# HOW TO TRY TO PRESERVE YOUR PRIVACY ONLINE

LIVIU VÂLSAN

21ST OF OCTOBER 2020

CERN COMPUTER SECURITY TEAM

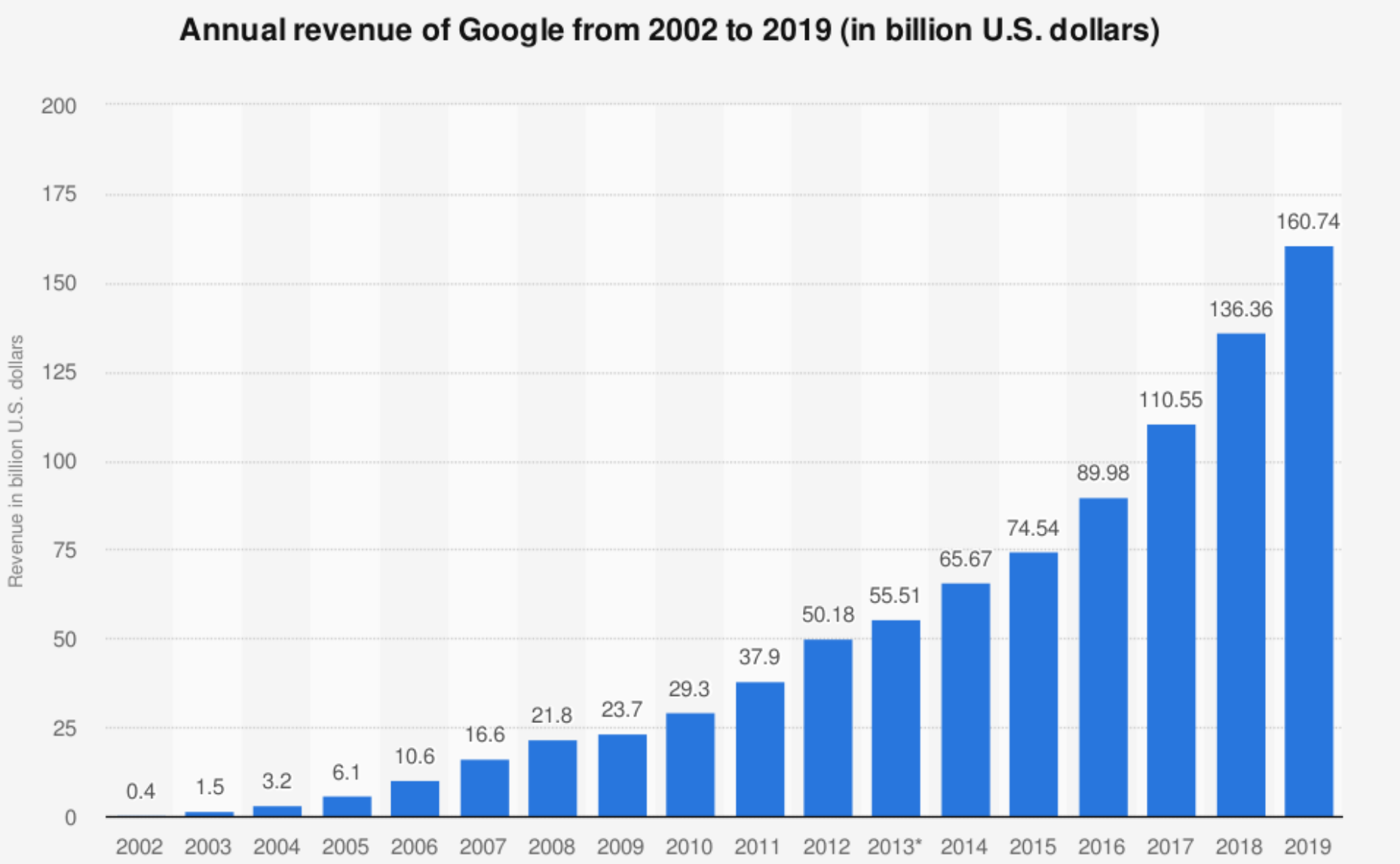
# DISCLAIMER

The opinions expressed in this presentation are solely those of the presenter and not necessarily those of the Organization or those of the CERN Computer Security Team.

