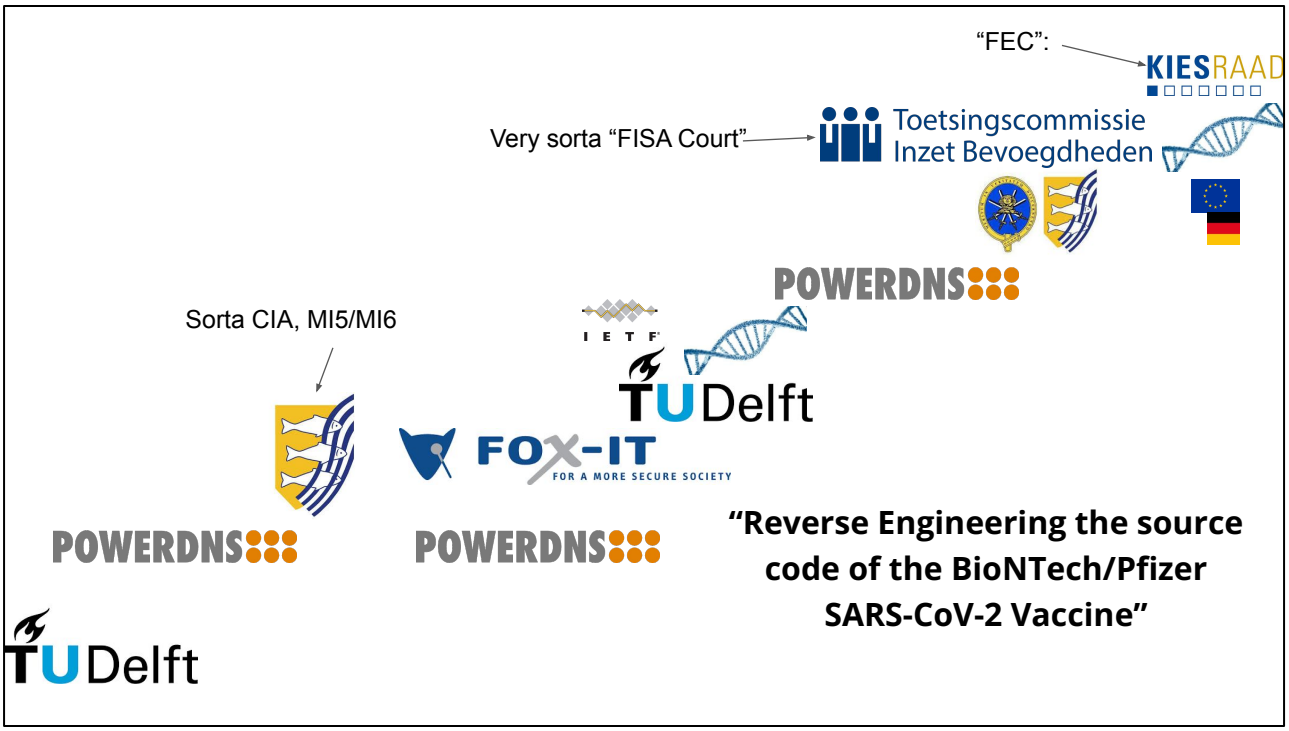
PRIVACY, CRIME, NATIONAL SECURITY, HUMAN RIGHTS: AND YOU IN THE MIDDLE

bert@hubertnet.nl / https://berthub.eu/

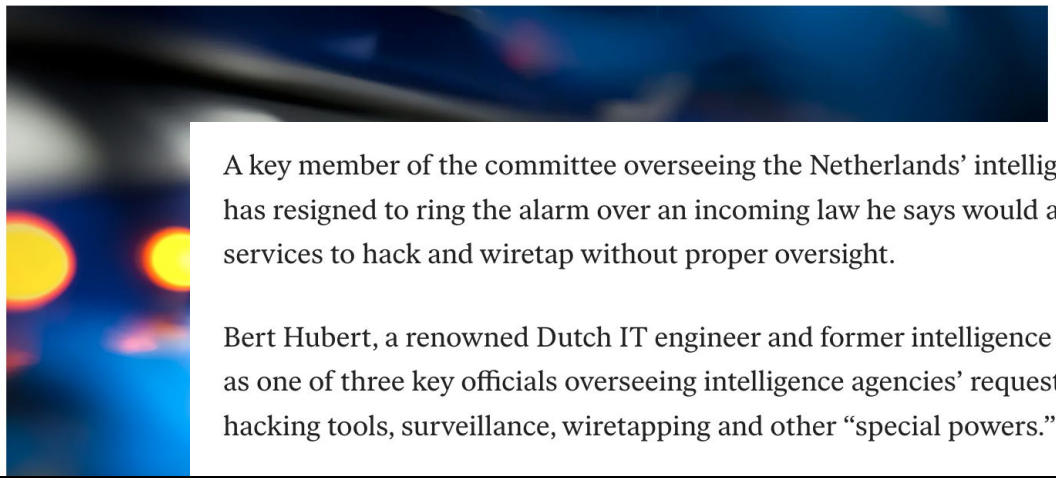


I've had a somewhat odd career so far.

This committee that regulates the Dutch intelligence and security agencies is/was unique in that it employs technical specialists at the heart of a place that in most countries only features lawyers. If you work at a department that studies policy and technology, this should warm your heart!
https://www.politico.eu/article/intelligence-watchdog-bert-hubert-netherlands-hacking-cyber-law/ has some stuff on this committee.

Intelligence watchdog resigns to blow whistle on Dutch hacking law

New law would expand powers for spooks to 'hack back' against Russia and China but cut back oversight.



A key member of the committee overseeing the Netherlands' intelligence agencies has resigned to ring the alarm over an incoming law he says would allow security services to hack and wiretap without proper oversight.

Bert Hubert, a renowned Dutch IT engineer and former intelligence official, served as one of three key officials overseeing intelligence agencies' requests to use hacking tools, surveillance, wiretapping and other "special powers."

I resigned because I thought a proposed law change was unacceptable. This made some noise and the law has still not been passed, so perhaps it helped. Or not.

I do not speak on behalf of the Dutch
(or any) government!

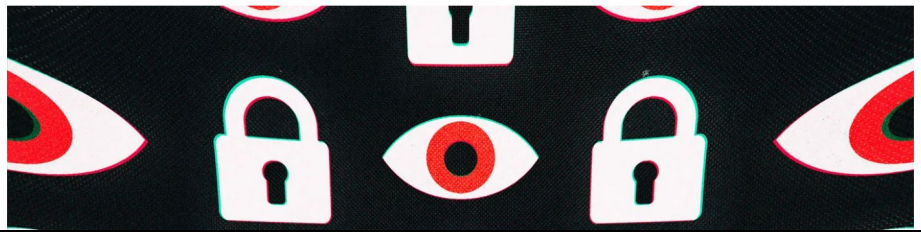
Should be clear enough!

LAW / POLICY / PRIVACY

