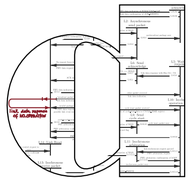
Ethics for Nerds

An Advanced Course in Computer Science
Summer Semester 2020

Contemporary Topics C4.1
Privacy

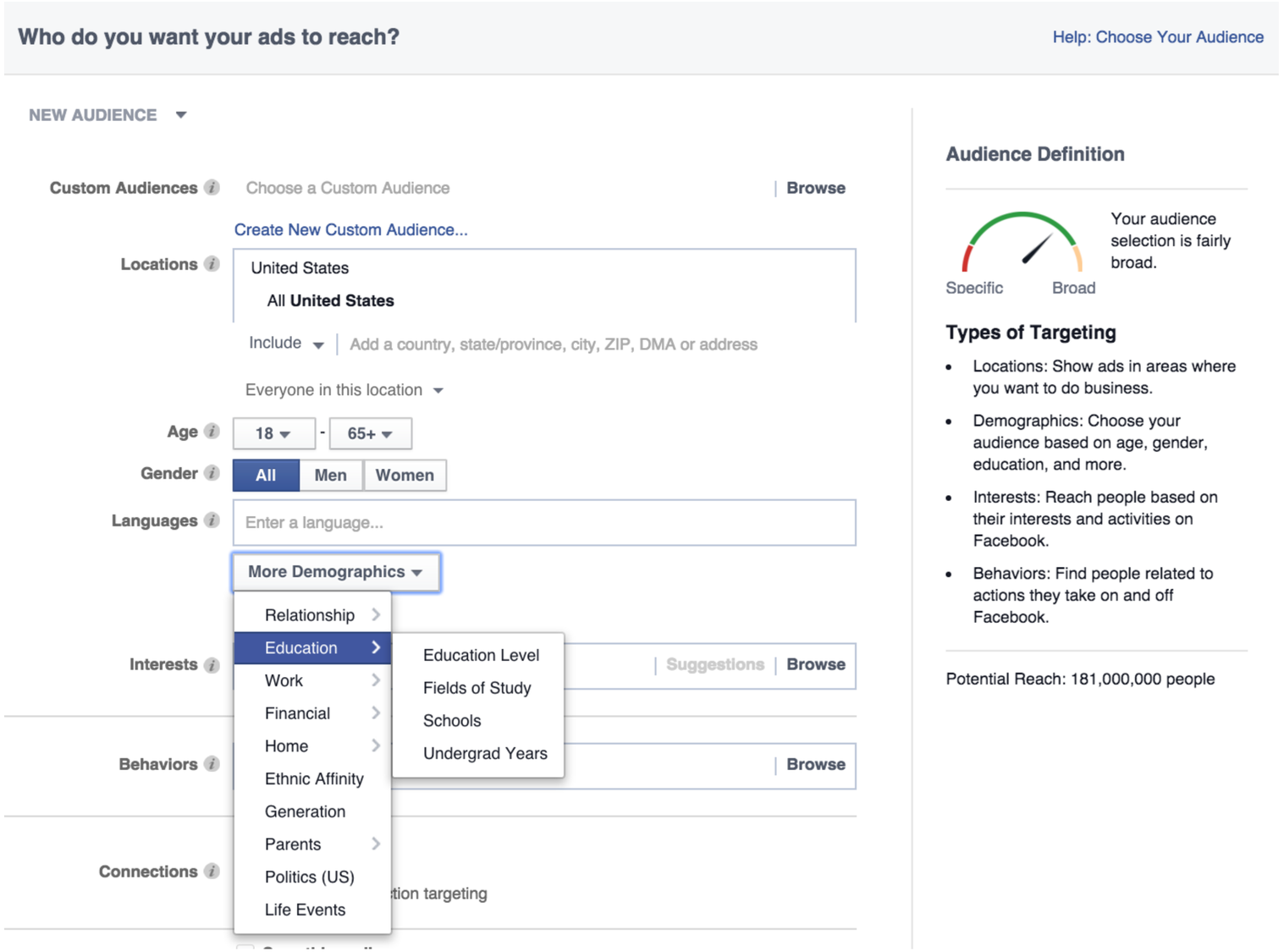
Privacy Violations and Privacy Threats



Prof. Holger Hermanns,
Kevin Baum, Sarah Sterz

UNIVERSITÄT
DES
SAARLANDES

MOTIVATION



https://www.stealthseminar.com/boost-webinar-registrations-facebook-ads

PRIVACY IS PRO TANTO GOOD

Some plausible claims about privacy and security (in the sense of public security):

- privacy and security are (somehow) valuable and
- violations/threats of privacy and/or security are *pro tanto* bad.

important term	intuition	sometimes used as opposite
pro tanto	can be outweighed/defeated by something else	all things considered
prima facie	at first sight	
other things being equal/ceteris paribus	something like “all other aspects are hold constant”, “other things being normal”, “as in the other case”, “if everything happens as expected” (also used as “don’t act like an idiot by adding unnecessary details to my thought experiment”)	

PRIVACY AND ANONYMITY

privacy

not being observed or tracked
(very roughly)

≠

anonymity

not being identified
(very roughly)

	anonymous	not anonymous
private	you are **both private and anonymous** when you hike alone and unobserved in an empty forest and nobody knows where you are	Merkel and Trump are **private, but not anonymous** when they have a talk in a back room with some people outside
not private	someone is **anonymous, but not private** if they are captured by a hidden camera in a dressing room that does not record any of their identifying features and nobody there knows who you are	you are **neither anonymous nor private** when posts your personal diary online along with your name and address

PRIVACY VIOLATION VS PRIVACY THREAT

privacy violating technologies

technologies that observe or track you
(very roughly)

$\subsetneq$

privacy threatening technologies

technologies that *can* observe or track you
(very roughly)

$\cap$ $\cap$

$\cap$ $\cap$

anonymity violating technologies

technologies that identify you or link identifiers of yours
(very roughly)

$\subsetneq$

anonymity threatening technologies

technologies that *can* identify you or link identifiers of yours
(very roughly)

PRIVACY IS PRO TANTO GOOD

Why a violation/threat of privacy is only *pro tanto* bad

CCTV in Public and Semi-Public Areas

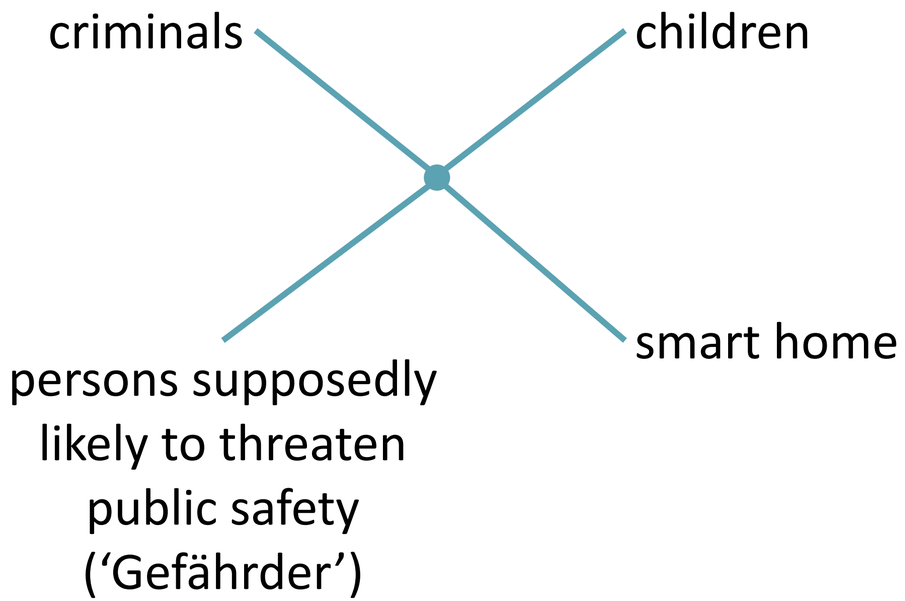
https://commons.wikimedia.org/wiki/File:HK_WTS_%E6%A8%82%E5%AF%8C%E5%BB%A3%E5%A0%B4_Lok_Fu_Plaza_mall_interior_CCTV_escalators_visitors_May-2013.JPG

