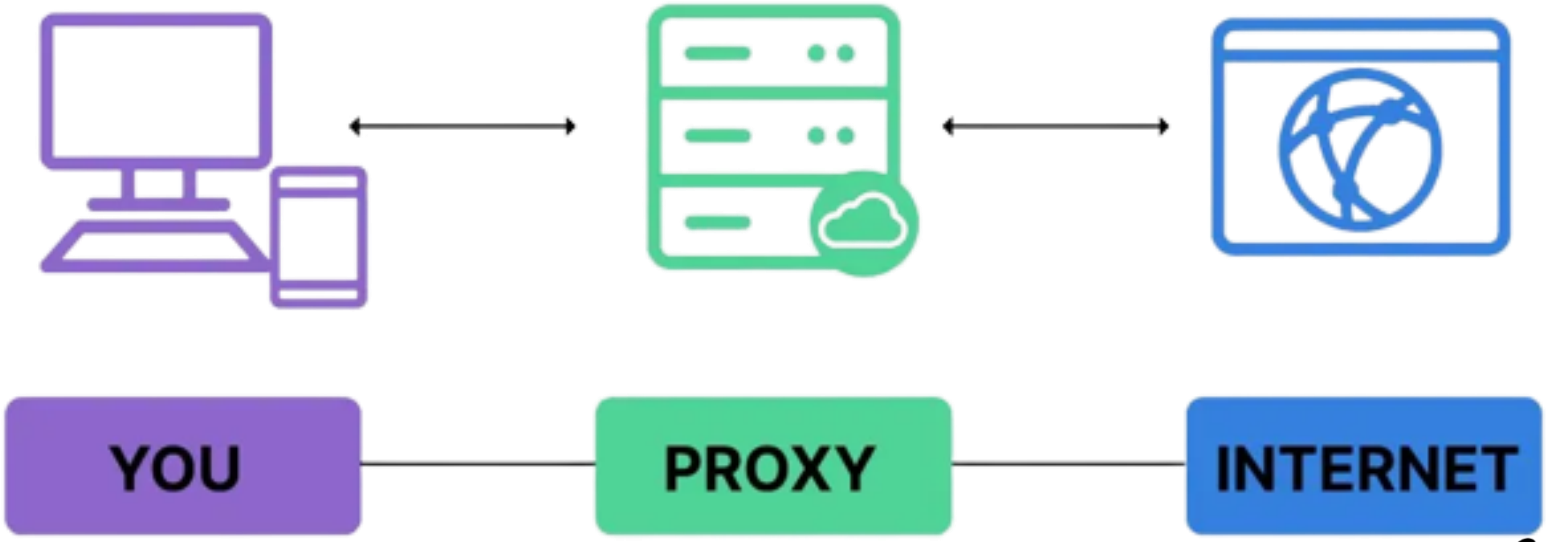
- Browser dependent
- Fingerprint stability problems
  - Browser fingerprints can change quite rapidly.



Defenses

Network-based Defense

- Interception proxies (e.g., Privoxy)
  - Forward and modify web traffic.
  - Have URI-based filtering capabilities and can modify the content and headers of web requests.
  - Can remove cookies or tracking codes.
- Not effective when TLS is used (cannot modify TLS connections).