US spy agencies are buying the same surveillance data advertisers crave / A new report from the US government says commercially collected data is as good as old-fashioned targeted surveillance.

By Wes Davis, a weekend editor who covers the latest in tech and entertainment. He has written news, reviews, and more as a tech journalist since 2020.

Jun 14, 2023, 4:51 PM GMT+2 | 8 Comments / 8 New



We worry about what government spies are collecting on us. But the private sector is not far behind.
https://www.theverge.com/2023/6/14/23759585/odni-spy-report-surveillance-data-location-tracking

Data brokers amass profiles of pregnant women – and, of course, it's all up for sale

'One common trait is that they have zero regard for the privacy of the individual'

Jessica Lyons Hardcastle

Mon 1 Aug 2022 // 22:32 UTC

Nearly three billion profiles and other pieces of data belonging to "actively pregnant" women or those "shopping for maternity products" worldwide are up for sale by US data brokers.

https://www.theregister.com/2022/08/01/pregnant_womens_data_sold/

However, selling access to a profile's location, health care, and purchase data could have more serious consequences in states like Texas, which now has a law on the books that allows any citizen who successfully sues an abortion provider, a health center worker, or anyone who helps someone access an abortion after six weeks to claim a bounty of at least $10,000.

https://www.theregister.com/2022/08/01/pregnant_womens_data_sold/ also

Who provided them with all that data?

We did

Who is responsible when technology is used for bad things?