http://timesofindia.indiatimes.com/photo/48478046.cms

https://www.flickr.com/photos/lydiashiningbrightly/4465608392

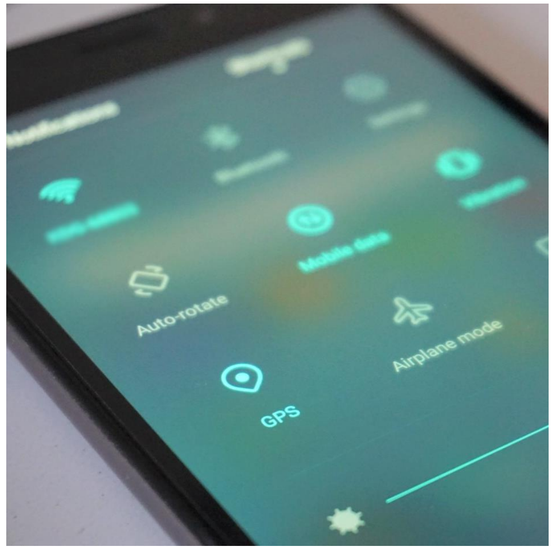
PRIVACY THREATENING TECHNOLOGY

GPS and Geofencing



https://en.wikipedia.org/wiki/File:Bracelet_%C3%A9lectronique.JPG

http://www.giftsandfreeadvice.com/free_advice/wp-content/uploads/2009/03/gpsimplant.jpg



https://www.weenect.com/shop-weenect-kids.html

(Telecommunications) Data Retention

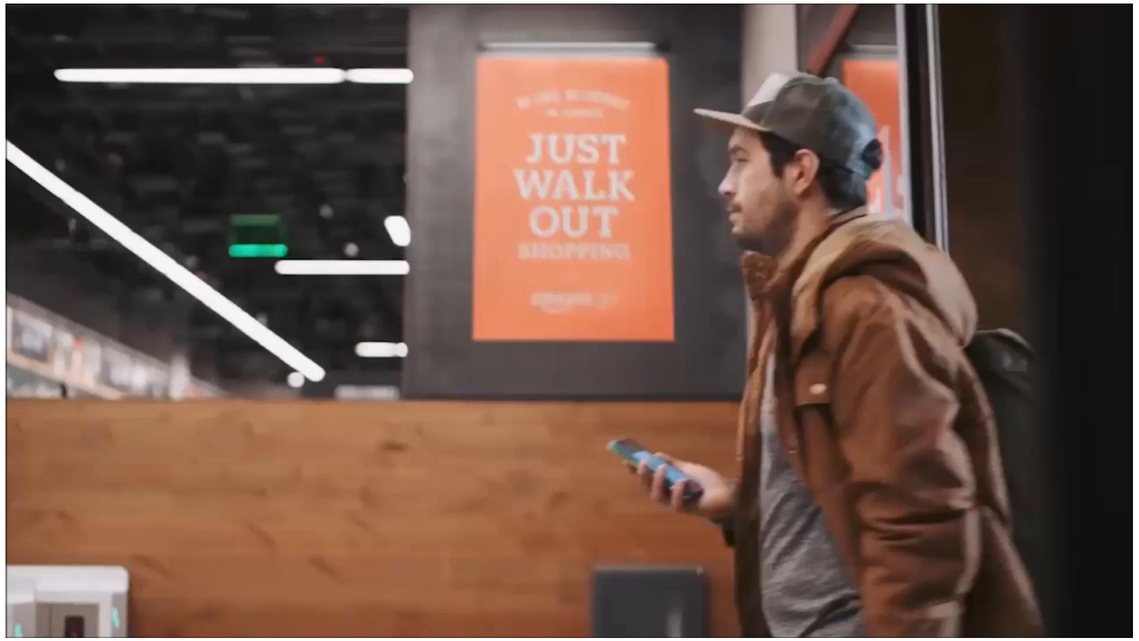
https://c1.staticflickr.com/2/1199/1424664967_2df8004538.jpg

https://de.wikipedia.org/wiki/Datei:Vorratsdatenspeicherung_Kritik_02.jpg

Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG

PRIVACY THREATENING TECHNOLOGY

Amazon



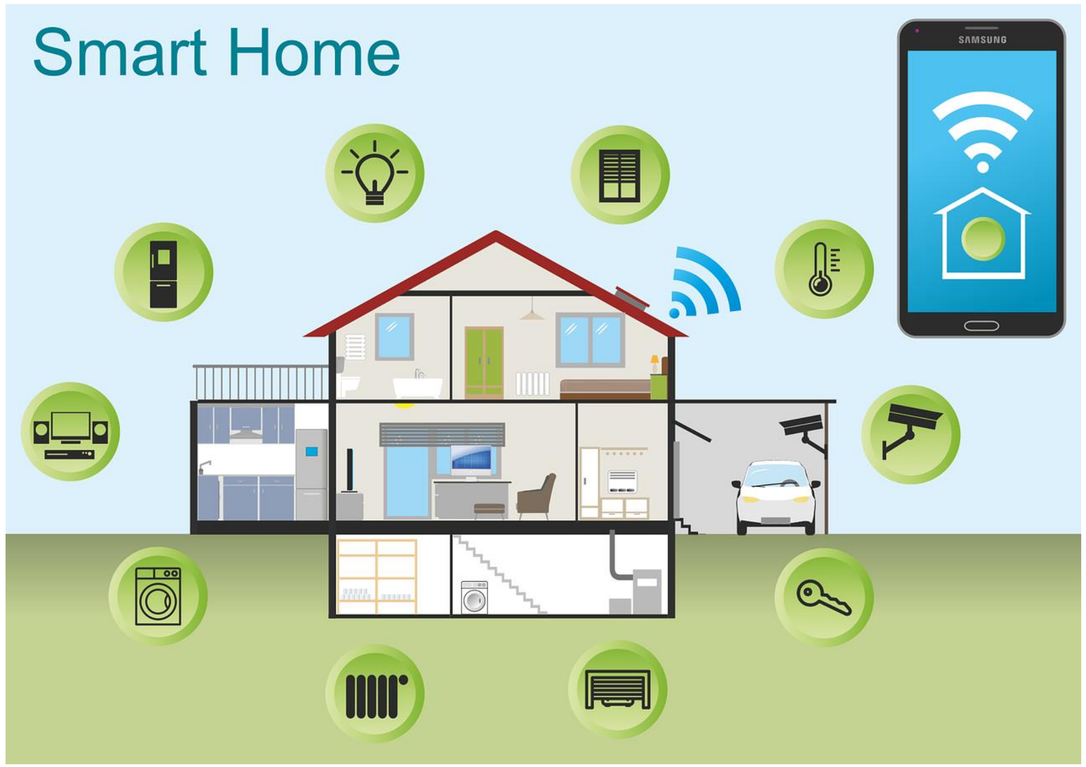
https://www.youtube.com/watch?v=NrmMk1Myrxc