*“Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.”*

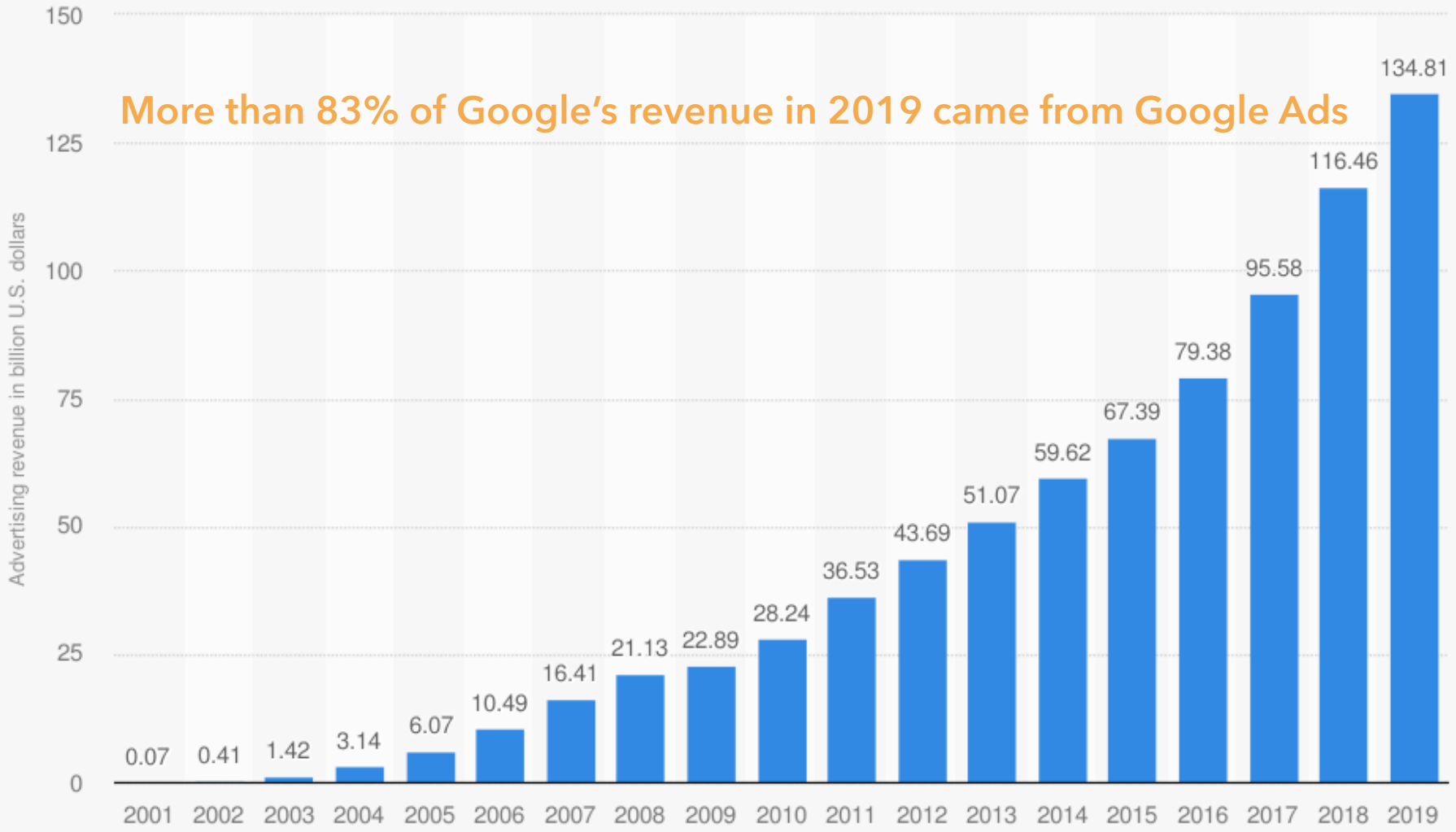
- Edward Snowden

Internet companies such as Google and Facebook are some of the wealthiest companies in the world




Source: https://www.statista.com/statistics/266206/googles-annual-global-revenue/

## Advertising revenue of Google from 2001 to 2019 (in billion U.S. dollars)



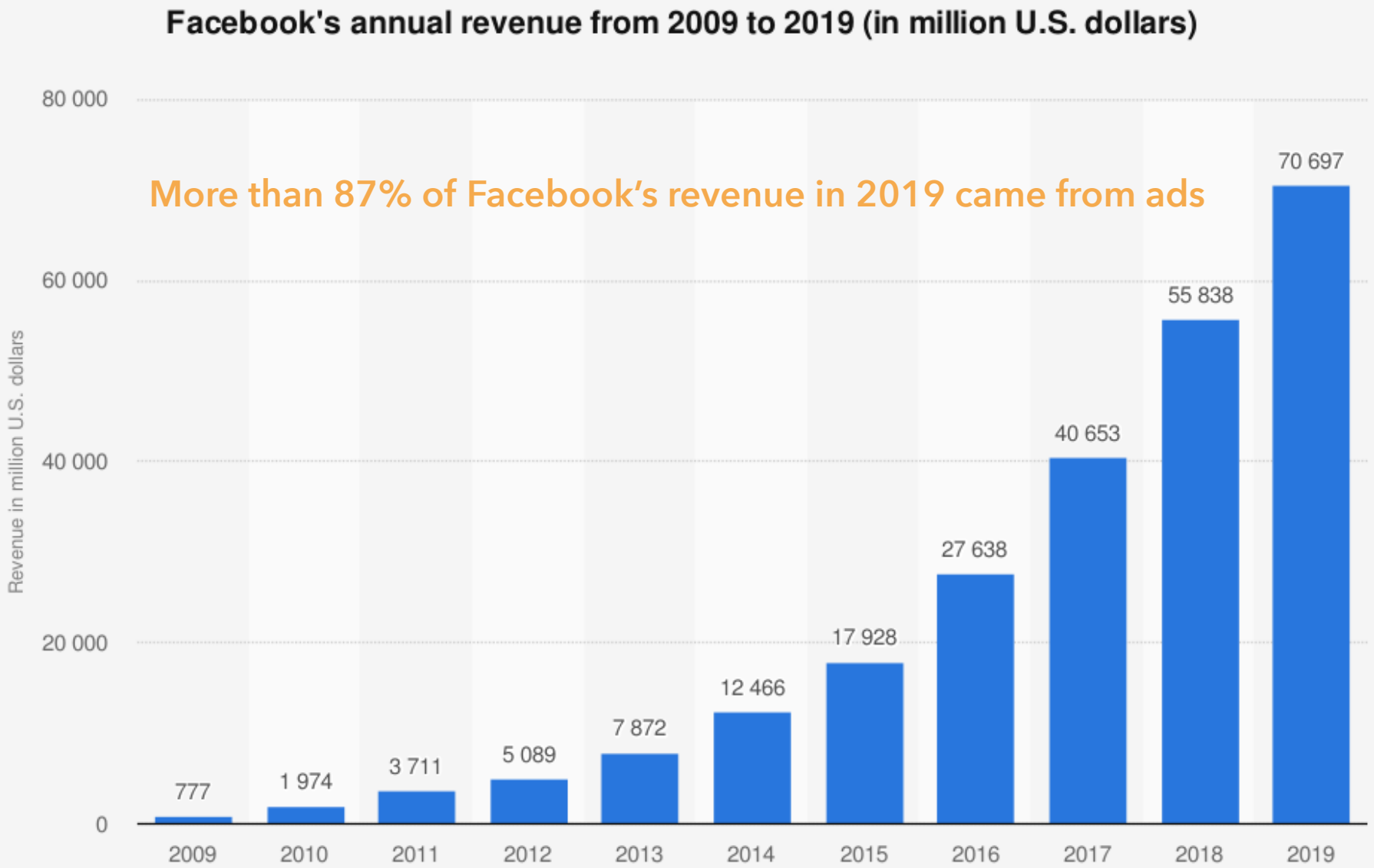

Sources
Google; Alphabet
© Statista 2020

Additional Information:
Worldwide; Google; 2001 to 2019

Source: https://www.statista.com/statistics/266249/advertising-revenue-of-google/

# GOOGLE ADS ECOSYSTEM

- Google's advertisements integration touches almost all of Google’s web properties.
- Any recommended websites or content you see when using the Google search engine, Gmail, YouTube, Google Maps, and other Google services are generated through the advertising platform.




Source: https://www.statista.com/statistics/268604/annual-revenue-of-facebook/

In the beginning of Silicon Valley large computing companies such as Microsoft or IBM were in the business of creating hardware and software, selling them out to customers.