Nuke

Nurse

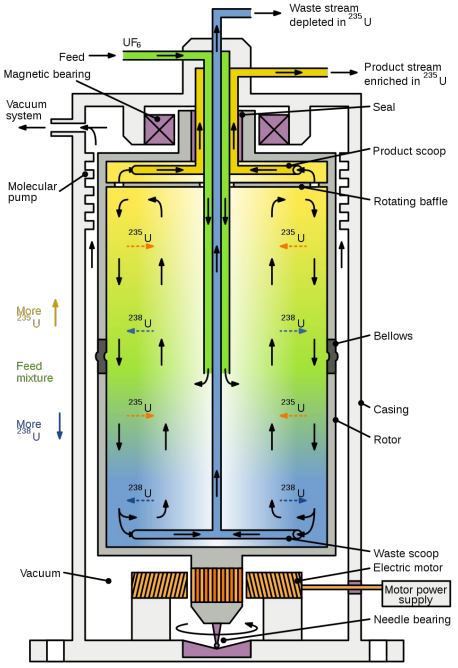
Land of Confusion, Genesis

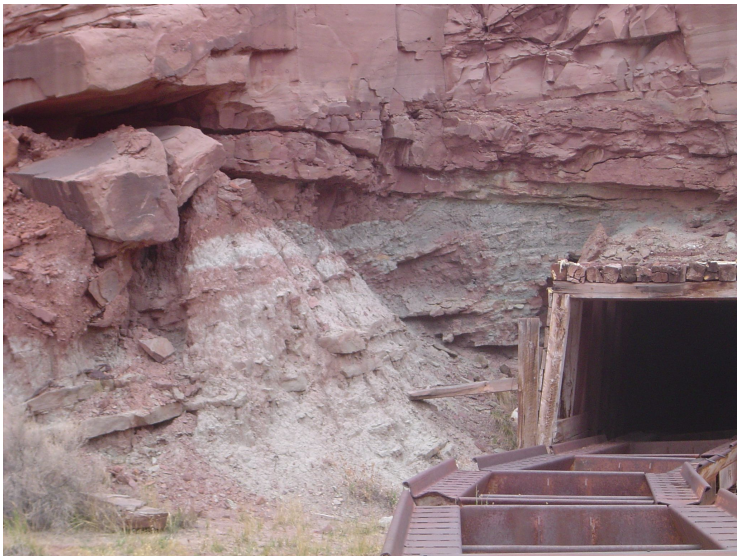
https://twitter.com/JimTomJazz/status/948418487151669248/photo/1

https://www.google.com/search?channel=fs&client=ubuntu-sn&q=war+games+key+sir#fpstate=ive&vld=cid:01893bee,vid:8-T_uhQ0iE4 - War Games, a very influential movie.

https://twitter.com/PantexPlant/status/1645577402205044739/photo/1 - the Pantex plant manufactures and maintains nuclear bombs.

We'll save your environment before launching the nukes





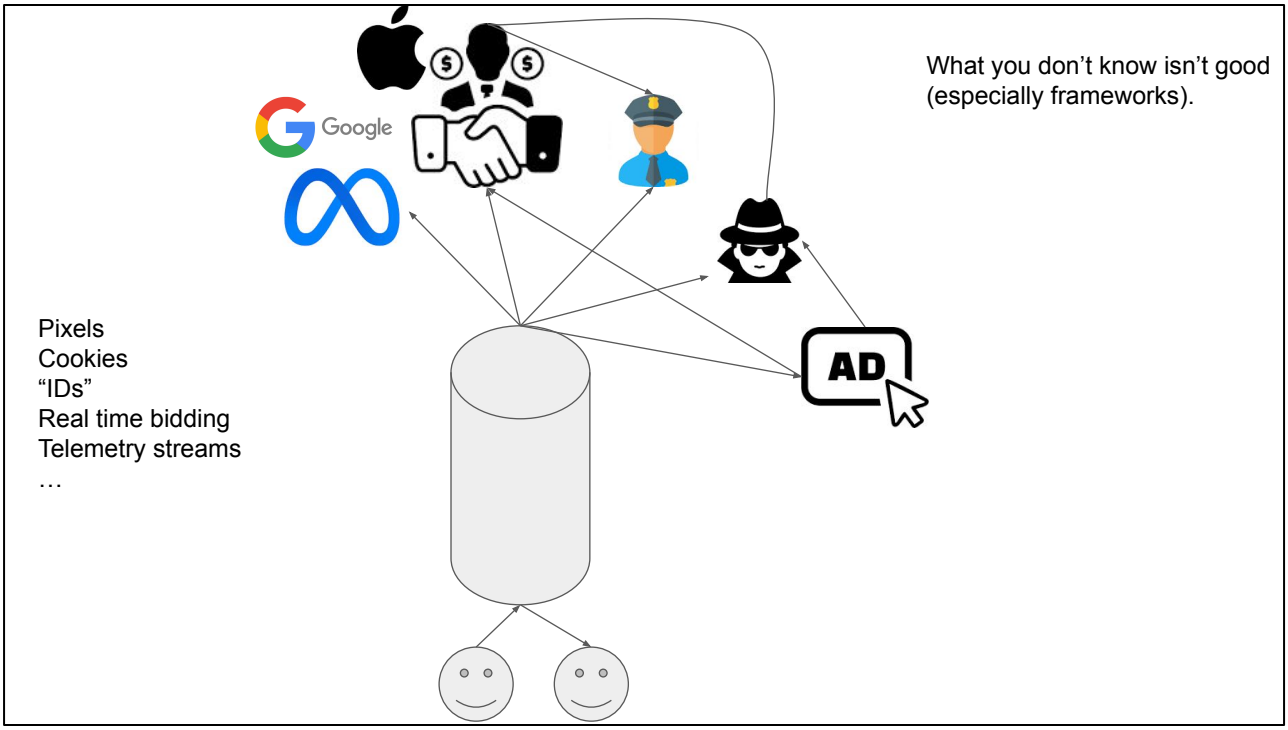
And the people that make uranium enrichment technologies, or who mine uranium? Are they responsible?