https://vimeo.com/80777503

amazon.com

PRIVACY THREATENING TECHNOLOGY

Smart Home

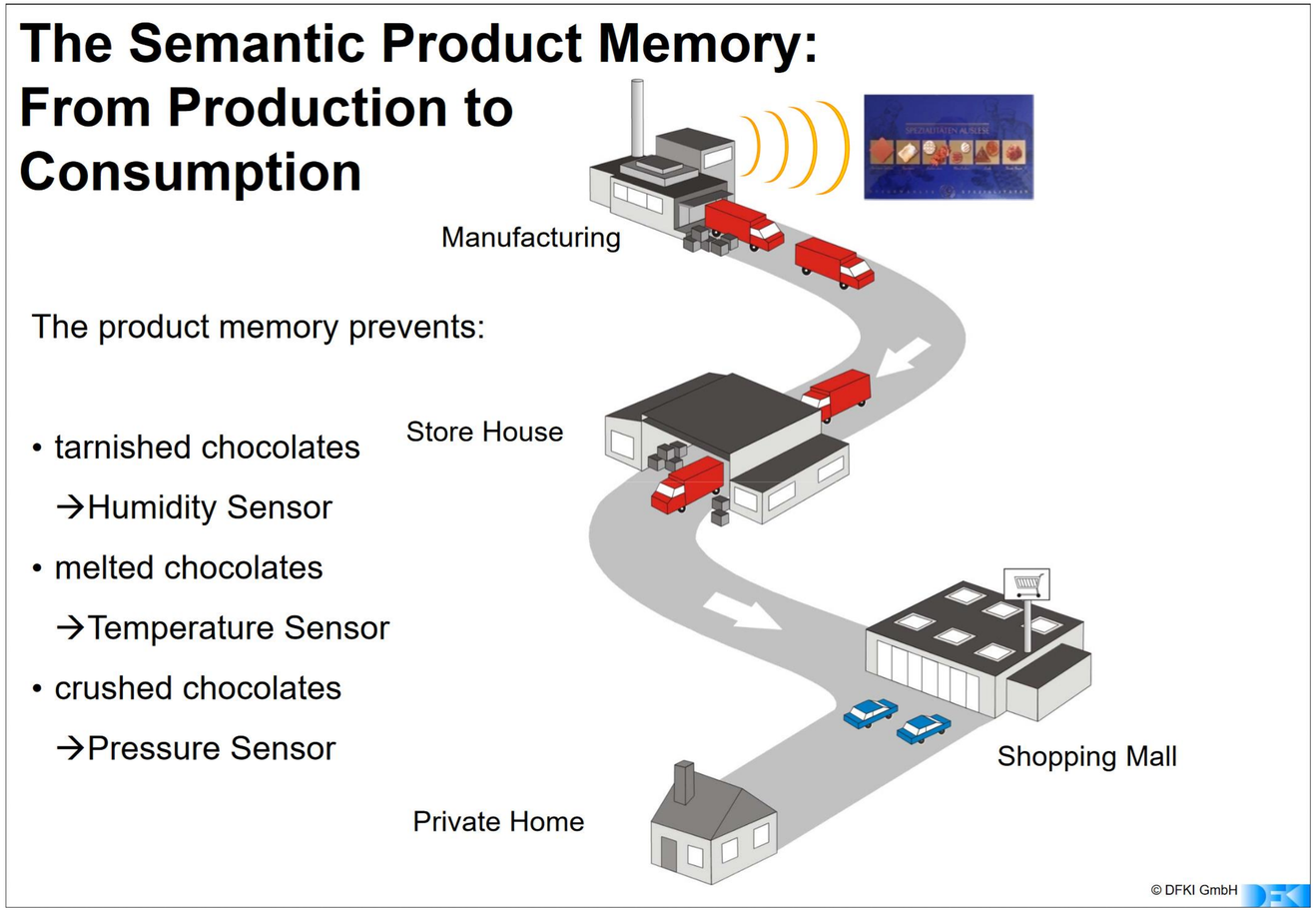


Fitness Tracker

Smart Speakers

https://www.techhive.com/article/3252155/best-smart-speakers.html

Semantic Product Memory



from Semantic Product Memories: Digital Lifelogs for Smart Products by Wolfgang Wahlster:
http://ki2009.uni-paderborn.de/fileadmin/ki2009/documents/keynotes/KI-2009_Keynote_Wahlster.pdf

PRIVACY THREATENING TECHNOLOGY

It’s not over yet, the list goes on and on and on…

- browser histories
- web cookies
- unencrypted email and messenger communication
- personalized ads
- social networks
- almost every Google/Microsoft/Apple product
- smart watches
- smartphones
- smart speakers like Amazon Echo
- RFID chips in passports
- your Netflix history
- smart TV systems
- smart toys
- Bluetooth beacons
- public Wi-Fi
- biometric recognition
- your Amazon data
- e-readers
- …

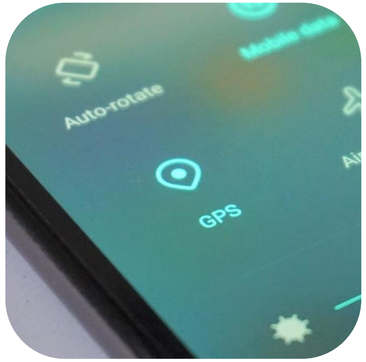
And now combine this…

You are shopping and your smartwatch asks you, if you really want to buy chocolate now, since you did not do your daily workout yet. It says, you rather should buy some lattice, since the one you have in your fridge looks moldy. And by the way, the fertilizer for your house plant came! You ordered it because your smart home measured, that the plant isn't really well. The Amazon drone dropped it on your balcony. You pick up the chocolate anyway, but your phone warns you, that it might be broken, so pick up another one. Your fridge alarms you that, while you are at it, you could bring some milk, since the milk you have expires tomorrow. On your way home, your phone turns on the heater for you. While you are putting the groceries away, your smartwatch praises you for buying lattice, but reminds you, that your workout is still due. And it has been adapted – you are informed that you are now capable of doing ten pushups more! Your fridge notices, that you did not bring milk and asks you, if it should order some for you…

How do you like this scenario?

PRIVACY THREATENING TECHNOLOGY

https://www.flickr.com/photos/lydiashiningbrightly/4465608392



https://c1.staticflickr.com/2/1199/1424664967_2df8004538.jpg

https://vimeo.com/80777503

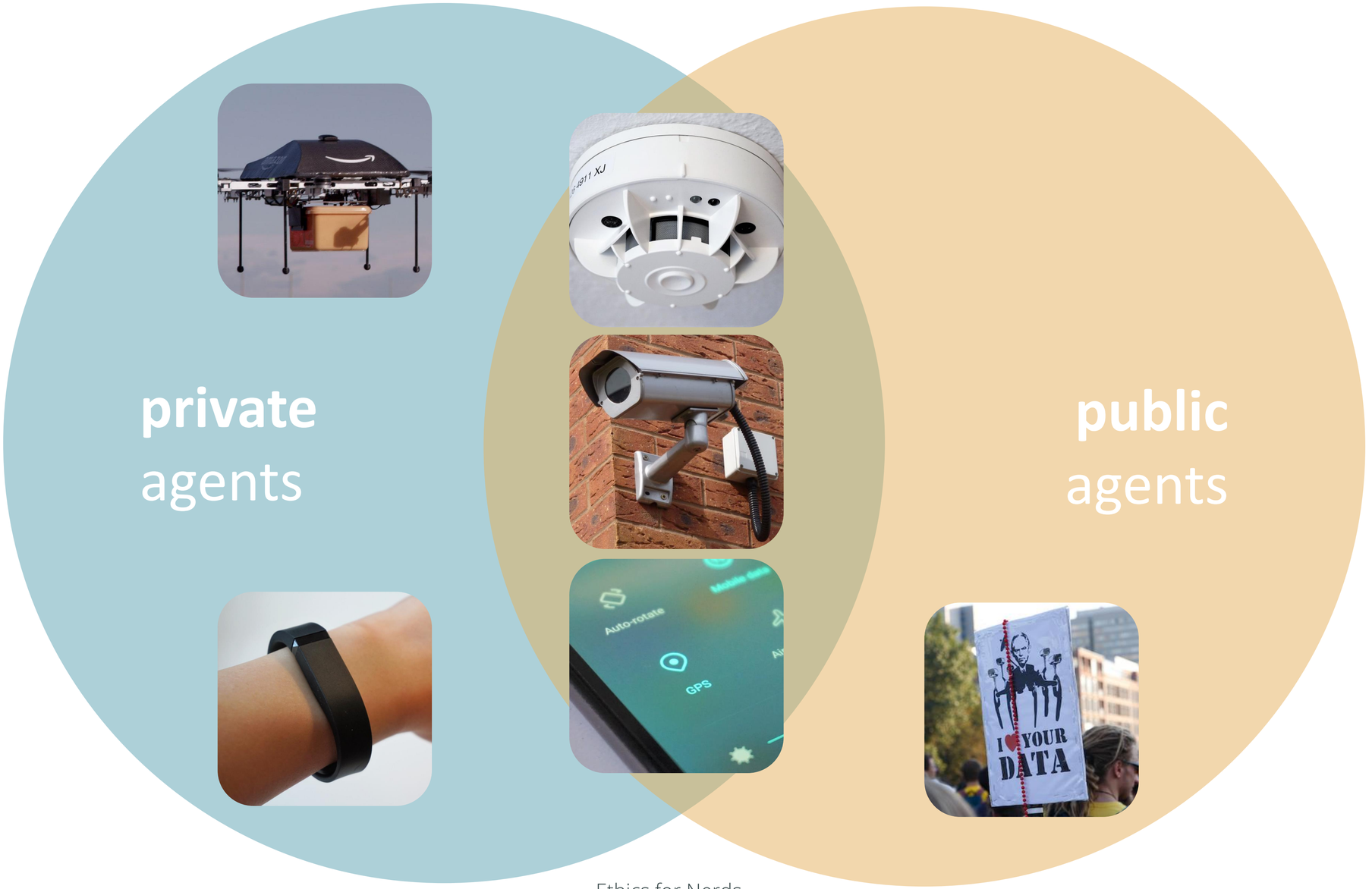
who provides privacy threatening technologies