Nowadays, the biggest companies in Silicon Valley are in the business of selling their users.

We don't pay for the services we use, advertisers pay for them.

So advertisers are the customers.

And we are the product being sold.

We are way past the point where Google is just a search engine and Facebook a place to see what you're friends are doing

Note: While this presentation mostly mentions Google and Facebook, most other public cloud companies try to follow their lead meaning that in many cases they are similarly as bad, just on a smaller scale.

# What's their business model?

Know your users and get them to spend as much time as possible in front of the screen.

What do the advertisers pay for?
To have their ads shown to the users of the service.

What is the product being sold?
The gradual, slight, imperceptible change in our own behaviour and perception.

# Surveillance capitalism

Every business wants a guarantee that if it places an ad, it will be successful.
These online ad services sell certainty.
For that you need to have great predictions.
And in turn, for that you need to have a lot of data.

These companies are trading in human futures at scale.

Everything, but everything you are doing online, it's being watched, tracked, measured and analysed.

Here's a small glimpse into what these companies know about you

Want to freak yourself out? I'm gonna show just how much of your information the likes of Facebook and Google store about you without you even realising it

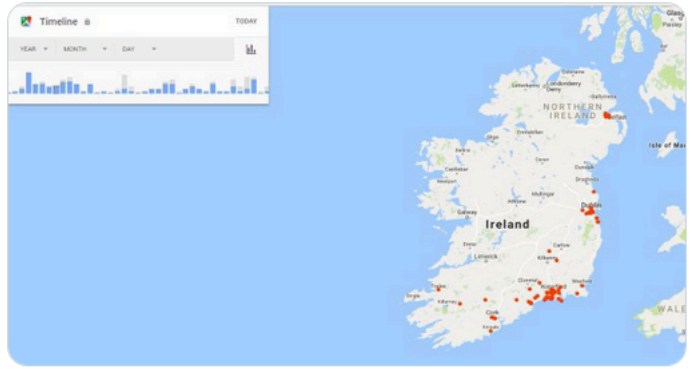
2:57 PM · Mar 24, 2018 · Twitter Web Client

**146.9K** Retweets **26.5K** Quote Tweets **240.6K** Likes

**Dylan Curran** @iamdylancurran · Mar 24, 2018
Replying to @iamdylancurran
1. google.com/maps/timeline?... Google stores your location (if you have it turned on) every time you turn on your phone, and you can see a timeline from the first day you started using Google on your phone

218 3.7K 9.8K

**Dylan Curran** @iamdylancurran · Mar 24, 2018
2. This is every place I have been in the last twelve months in Ireland, going in so far as the time of day I was in the location and how long it took me to get to that location from my previous one




78 1.7K 6.2K

**Dylan Curran** @iamdylancurran · Mar 24, 2018
3. myactivity.google.com/myactivity Google stores search history across all your devices on a separate database, so even if you delete your search history and phone history, Google STILL stores everything until you go in and delete everything, and you have to do this on all devices

78 2.5K 7.3K

**Dylan Curran** @iamdylancurran · Mar 24, 2018
4. google.com/settings/ads/ Google creates an advertisement profile based on your information, including your location, gender, age, hobbies, career, interests, relationship status, possible weight (need to lose 10lbs in one day?) and income

48 1.9K 5.5K

**Dylan Curran** @iamdylancurran · Mar 24, 2018
5. Google stores information on every app and extension you use, how often you use them, where you use them, and who you use them to interact with (who do you talk to on facebook, what countries are you speaking with, what time you go to sleep at) security.google.com/settings/secur...

32 1.7K 4.6K

**Dylan Curran** @iamdylancurran · Mar 24, 2018
6. youtube.com/feed/history/s... Google stores ALL of your YouTube history, so they know whether you're going to be a parent soon, if you're a conservative, if you're a progressive, if you're Jewish, Christian, or Muslim, if you're feeling depressed or suicidal, if you're anorexic...

52 2K 5.5K

**Dylan Curran** @iamdylancurran · Mar 24, 2018
7. Google offers an option to download all of the data it stores about you, I've requested to download it and the file is 5.5GB BIG, which is roughly 3 MILLION Word documents google.com/takeout

78 3.3K 9.2K

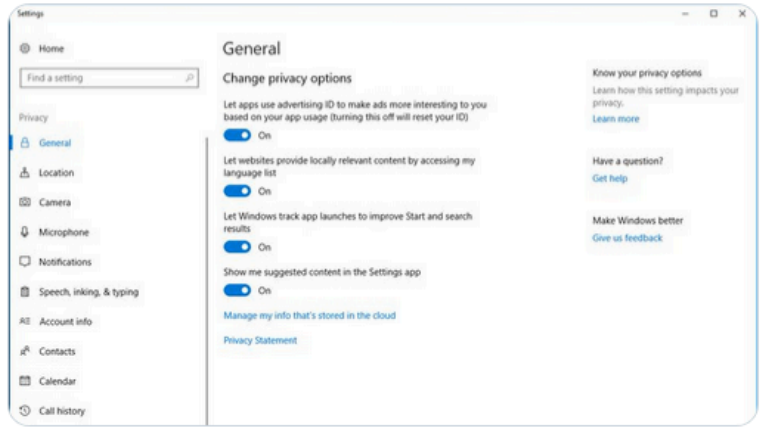
**Dylan Curran** @iamdylancurran · Mar 24, 2018
8. google.com/takeout This link includes your bookmarks, emails, contacts, your Google Drive files, all of the above information, your YouTube videos, the photos you've taken on your phone, the businesses you've bought from, the products you've bought through Google...

26 1.7K 4.9K

**Dylan Curran** @iamdylancurran · Mar 24, 2018
9. Your calendar, your Google hangout sessions, your location history, the music you listen to, the Google books you've purchased, the Google groups you're in, the websites you've created, the phones you've owned, the pages you've shared, how many steps you walk in a day...

12 1.3K 3.5K

**Dylan Curran** @iamdylancurran · Mar 24, 2018
16. Side-note, if you have Windows 10 installed, this is a picture of JUST the privacy options with 16 different sub-menus, which have all of the options enabled by default when you install Windows 10




33 1.5K 4K

**Dylan Curran** @iamdylancurran · Mar 24, 2018
17. This includes tracking where you are, what applications you have installed, when you use them, what you use them for, access to your webcam and microphone at any time, your contacts, your e-mails, your calendar, your call history, the messages you send and receive...