Defense via Browsers

Brave

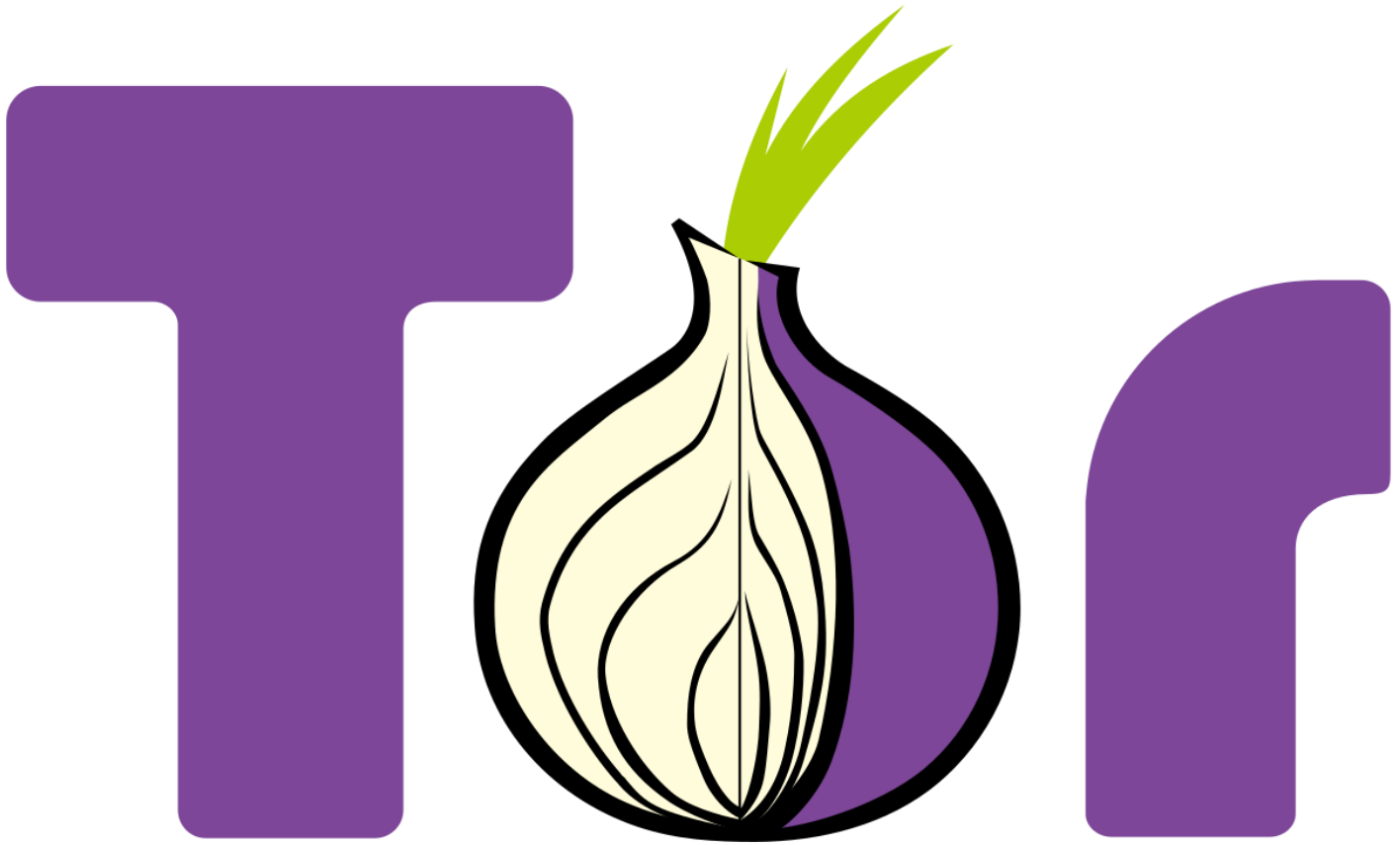
Security and Privacy							
Private Browsing mode	✓	✓	✓	✓	✓	✓	✓
Blocks third-party tracking cookies by default	✓	—	✓	✓	✓	✓	✓
Blocks cryptomining scripts	✓	—	✓	—	✓	✓	—
Blocks social trackers	✓	—	✓	✓	—	✓	—

Portability							
OS availability	✓	✓	✓	—	✓	✓	—
Mobile OS availability	✓	✓	✓	—	✓	✓	—
Syncs with mobile	✓	✓	✓	✓	✓	✓	—
Password management	✓	✓	✓	✓	✓	✓	✓
Primary password	✓	—	✓	—	✓	—	—

Epic

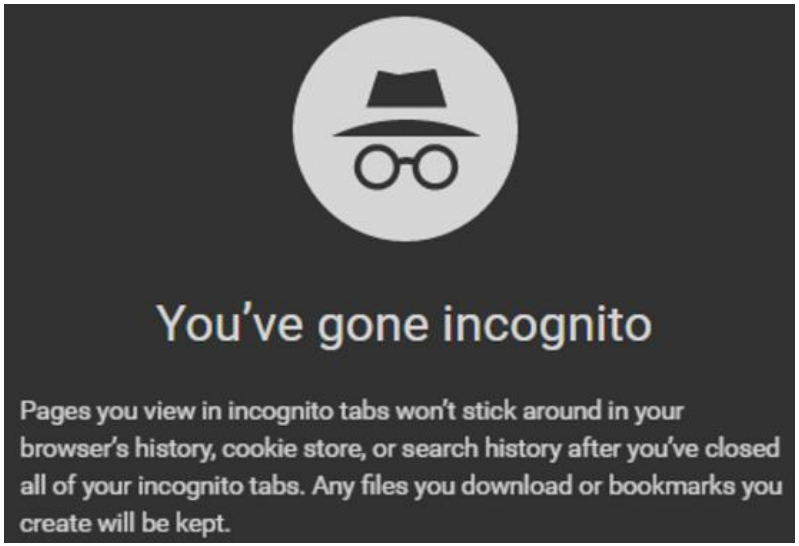
Vivaldi

Coming Soon



Private Browsing

- Aims to protect browser state from adversaries with physical access to the machine.
- It does not primarily address the threat model of web tracking.
- Clearing of cookies when exiting private browsing mode can help, but it is not sufficient to address the problem of tracking.