why we allow privacy threats

what choice we have to use those technologies (currently)

PRIVACY THREATENING TECHNOLOGY

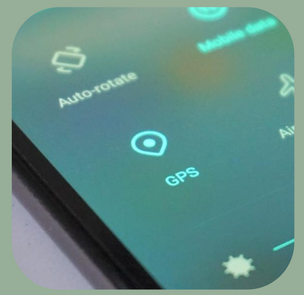
Who provides privacy threatening technologies



Why we allow privacy threats

motivation from **security**

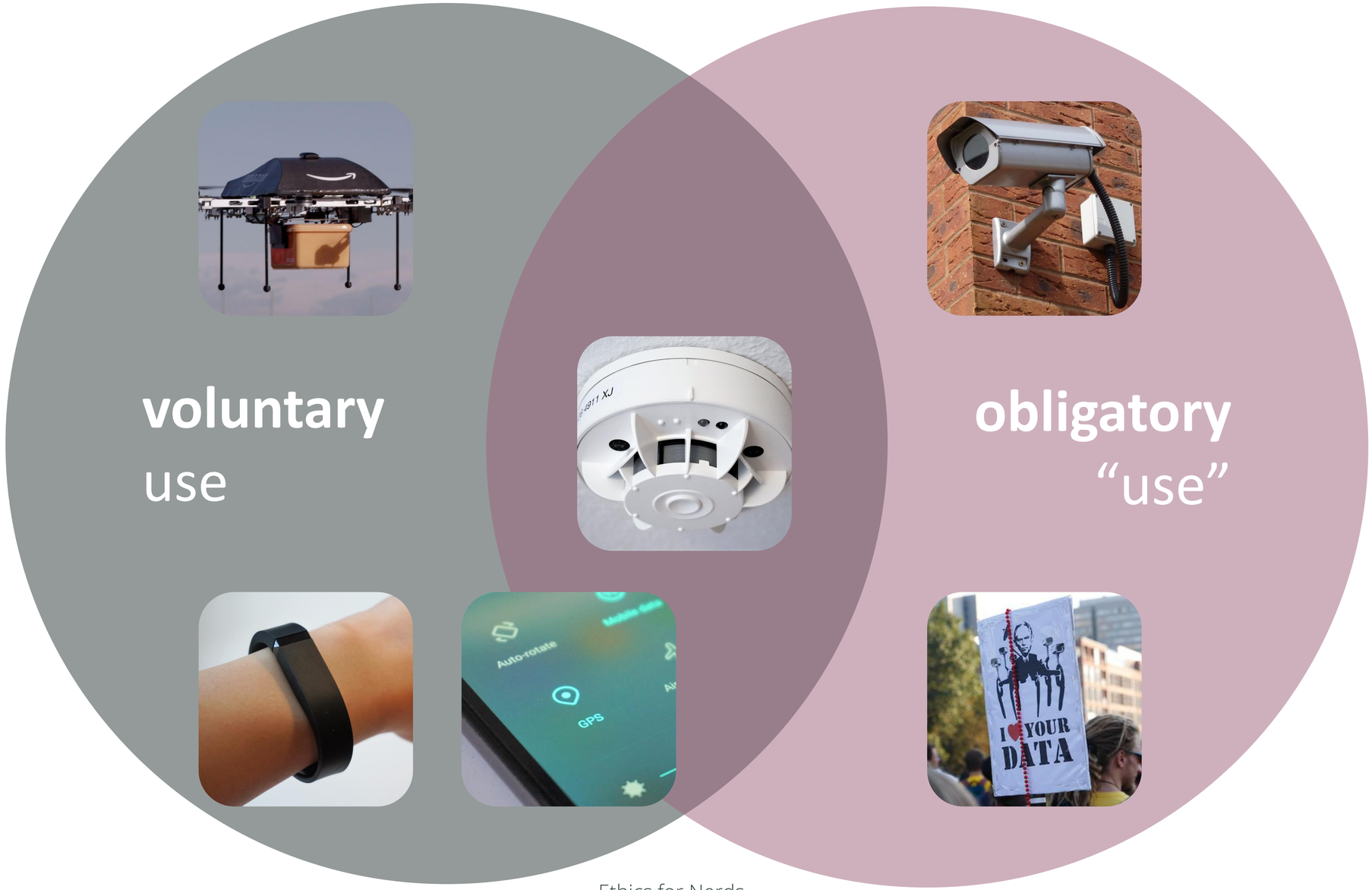
(or more malicious motivations like caving for power)



motivation from **convenience**, **indifference** etc.

PRIVACY THREATENING TECHNOLOGY

What choice we have to use those technologies (currently)

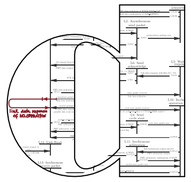


Ethics for Nerds

An Advanced Course in Computer Science
Summer Semester 2020

Contemporary Topics C4.1
Privacy

Actionable Advice



Prof. Holger Hermanns,
Kevin Baum, Sarah Sterz

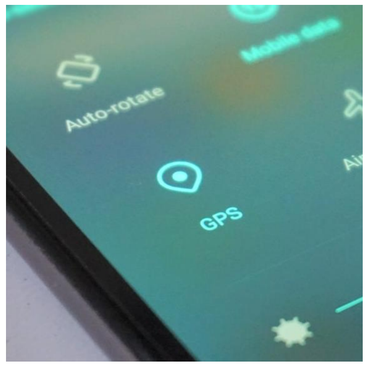
UNIVERSITÄT
DES
SAARLANDES

ONE PROBLEM

privacy violating technologies $\subsetneq$ privacy threatening technologies

How to distinguish this from this in an individual case where you lack information?