18 1.2K 3.1K

**Dylan Curran** @iamdylancurran · Mar 24, 2018
18. The files you download, the games you play, your photos and videos, your music, your search history, your browsing history, even what RADIO stations you listen to

11 995 2.7K

**Dylan Curran** @iamdylancurran · Mar 24, 2018
19. This is one of the craziest things about the modern age, we would never let the government or a corporation put cameras/microphones in our homes or location trackers on us, but we just went ahead and did it ourselves because fuck it I want to watch cute dog videos

87 5.7K 17K

Just to get an idea of what kind of behaviours any website can monitor:

https://clickclickclick.click
https://panopticlick.eff.org

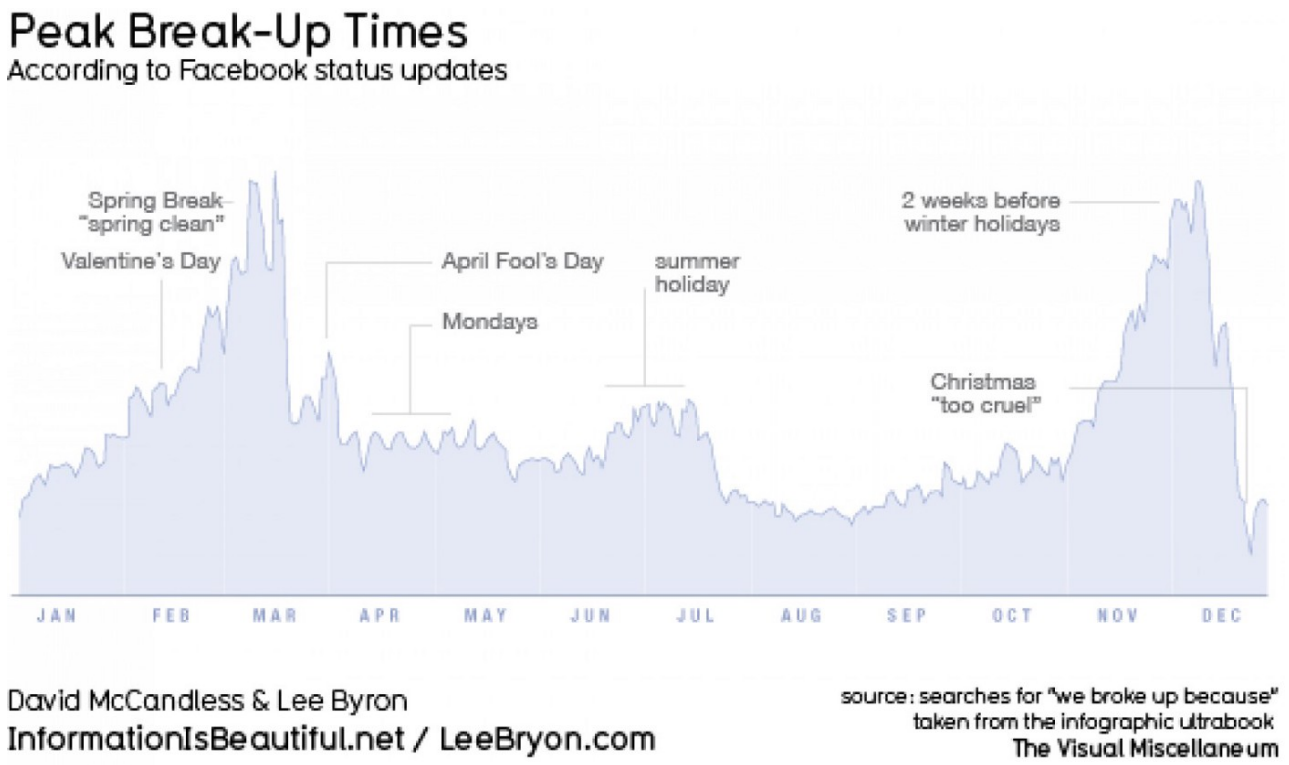
All the actions we've ever taken online,all the searches, all the clicks we've ever made, all the videos we've watched, all the likes are aggregated to build a more and more accurate model of ourselves

Those models are then used to make predictions:
Where you'll go.
What videos are likely to keep you watching.
What kind of emotions tend to trigger you.

By collecting huge amounts of online browsing data these Internet tech giants get to know us better than anyone else.
Better than our spouses.
Better than any family member.
Better than our closest friends.

# FACEBOOK RELATIONSHIP PREDICTIONS

- In 2017 Facebook's algorithms had an 80% success rate to know 2 months in advance that you are going to break up with your partner, before you even know it yourself



# GOOGLE DATA COLLECTION

- Google knows about your health issues, even very intimate ones.
- They also know infections rates (e.g. flu or SARS-CoV-2) for a region or country, a few days before doctors and health administration.

# SHOPPING PROFILING (ONLINE & OFFLINE)

- Being able to figure out pregnancy
- Weather apps that can predict shopping habits
- Amazon shipping products to you before you even purchase them because Amazon knows what you want better than you do

It’s not the data that you knowingly give these companies that’s being sold.

What they sell is the behavioural data they infer based on your interactions with their services.

If you ask for it, these companies will comply and give you your data back.

But they will not give you any of the behavioural data that they inferred.

DISCLAIMER (1):

There is no such thing as 100% security.

There is no such thing as 100% privacy online.

Need to strike the balance between privacy and convenience / usability.

# DISCLAIMER (2):

You can apply the best privacy protections possible, if your family and peers are not at the same privacy level, your privacy will suffer as a result.

The same way we do security in depth, I recommend looking at privacy in depth.

Assume that your privacy controls will fail.

Always try to have a second layer of controls.

Redundancy is the key.