Or people that make mining equipment? Or Liese Meitner who discovered nuclear fission way way back in the day?

Data aren’t nuclear weapons, but data can cancel democracies.

"The sad truth is that most evil is done by people who never make up their minds to **be** or **do** either good or evil." - Hannah Arendt, The Life of the Mind

You can be a passive participant in setting up full surveillance society, without even knowing it.



This is how it works these days - people communicate or interact with each other, and full logs and telemetry and everything are being stored and traded between advertising companies, google, meta, apple, “data brokers”, cops, spies. Every bit of data your app logs potentially goes onto the pile one day.

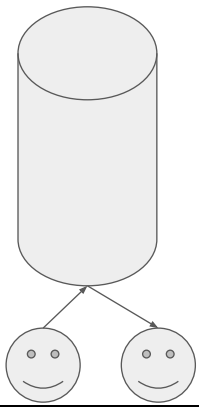
The Washington Post
Democracy Dies in Darkness

The three companies tracked the information that users typed into their tax preparation websites using pixels, a common technology utilized on almost all websites for customer ad targeting on social media. Google and Meta, Facebook's parent company, offer this tracking technology to website administrators. When users typed their information into the tax forms, the report says, pixel technology sent that data to Google and Facebook — including users' approximate annual gross income, the amount of money they received as a tax refund, whether they are married and have children, and whether they ever clicked on a long list of tax forms that would reveal more about their income and life events.

https://www.washingtonpost.com/business/2023/07/12/tax-software-data-facebook-google/

Legal situation, most Western countries

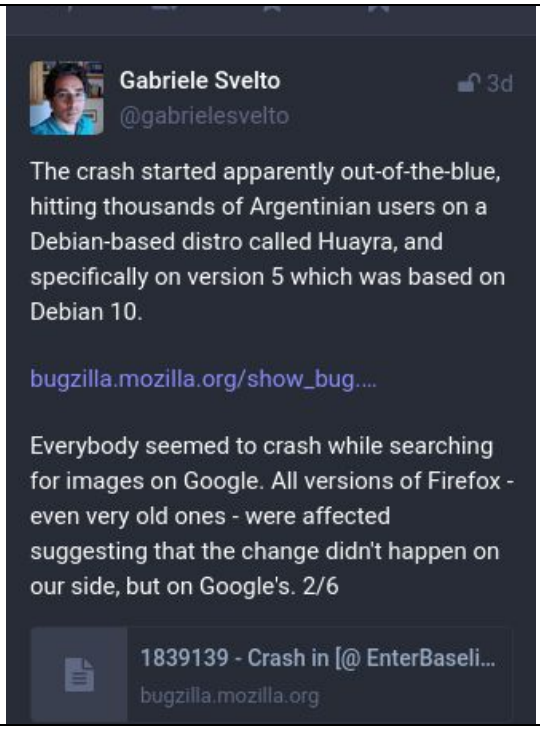
- Police, tax people, forester (!): can ask for specific information from a specific person/group. **You generally have to give what you have**.
  - Metadata/content depending on warrant
  - For specific cases (communications) you MUST make certain data available, even if you'd normally not store it
  - The more you store, the more you have to give
- Civil lawsuits: could ask for the same thing, messier
- "National security": Can ask for (access to) **bulk** data
  - "All your customers" / "all your data"
  - Can't give what you don't have / can't decrypt what you have the key for
- **NO DEVELOPER / SYSADMIN EVER SHOULD BE THE POINT OF CONTACT IT IS NOT YOUR JOB AND IT COULD HARM YOU. SEND IT UPSTAIRS ALWAYS. WAIT FOR INSTRUCTIONS.**