https://www.flickr.com/photos/lydiashiningbrightly/4465608392



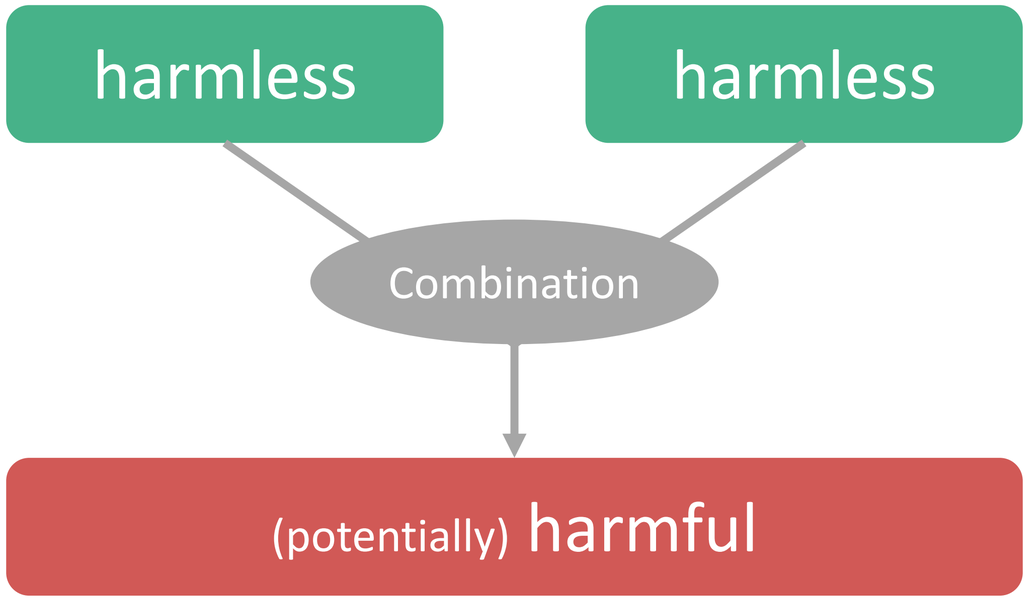
https://c1.staticflickr.com/2/1199/1424664967_2df8004538.jpg

https://vimeo.com/80777503

ANOTHER PROBLEM

The Combination-Problem

It’s possible that:

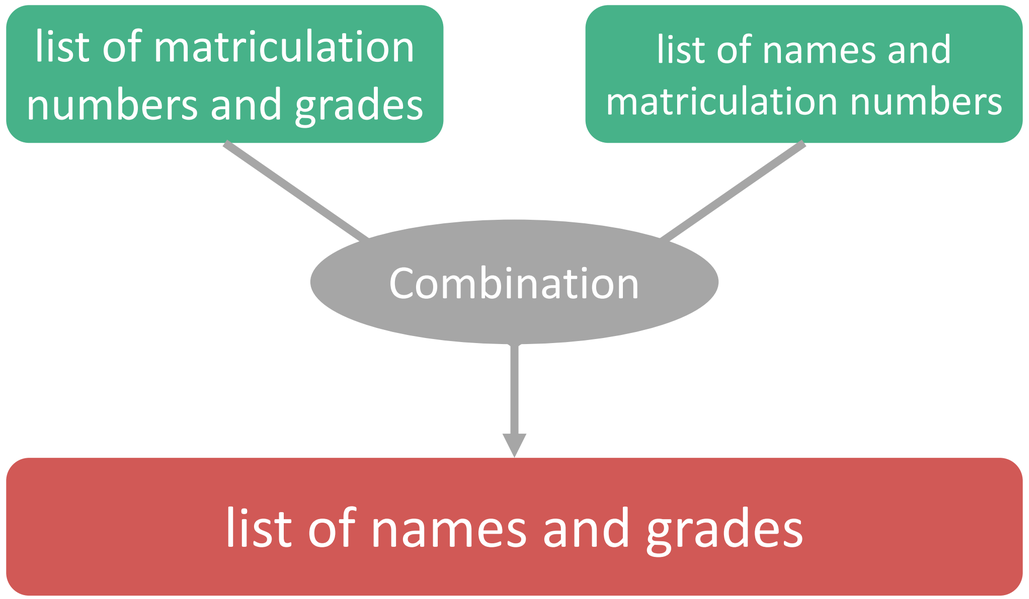


Lots of small harmless pieces

can make a harmful whole

The Combination-Problem (Example 1)

It’s possible that:

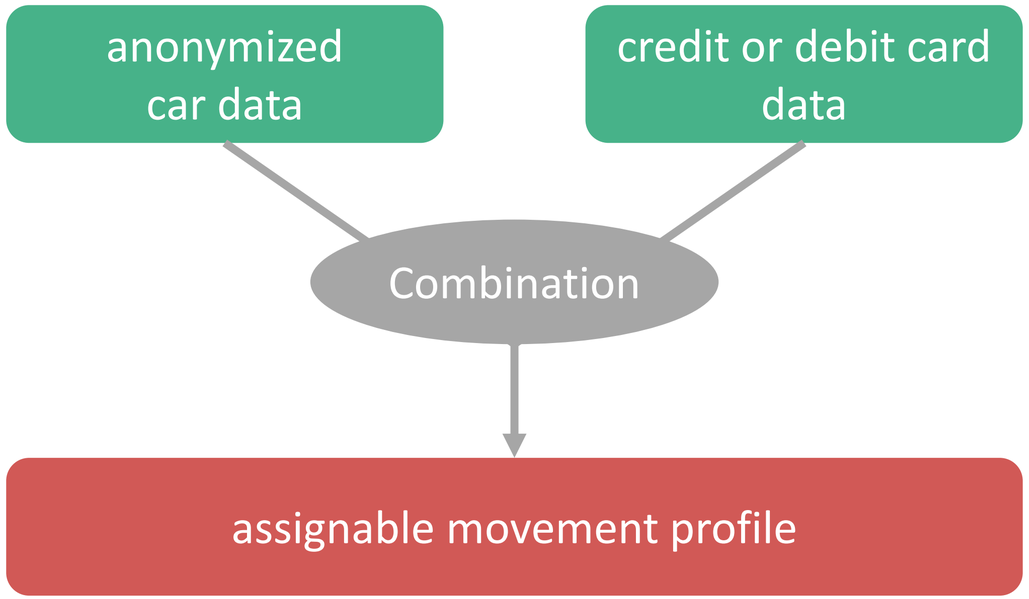


Lots of small harmless pieces

can make a harmful whole

The Combination-Problem (Example 2)

It’s possible that:



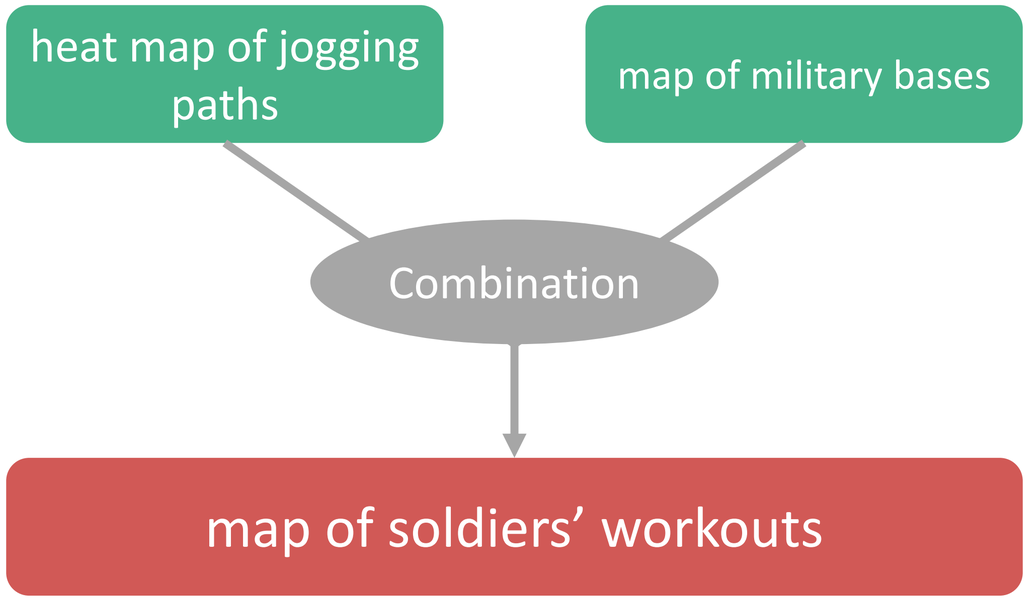
Lots of small harmless pieces

can make a harmful whole

ANOTHER PROBLEM

The Combination-Problem (Example 3)

It’s possible that:

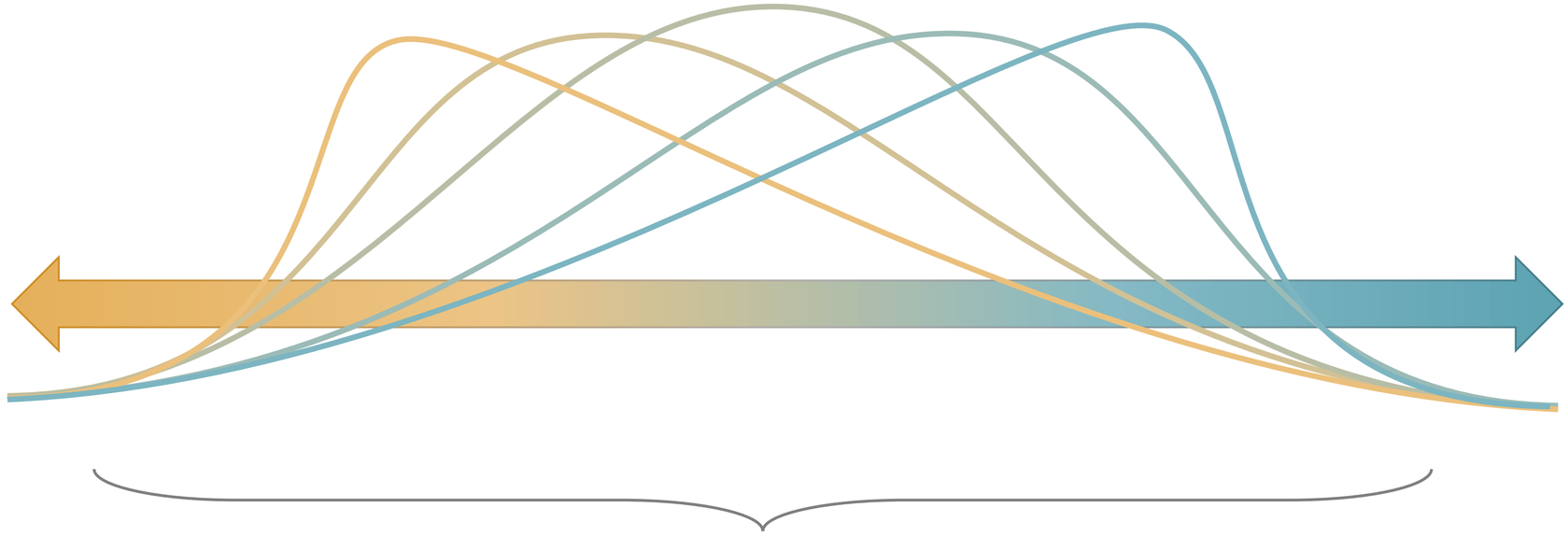


Lots of small harmless pieces

can make a harmful whole

YET ANOTHER PROBLEM

Suppose we can (to some degree) trade in security for privacy and vice versa



maximum security*, but minimal privacy

would be quite bad

we want to get to an optimal point in between
problem: we don't know where this point is and whether it is unique