# SW PRIVACY GENERAL REMARKS (1)

- After installing any piece of software (be it an OS or application), registering for a new online service or after taking any IoT device out of the box, take the time to go through the settings and check whether the defaults are appropriate privacy-wise
  - In most cases they are not
  - Do not assume that privacy settings apply equally to all (1) (2)
- Ask yourself if you really need to install an app / proprietary software
  - In most cases you can simply use a web browser
  - In general you have more control over the privacy you get by using a web browser than you do when using a proprietary app

# SW PRIVACY GENERAL REMARKS (2)

- Make use of zero-knowledge encryption whenever possible
  - The user is the only one in possession of the encryption keys
  - The cloud service is storing encrypting blobs with no (easy way) of decrypting them
- Whenever possible opt for a paid service over a “free” one
  - Provided that the paid service is providing privacy guarantees and not merely additional features
- When subscribing for a service or installing an app read the terms of service and the privacy notice
  - Not always feasible

# MOBILE APPS - PERMISSIONS

- Before installing an app check what permissions it requires
  - If several equivalent apps exist choose the one asking for the least amount of permissions
  - Ideally the need for each permission should be clearly explained
- Do not automatically grant the requested permissions
  - In most cases apps will work even without granting permissions
  - In some cases you can grant a permission one time only
- Note that you, as a user, do not have a saying about all permissions, some of them are implicit

# WEB BROWSER PRIVACY - GENERAL

- Not all browsers are created equally (at least privacy-wise)
- Use a privacy focused web browser
  - What Do Browsers Say When They Phone Home
- Enable the built-in privacy features
  - Do not track feature (note that not everyone will respect it)
- CERN Computer Security bulletin article

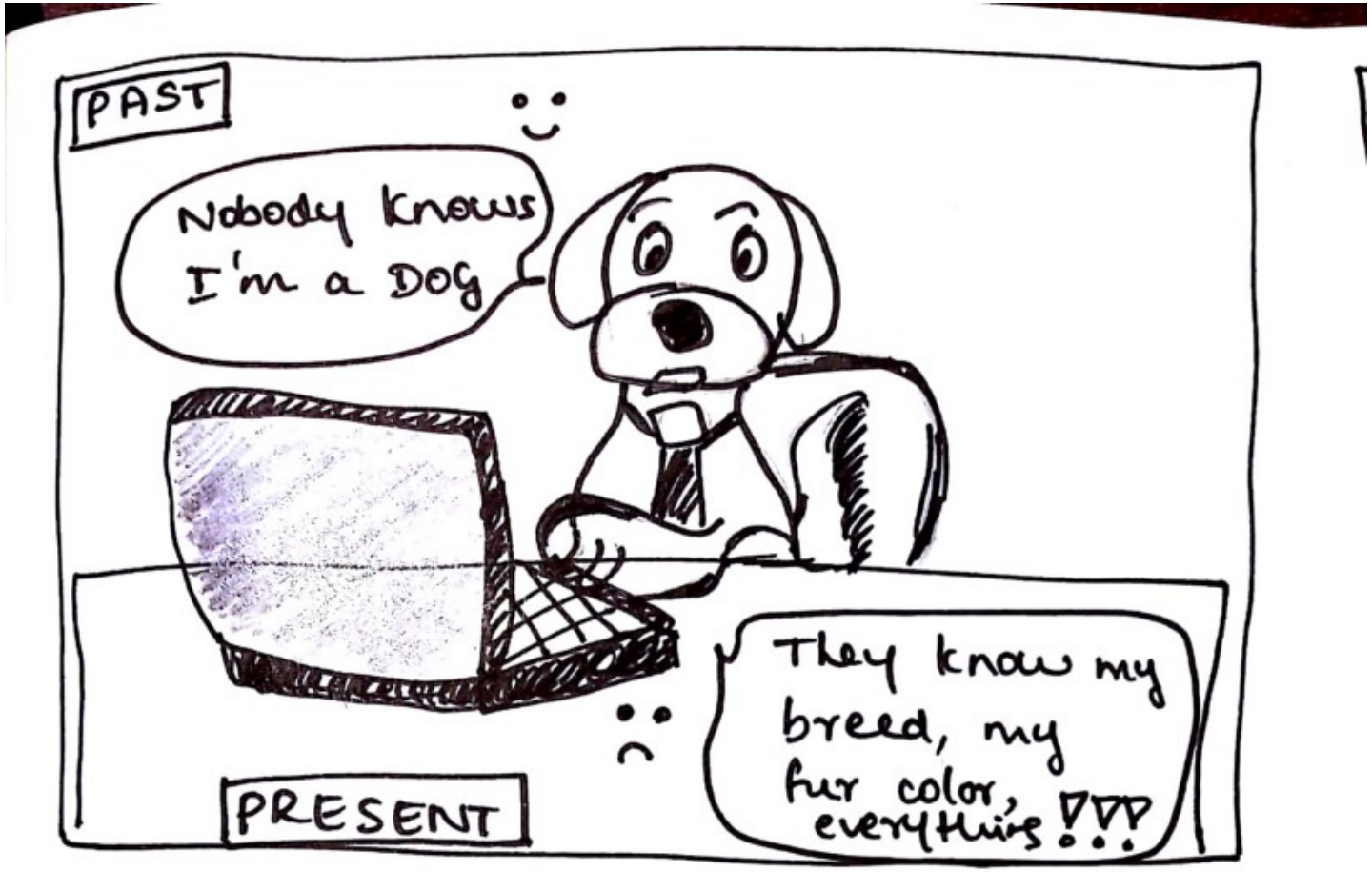
# WEB BROWSER PRIVACY - AD BLOCKERS

- Use ad blockers and extensions blocking 3rd party trackers
  - uBlock Origin
  - Privacy Badger
  - LocalCDN
  - Ghostery
  - Firefox Multi-Account Containers
- Be aware of potential security implications
  - Make sure to carefully review any extension before using it