IMEI, IMSI, cell tower data, air pressure, walking speed, **gait**, temperature, battery status, blood pressure, pulse rate, cycling speed, ovulation details, bluetooth identifiers, paired devices, websites visited, search terms, **other apps installed**, waking/sleeping hours, which shops are visited, Wifi beacons (for within building location, or within store), typing speed, odometer data, driving speed, lane assist frequency, house layout, screen resolution, brightness, fonts installed, **versions of all hardware and software (libraries)**, various tracking IDs/advertising IDs, API keys, total usage times, languages enabled, serial numbers, storage capacity, FPS/performance figures etc.

Probably way more.

A lot of this is honest “nice to have” debugging data


Gabriele Svelto
@gabrielesvelto
3d
The crash started apparently out-of-the-blue, hitting thousands of Argentinian users on a Debian-based distro called Huayra, and specifically on version 5 which was based on Debian 10.
bugzilla.mozilla.org/show_bug....
Everybody seemed to crash while searching for images on Google. All versions of Firefox - even very old ones - were affected suggesting that the change didn't happen on our side, but on Google's. 2/6
1839139 - Crash in [@ EnterBaseli...
bugzilla.mozilla.org

Useful!


Andrej Karpathy
@karpathy
"A popular Bluetooth car battery monitor app sends GPS, cell phone tower cell IDs and Wifi beacon data to servers in Hong Kong, mainland China."
Most apps are actively adversarial to users. Need much stronger permissions protections from operating systems.
doubleagent.net
Part 1 - Discovering that your I
Reverse engineering an Andro
connected car battery monito
11:56 PM · Jun 26, 2023 · 114.6K Views
87 Retweets 7 Quotes 826 Likes 141 Bookmarl
Andrej Karpathy
@karpathy
An air quality monitor I bought earlier forced me to get an app, pair to it, create account, then requested a ton of permissions (including precise location), and refused to report air quality without. I expect many people in that position accept to just click it away. Parasitic.
11:56 PM · Jun 26, 2023 · 51.2K Views
27 Retweets 465 Likes 5 Bookmarks

Bad!

Individually innocent pieces of metadata can be combined to enable precise tracking across devices and IDs.

Board, shareholders, interests

Director

Product Manager

Project Manager

You

“I only type it in, I just do what I’m told”

Board, shareholders, interests

Director

Product Manager

Project Manager

You

Every layer fills in a lot. That is the freedom you have in your layer.

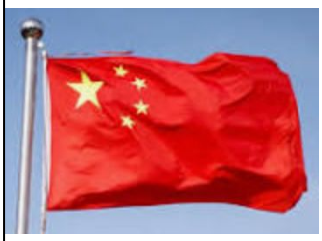
- What your app has no **PERMISSION** to see, you can't **collect**
- What you don't **collect**, you can't **transmit**
- What you don't **transmit** can not be **stored**
- What is not **stored** can't be **sold or leaked**
- (What is quickly rotated is at least protected somewhat)

Many of these things
are choices **YOU**
make, often without
anyone asking you to.

Simply by choosing conservative defaults, you can avoid a lot of pain later on. **Do not log “*”**.

Everything you collect, transmit, store, log is up for interception, analysis, sale.. And leaking.

Cyber
Resilience Act



"We are here"

"consumer connectable product security regime"

(a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state;

(b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;

(c) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms;

(d) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;

(e) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');

(f) protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;

GDPR but now for your device DESIGN

Soon EU regulations may forbid your app from collecting data not required for the functioning of the app.