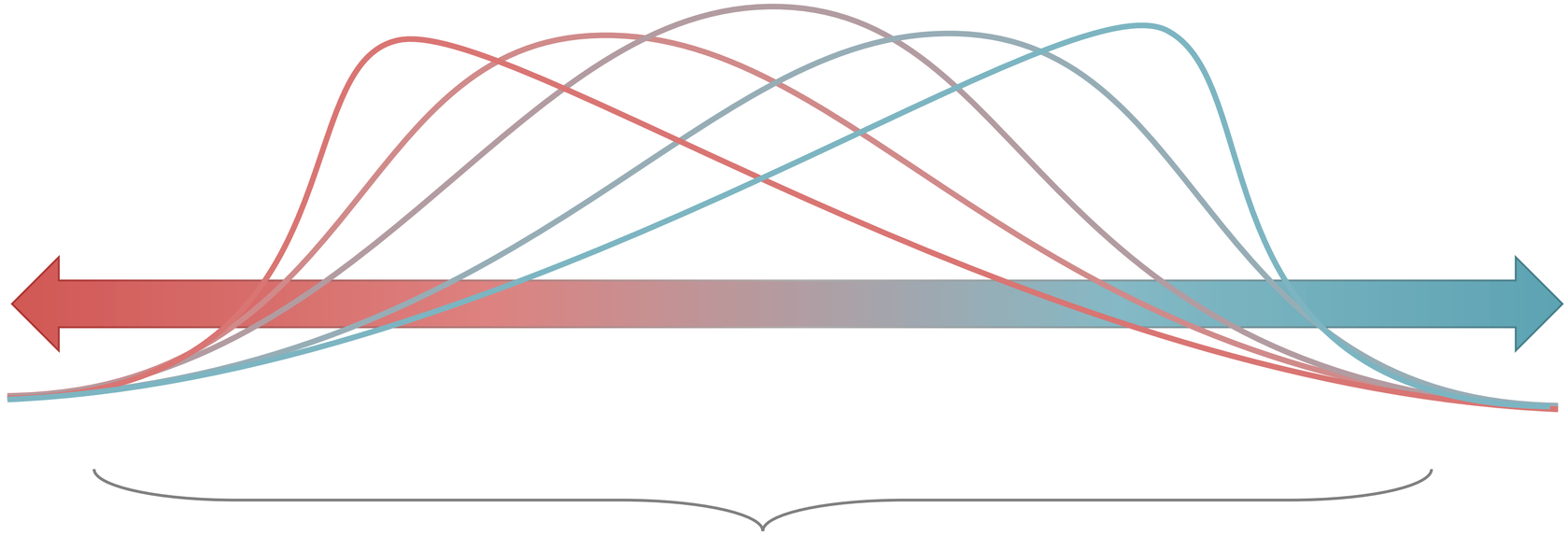
maximum privacy, but minimal security*

would be quite bad

*not *data*, but *public* security

YET ANOTHER PROBLEM

Suppose we can (to some degree) trade in security for privacy and vice versa



maximum convenience, but minimal privacy

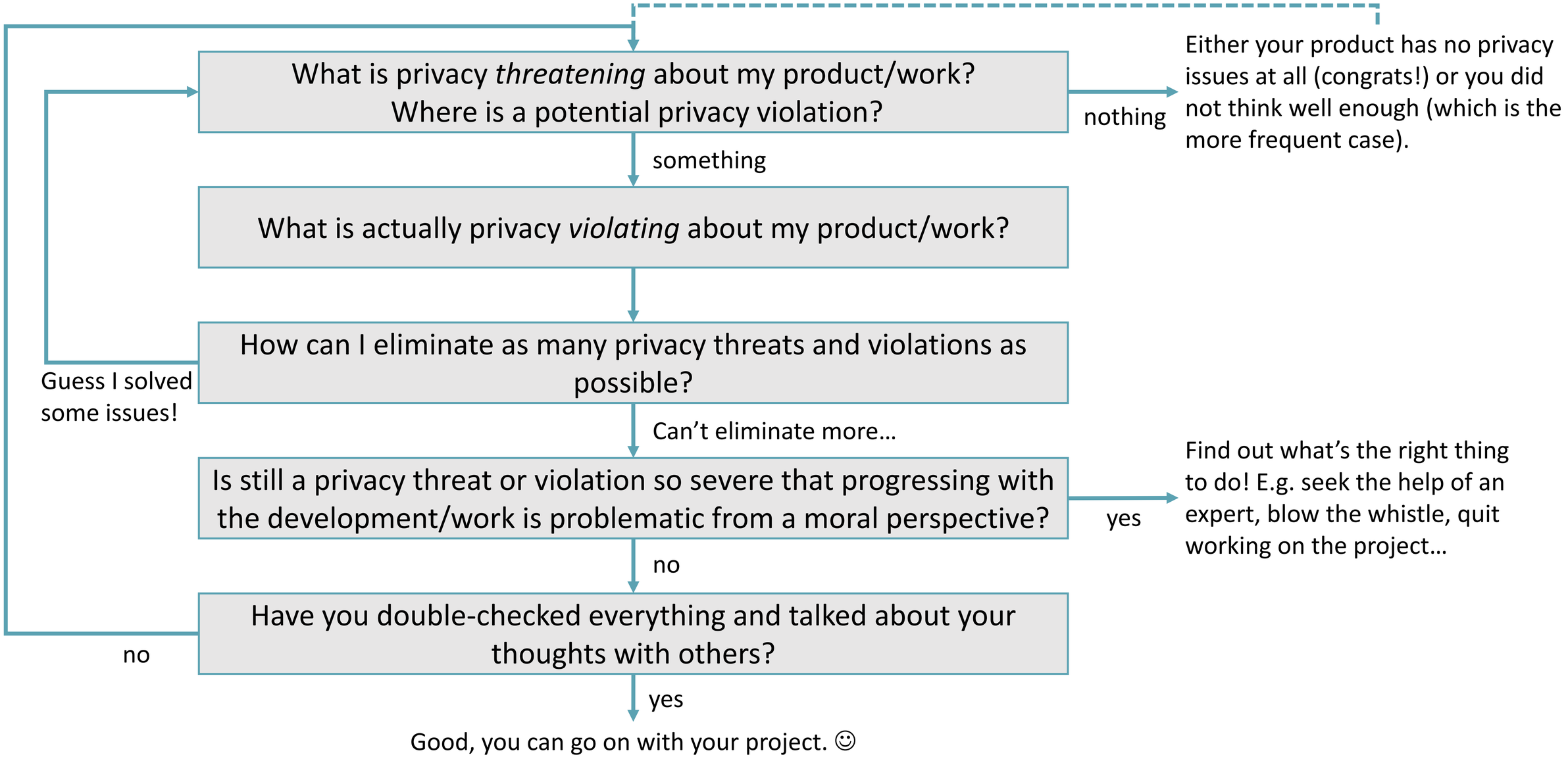
would be quite bad

we want to get to an optimal point in between
problem: we don't know where this point is and whether it is unique

maximum privacy, but minimal convenience

would be quite bad

WHAT YOU CAN DO WHEN YOU ADD A FEATURE TO YOUR PRODUCT

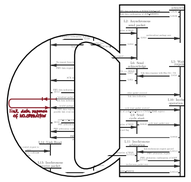


Ethics for Nerds

An Advanced Course in Computer Science
Summer Semester 2020

Contemporary Topics C4.3
Privacy

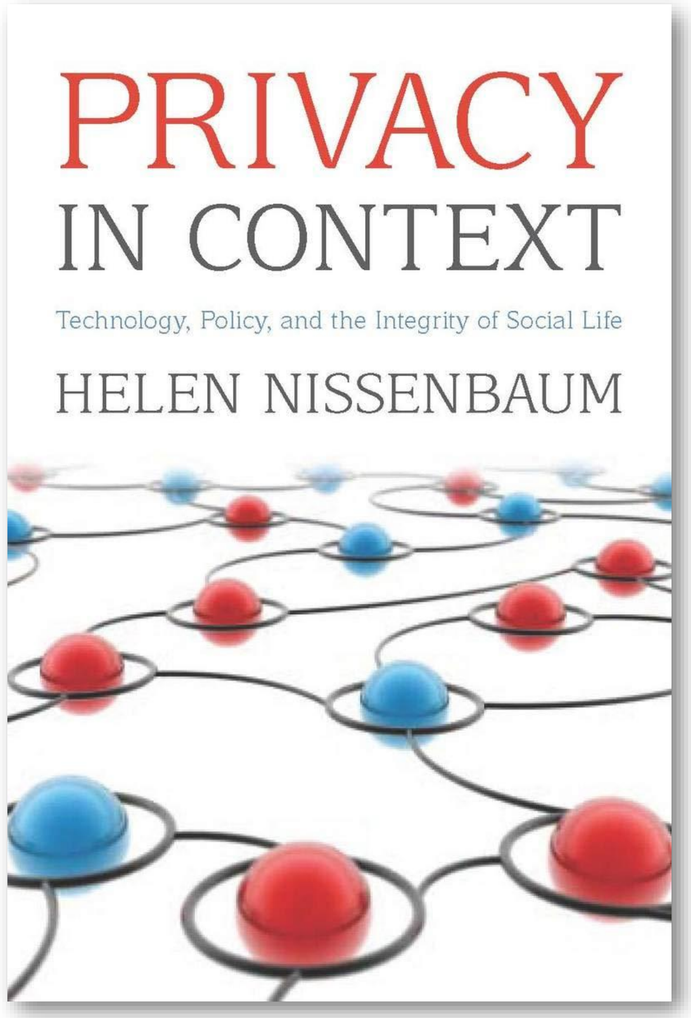
A Benchmark for Privacy



Prof. Holger Hermanns,
Kevin Baum, Sarah Sterz

UNIVERSITÄT
DES
SAARLANDES

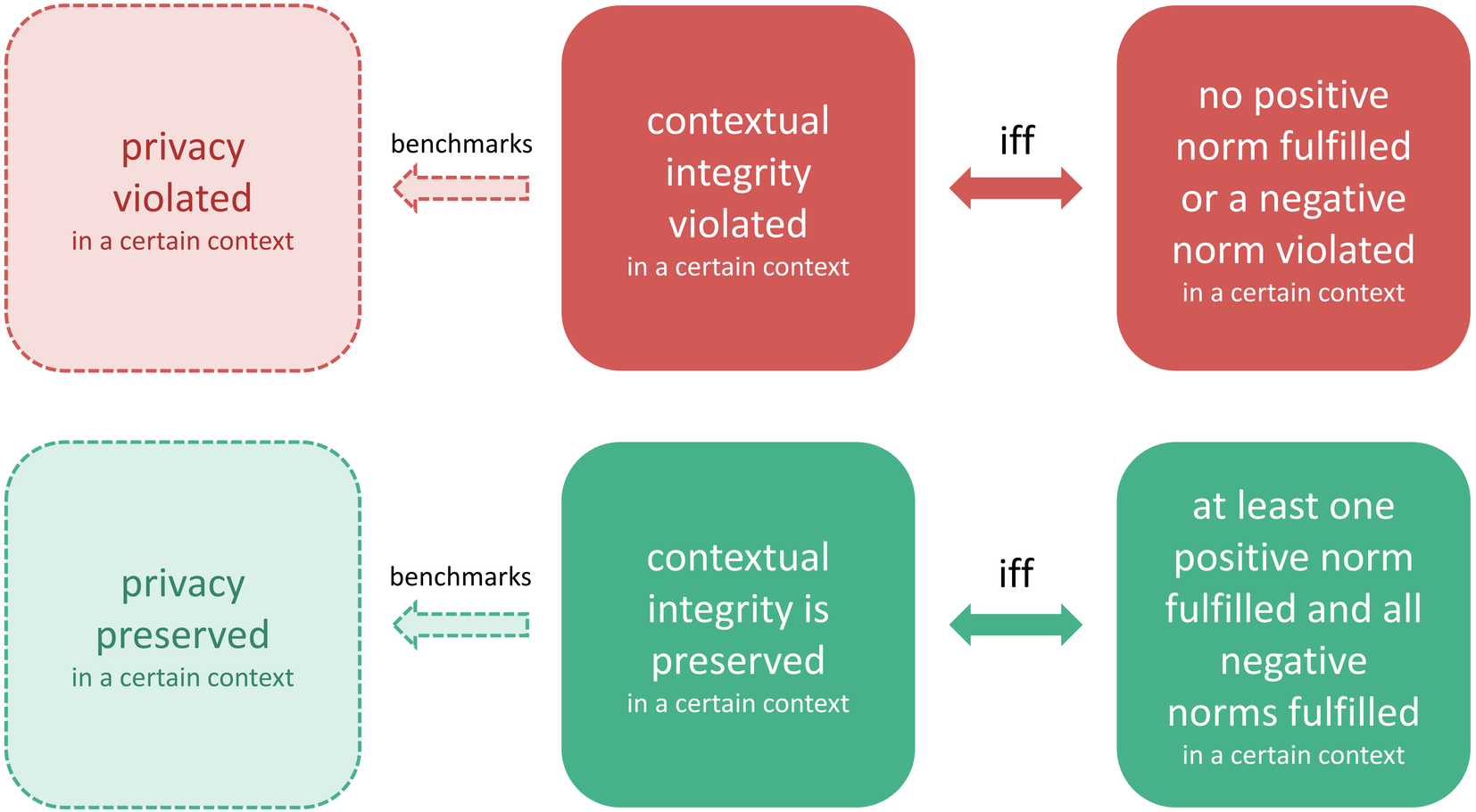
NISSENBAUM



Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Barth, A., Datta, A., Mitchell, J. C., & Nissenbaum, H. (2006). Privacy and contextual integrity: Framework and applications. In *2006 IEEE symposium on security and privacy (S&P'06)* (pp. 15-pp). IEEE.