# COOKIES

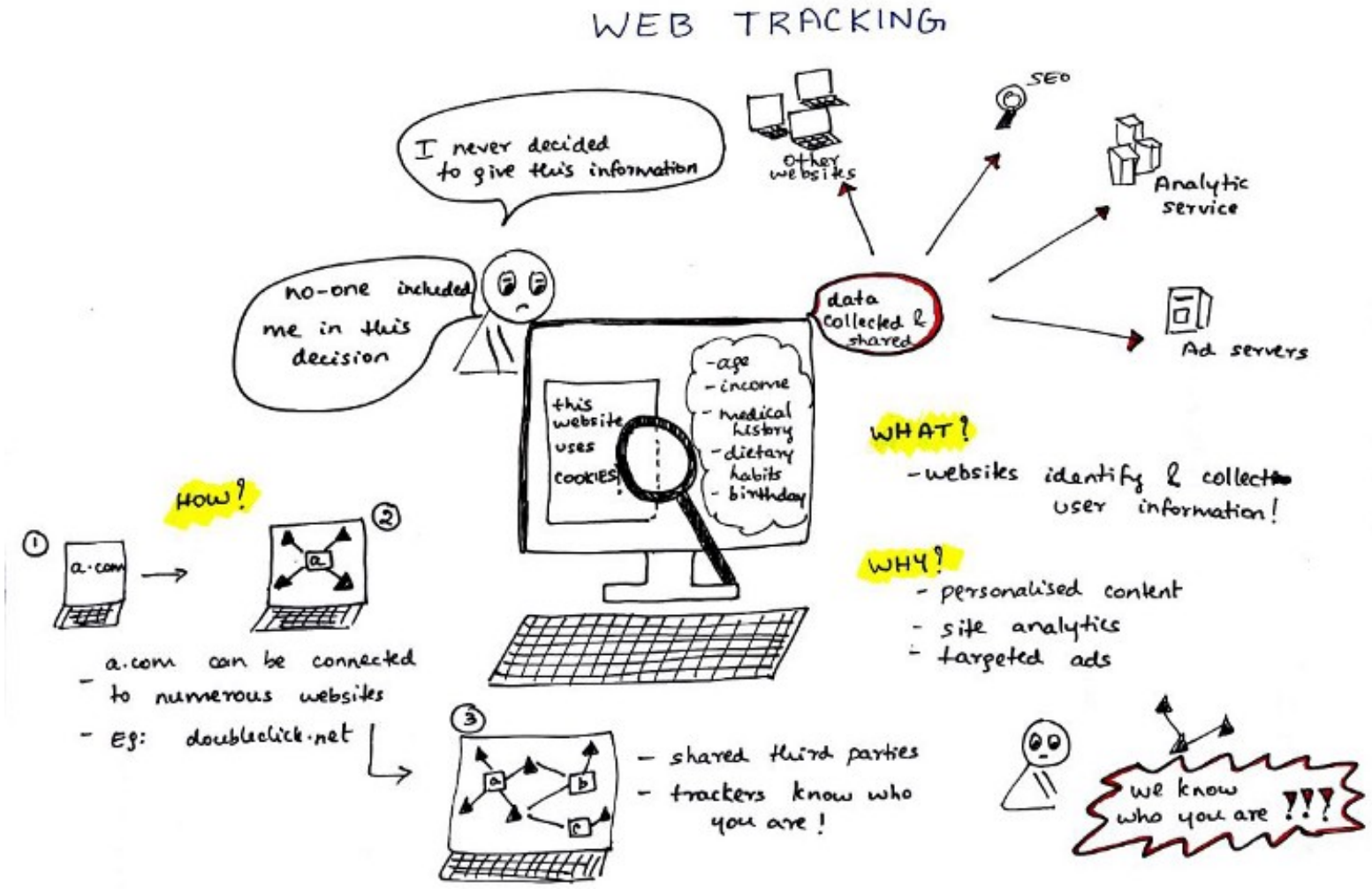
- These cloud companies are able to track you across websites via the use of (3rd party) cookies
  - Scripts or other resources that are embedded on many websites:
    - Google Analytics, Google reCAPTCHA, Facebook Like button, various social network sharing buttons
- Google and Facebook can track your every move, even if you are not logged in and even if do not have a Google or Facebook account

# 3RD PARTY COOKIE WEB TRACKING



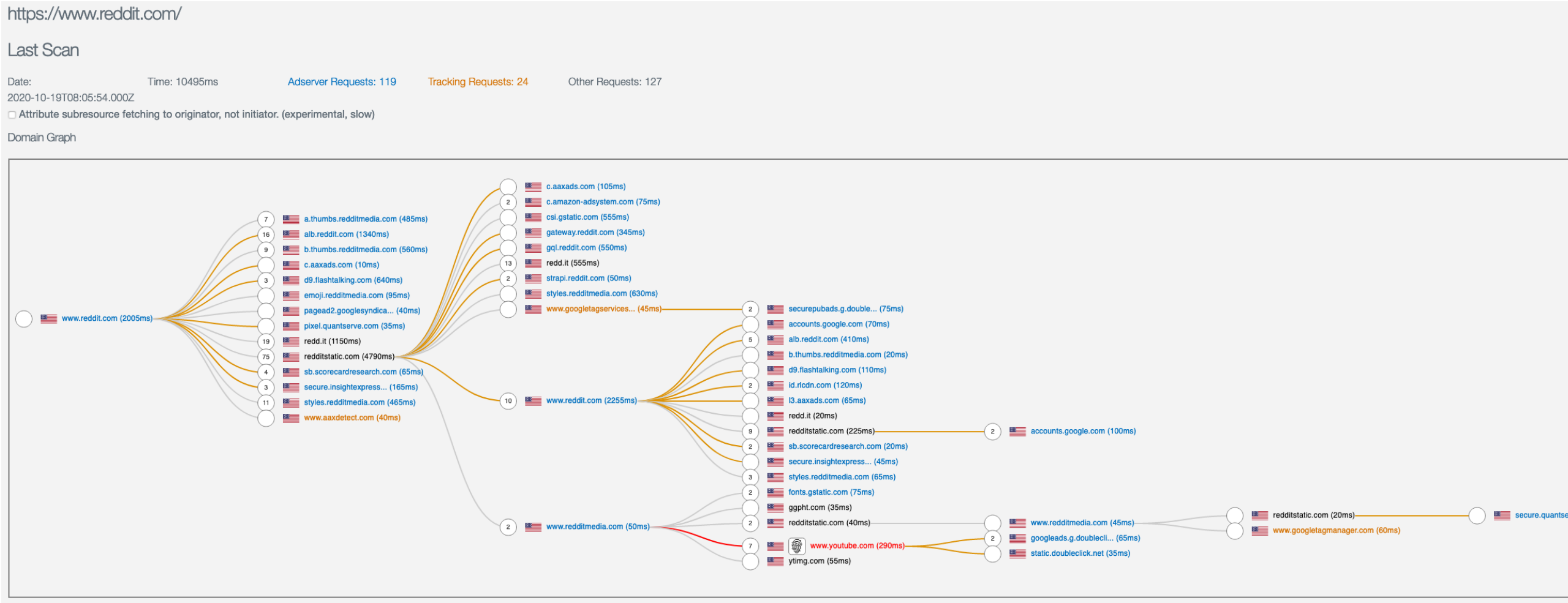

Source: https://www.freecodecamp.org/news/what-you-should-know-about-web-tracking-and-how-it-affects-your-online-privacy-42935355525/