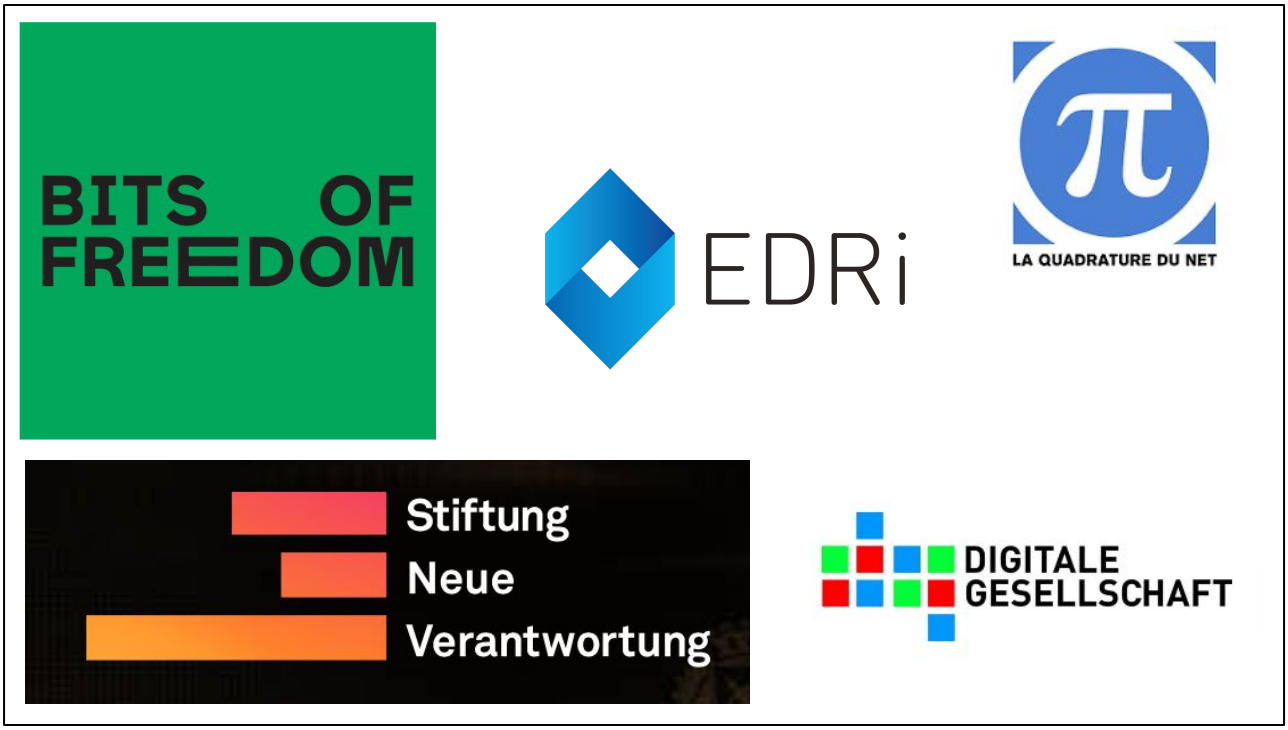
The balance

- People will use your stuff while committing crimes
- The data you have could be useful to fight crime
  - For banks, storing absolutely everything is mandatory
  - Classic telecommunication companies similar
- You can make your data protection SO GOOD that you will be unable to supply anything useful to law enforcement
  - Signal
- Apple achieved this at some point
- Sets you up for some HARSH CHOICES
  - “A child was abducted and you can’t help us”

The balance

- Your product/thing is not created to help law enforcement
- But you also don't want to be of active help for criminals & bad people
- Data that you leak can be helpful for "a more secure society"
- Data that you HAVE can also be sold to target vulnerable people
  - And this is already happening
- Most (very large) companies come to some kind of understanding eventually where this balance lies
  - .. unencrypted backups ..
  - …
- **Large companies can not resist governments when asked for data that they have**

As techies, we are not well equipped to think about the harm data can cause.



These are some sample organizations that think a lot about these problems, and hold interesting presentations and events. Go visit them!

Final notes & what to do

- Living in a safe society is nice, caricatures that law enforcement never needs data are plain wrong
  - Think hard before creating a darkweb store!
- However, handing out too much data is bad, even to governments
  - Handing out data to “databrokers” and unclear processors is worse
- By limiting how much data you (can) collect, transmit, store, process, a reasonable balance can be kept
- What isn’t there can’t leak
- Nice to have data: how nice is it really?
  - Also may be illegal
  - When in doubt, do not log.
- Educate yourself so you know who is at risk of your data leaking or not being available

PRIVACY, CRIME, NATIONAL SECURITY, HUMAN RIGHTS: AND YOU IN THE MIDDLE

You have a real role to play. Please play it well!

bert@hubertnet.nl / https://berthub.eu/