Browser Extensions

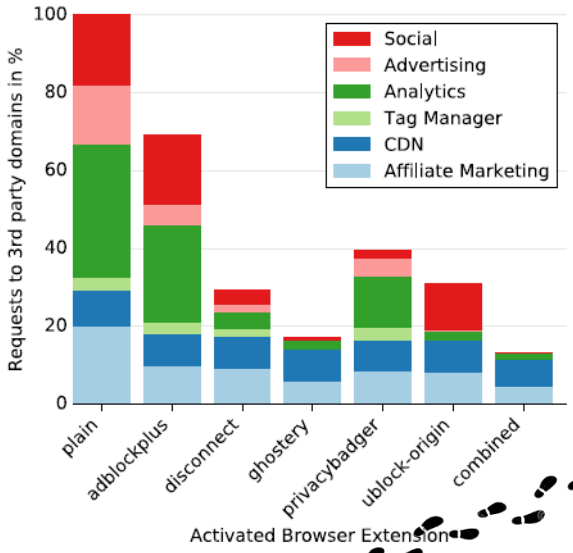
- Ad blockers
  - Block advertisements from websites.
  - Fail to block several other non-advertising third-party trackers.
- Tracker blockers
  - Block third-party trackers.
- Content blockers
  - Block both ads and trackers.

Extension Studied	Blocking Method
Ad blockers	
AdBlock AdBlock Plus	EasyList, EasyPrivacy (Not default)
Tracker blockers	
Ghostery	Ghostery Blocklist
PrivacyBadger	Heuristics
Disconnect	Disconnect Blocklist
Content blockers	
uBlock uBlock Origin	EasyList, EasyPrivacy, Misc. lists

Blockers

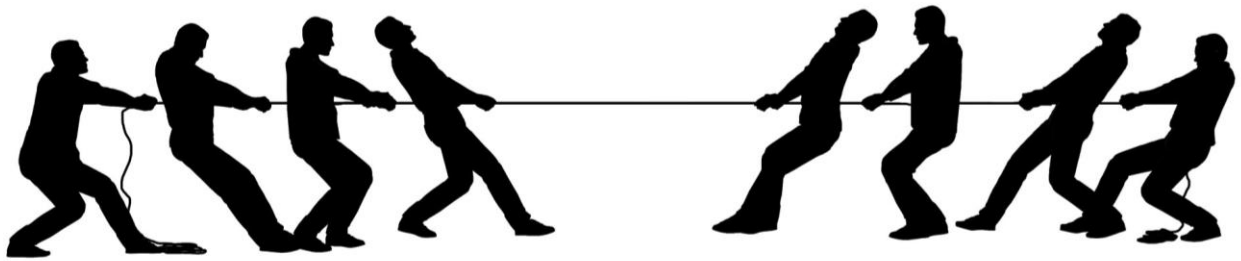
- Ad blockers (e.g., AdBlock Plus, uBlock)
  - Searches the rendered HTML page (DOM tree) through regular expressions and blocks the downloading of web-components (bugs, ads, JS).
- Tracker blockers (e.g., Ghostery, Disconnect, PrivacyBadger)
  - Companies behind these tools maintain blocking rules or use heuristics.

- NoScript: Blocks Java, JavaScript, Flash, SilverLight, …, but also breaks most of the functionality on the site.
- AdBlockPlus: most widespread extension, where the functionality of the site is untouched, but undesired content remain.



The Blocking War

- There is an ad-blocking arms race
  - Ads ➔ Adblocks ➔ Anti Adblocks ➔ Anti-anti Adblocks ➔ …



- Regulations require ads to be clearly labeled so that a human can recognize them, which has created a built-in advantage for consumers and ad-blockers.
- Tracking is executed on the client's machine.
  Browsers can always be modified, extended to suppress ads.
  - Hence, ad industry cannot win!

Take Away

- Profiling can be used for personalized manipulation.
- Online privacy is inherently interdependent.
- Our data reveals much more about ourself than what we think.
- Data scattered across the internet is collected by Data Brokers who sell it for profit.
- There are a handful of ways one can be tracked on the internet, e.g., storage-based (via cookies) and cache-based (via caches).
- Fingerprinting is based on properties which do not change rapidly over time (e.g., browser extensions).
- Specific browsers (e.g., Brave) and extensions (e.g., Ghostery) could mitigate the risk.
- In this mouse-cat game the ad industry has the disadvantage.

Control Questions

- What are the advertiser, the publisher, and the advertiser network?
- What is fingerprinting?
  - Give two examples of browser fingerprinting!
- What is inter-dependent privacy?
  - Provide two examples!

References

- Psychological targeting as an effective approach to digital mass persuasion
- Computer-based personality judgments are more accurate than those made by humans
- Private traits and attributes are predictable from digital records of human behavior
- Predicting Twitter User Demographics using Distant Supervision from Website Traffic Data
- Deep neural networks are more accurate than humans at detecting sexual orientation from facial images.
- Smartphone-Based Blood Pressure Measurement Using Transdermal Optical Imaging Technology
- Artificial intelligence-enabled retinal vasculometry for prediction of circulatory mortality, myocardial infarction and stroke
- De-anonymizing Web Browsing Data with Social Networks
- Xhound: Quantifying the fingerprintability of browser extensions
- Block me if you can: A large-scale study of tracker-blocking tools

- TED Video