# 3RD PARTY COOKIE WEB TRACKING




Source: https://princiya777.wordpress.com/2018/04/02/web-tracking-cartoon/

# 3RD PARTY COOKIE WEB TRACKING




Source: https://adsbydomain.fouanalytics.com/q/www.reddit.com

# RECAPTCHA (1)

- How do you think that Google knows you are not a robot when you tick that checkbox?
- You may have not noticed it, but since 2017 Google has introduced “invisible reCAPTCHAs”, CAPTCHAs that automatically disappear when a human user is detected
- Already in use on more than 4.5 M websites
- Google analyses the way users navigate through a website together with all their web activity and assigns them a risk score based on how malicious their behaviour is

# RECAPTCHA (2)

- Lower risk score when logged in to a Google account as opposed to not being logged in or using a private browser like Tor or a VPN
- To make this risk-score system work accurately, website administrators are supposed to embed reCaptcha v3 code on *all* of the pages of their website, not just on forms or log-in pages
  - Google is getting data about every single webpage you go to that is embedded with reCaptcha v3
- reCaptcha's API sends hardware and software information, including device and application data, back to Google for analysis

# SEARCH ENGINE PRIVACY

- Use a search engine that preserves your privacy, one that does not log your activity
  - DuckDuckGo
  - StartPage
  - Qwant
  - Ecosia
- Make sure to change from the default (Google) search engine on every browser / device you use

# TOR

- The Onion Router
- Good option for preserving privacy
- Comes with drawbacks:
  - Poor user experience
  - Exit nodes compromised / prone to abuse
  - Many services block access using Tor

# VPN

- May be a good option to keep your IP private
- Great if you are in control of the VPN
- Do not ever use free VPN service
  - There is no such thing as a free lunch
  - In the end they monetize you one way or another, either by selling your data or by providing an access to your device and network to whoever – see Hola VPN / Luminati SDK
- Be wary of public VPN services
  - Who do you trust more, your ISP or the VPN provider?
  - Same applies to DNS over HTTPS

# FIREWALL

- Everyone has (I hope) enabled a local firewall for incoming connections
- Use also an outgoing firewall
  - Allows you to restrict outgoing connections
- Some good options for some OSes:
  - macOS: Little Snitch
  - Android: Netguard
- Some other OSes may miss good options

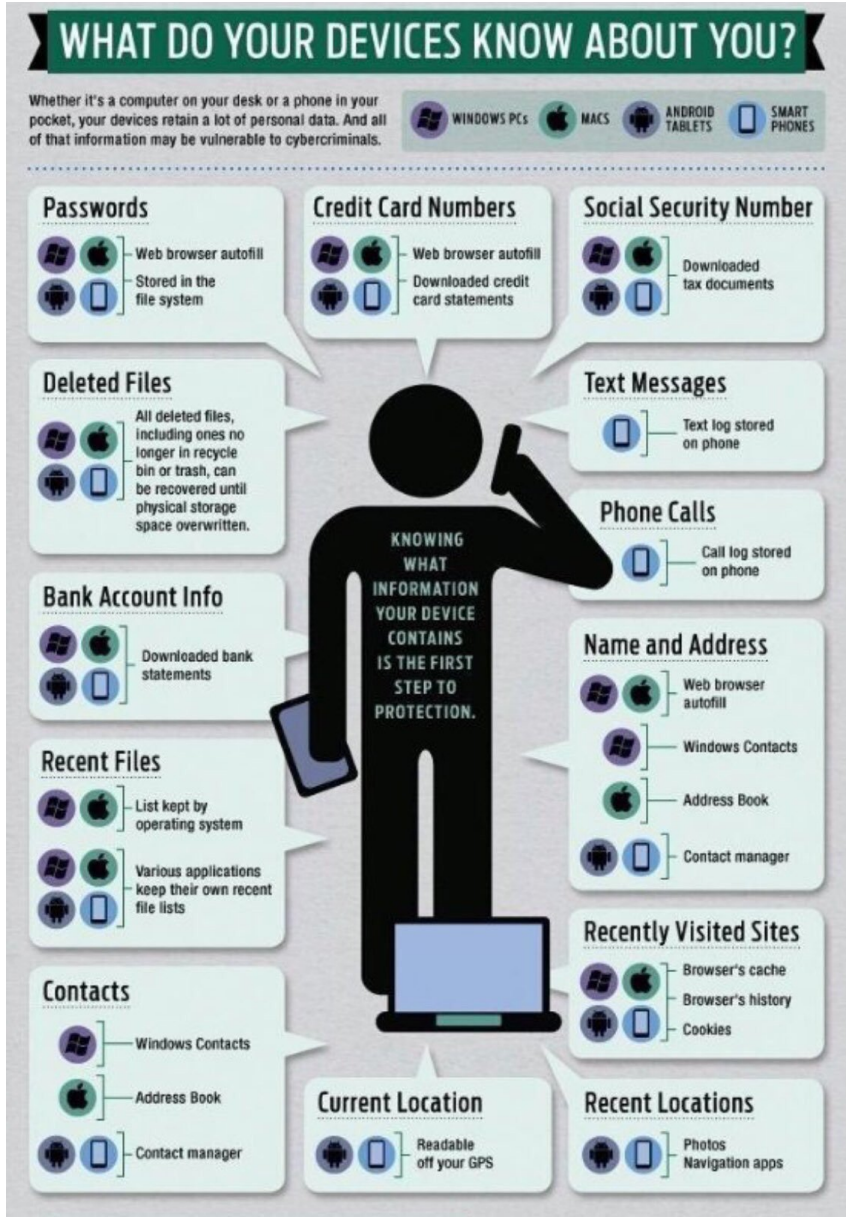
# MEDIA FILES

- Do not take or store any inappropriate, intimate or very personal pictures & videos
- Avoid showing face and more intimate parts in the same photo
  - If you really want to do that, do it the old fashioned old way using an analog camera / Polaroid and store them in a (physical) safe
- Do not ever upload anything online that you want to remain private, regardless of the cloud service used and the privacy settings you apply
  - In many cases having it on the local device also means having it into the cloud
- Do not assume that if you delete something that it will really be deleted (in most cases it will not)

# SOCIAL MEDIA

- Before you post comments or share content on support forums, social media, etc, think: are you compromising your privacy and security of a result of it?
- Sadly social media security and privacy setting can't be trusted
  - Assume that whatever you're posting on social media is / will become public, regardless of the privacy settings
  - *Same applies to what are supposed to be private conversations
- Do not use social media accounts to login to other services
  - Create individual accounts with each service you use