NISSENBAUM



negative norms: state necessary conditions for information flow

Example: the doctor may share the diagnosis with colleagues *only if* the patient explicitly consented

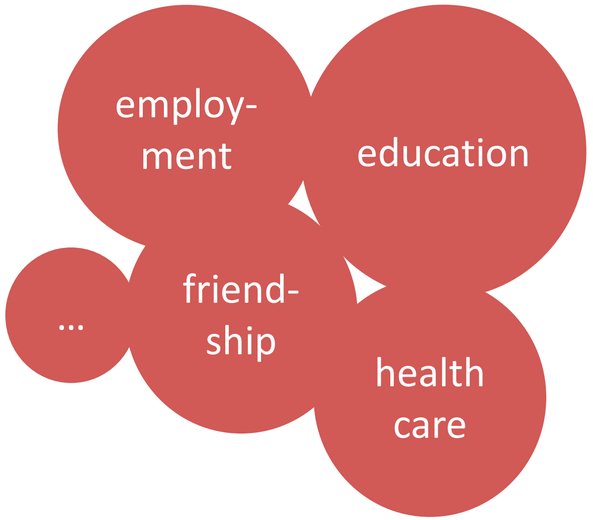
positive norms: state sufficient conditions for information flow

Example: the doctor may share the diagnosis with colleagues *if* the patient explicitly consented

NISSENBAUM

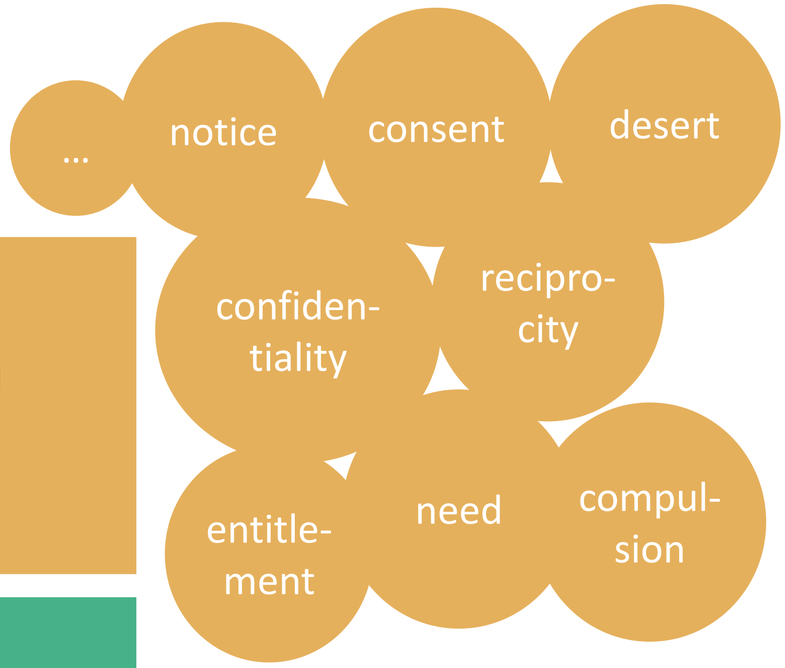
Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Both negative and positive norms have four key parameters:



context

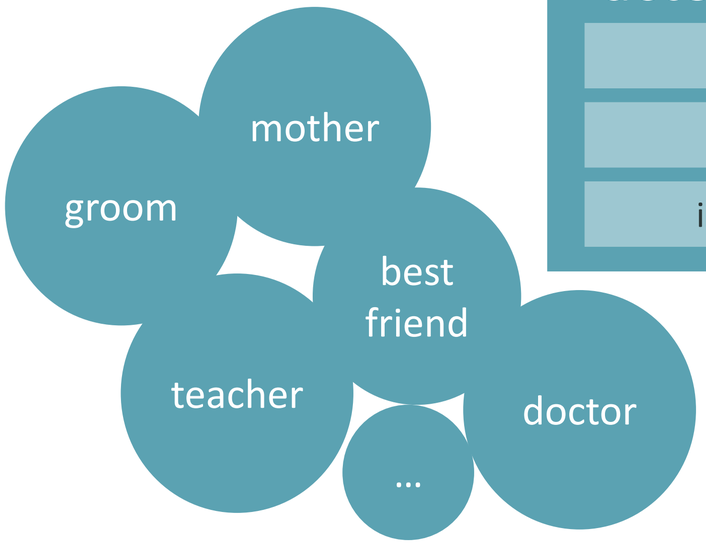
transmission principles

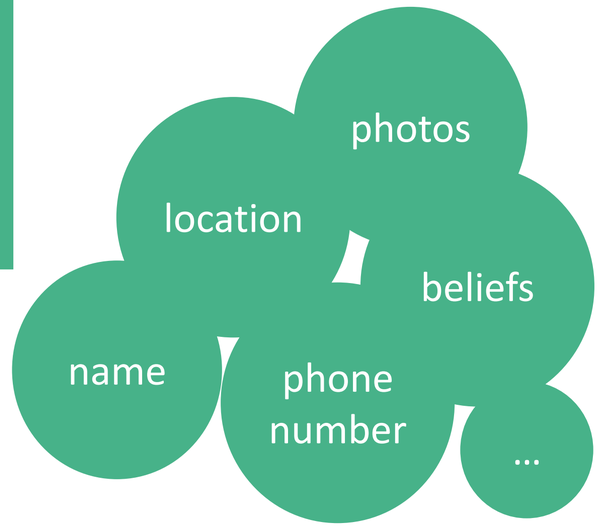


actors (and their roles)

- sender
- recipient
- information subject

attributes





NISSENBAUM

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Examples for transmission principles (not a complete list!):

Confidentiality:	the party receiving information is prohibited from sharing it
Reciprocity:	information flow must be bidirectional
Desert:	an actor deserves to receive some information
Entitlement:	an actor is entitled to know something
Compulsion:	one party is compelled or mandated to reveal some information
Need:	one party needs to know some information of a particular kind
Notice:	if information is shared, it must be known to the subject (that it is so and the content)
Consent:	the subject has to express her consent explicitly before sharing information

Not every transmission principle is in place in every situation. Which ones are in place depends on many factory: the context, the roles of the actors, the historical and cultural context, …

Example

A doctor talks to his colleague about a case of his and tells them that a certain patient has a certain condition with the intention to get consultation.

Context: Healthcare

Actors: Doctor A (sender), doctor B (recipient) and patient P (information subject)

Attribute: has a certain condition

Transmission principles in place:

- recipient confidentiality (B cannot tell anybody else)
- need (B needs to know the diagnosis if she is supposed to give a consultation)

→ a positive norms respected (need), and no negative norm violated (confidentiality), so contextual integrity is preserved

Example

A doctor talks to a patient about a case of his and tells him that a certain patient has a certain condition with the intention to entertain the patient he is talking to.

Context: Healthcare

Actors: Doctor A (sender), patient B (recipient) and patient P (information subject)

Attribute: has a certain condition

Transmission principles in place:

- sender confidentiality (A cannot tell anyone who is not medical staff)

→ a negative norm is violated, so contextual integrity violated