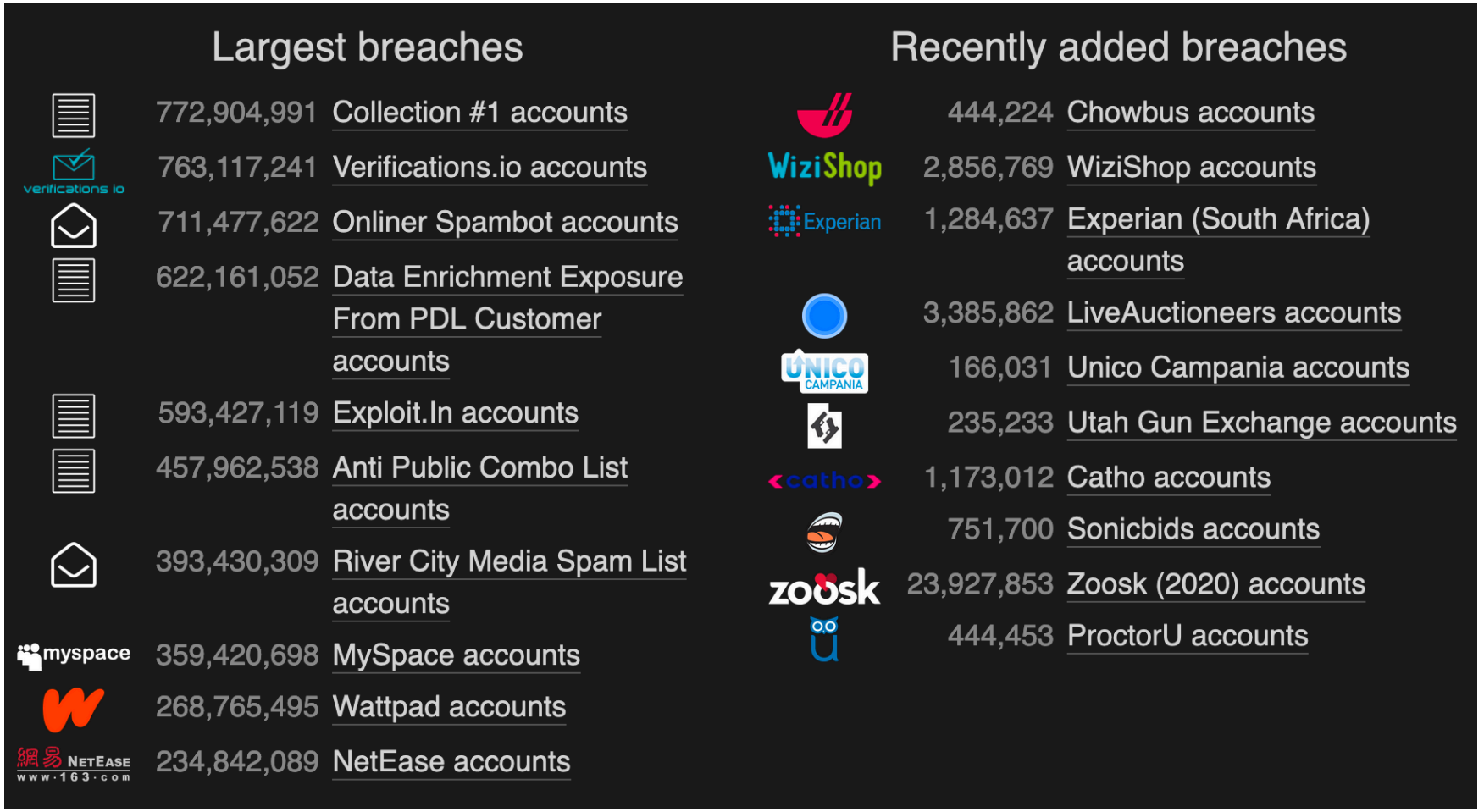
# WHAT DO YOUR DEVICES KNOW ABOUT YOU?




Source: https://twitter.com/CurtisSChin/status/858862322915446785/photo/1

In the vast majority of cases, what's on your device is in the cloud as well

# DATA BREACHES




See also the CERN Computer Security monthly reports

Source: https://haveibeenpwned.com

# COMMUNICATION TOOLS

- Favour zero-knowledge, end 2 end encrypted communication tools / protocols
  - Signal
  - Telegram
  - WhatsApp
- Beware that in many cases even though the service itself may be using end-to-end encryption, the company operating the service still has all the metadata in clear text and the backups in many cases are not encrypted, e.g. WhatsApp.

# EMAIL

- Use a paid email provider, some good options are:
  - Fastmail
  - ProtonMail
  - Hushmail
- Use a different username, email address and password for each service that you are registering for:
  - Reduces to 0 the chance of account hijacking
  - Allows you to easily determine what email / service leaked
  - Also allows to determine which service has breached your privacy

# AUTHENTICATION USING BIOMETRICS

- Very, very convenient, but should be used with care
- Biometric data should never, ever leave the device
- If they leak, they can't be changed (not easily in any case)

# CONCLUSIONS & MITIGATIONS

- Not easy to protect your privacy, these giants hold a monopoly on different services
  - Privacy preserving alternatives not always available or mature
- Think about privacy in depth
- Ironically, to be able to take some control over your data, you need to be logged in at all times
- Regulation (e.g. GDPR) can help, but cloud companies are making use of loopholes (e.g. Privacy Shield, standard contractual clauses, etc)

# CONCLUSIONS & MITIGATIONS

- As it currently stands these giants are mostly unregulated
- One possible solution could be tighter regulation and splitting them apart into smaller independent businesses, thanks to antitrust law

# FURTHER RESOURCES - ONLINE TOOLS & GUIDES

- https://securityplanner.org
- https://privacy.net/analyze
- https://whoer.net/
- https://panopticlick.eff.org/
- The Electronic Frontier Foundation's Surveillance Self-Defense Tips, Tools and How-tos for Safer Online Communications

# RESOURCES RECEIVED DURING THE TALK

- Data privacy projects with CERN involvement:
  - The Web - Take 3: Solid project
  - Collaboration between CERN developers and the Solid project
- Second International Symposium on Open Search Technology

# FURTHER RESOURCES - BOOKS

- *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* by Shoshana Zuboff
- *Permanent Record* by Edward Snowden

# FURTHER RESOURCES - DOCUMENTARIES

- *The Social Dilemma* on Netflix