A Taste of Privacy Threat Modeling

Kim Wuyts

@wuytski

@kimw@mastodon.social

DO YOU REALLY NEED ALL OF IT?

Only take what you
really need
or it can get messy

1. WHAT IS GOING ON?

2. WHAT CAN GO WRONG?

SCOOP WILL FALL OFF

DOESN'T LIKE THE FLAVOR

TOO MUCH TO FINISH

IT STARTS MELTING AND MAKE A MESS

STARTS EATING THE CONE

3. WHAT TO DO ABOUT IT?

LIMIT TO 2 SCOOP

FAVORITE FLAVOR

IN A CUP

4. WAIT A MINUTE?!

LIMIT TO 2 SCOOP

DIFFERENT APPETITE?

FAVORITE FLAVOR

DIFFERENT SHOP,
DIFFERENT PREFERENCE?

IN A CUP

+ NAPKINS
(LOTS OF NAPKINS!!)

THREAT MODELING

1. WHAT IS GOING ON?

2. WHAT CAN GO WRONG?

3. WHAT TO DO ABOUT IT?

4. WAIT A MINUTE?!

Kim Wuyts

Privacy engineering researcher | Threat modeling enthusiast | privacy-by-design advocate | LINDDUN privacy threat modeling designer

- PhD in privacy engineering
- Researcher at imec-DistriNet, KU Leuven, Belgium

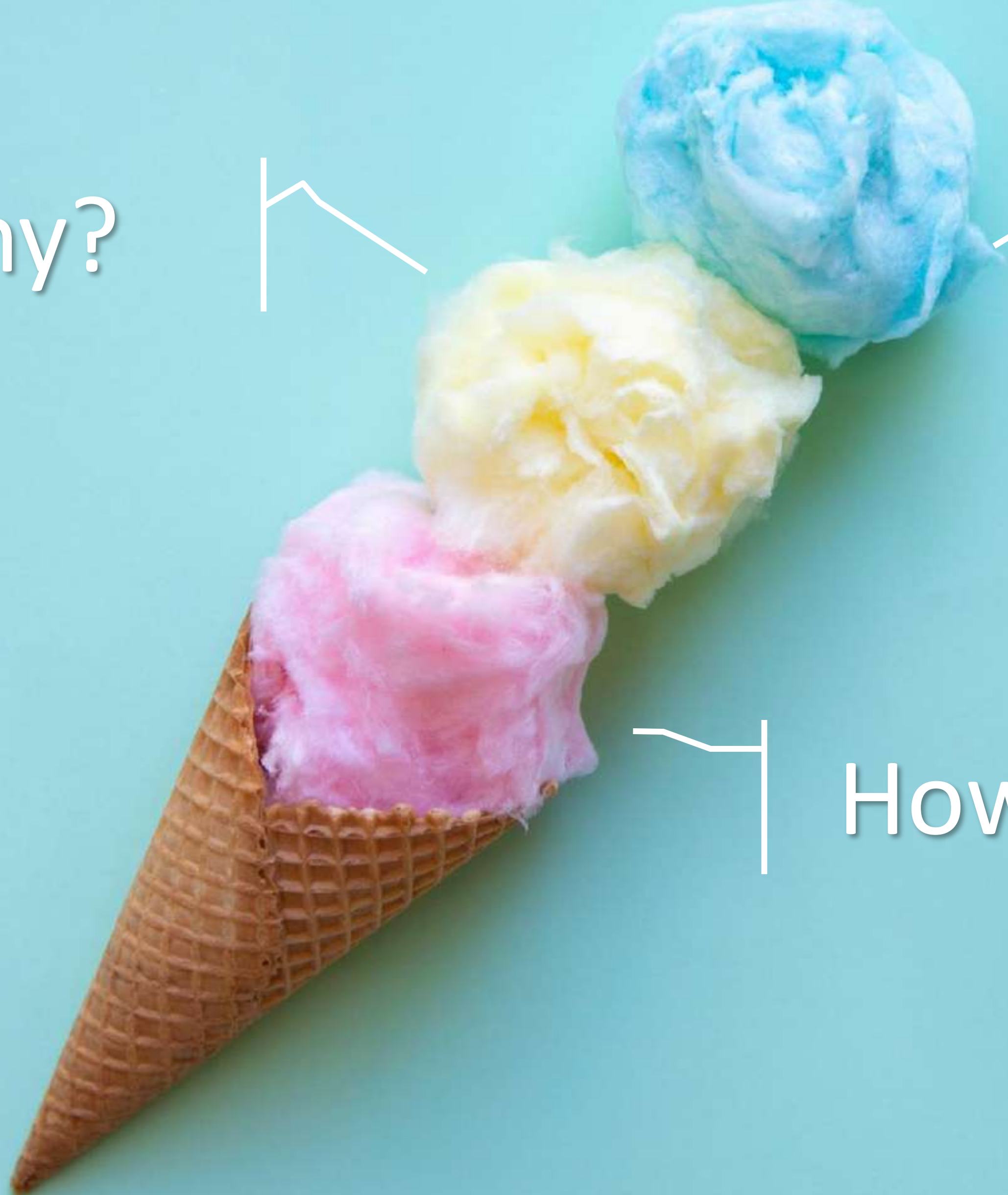
✉ Kim.Wuyts@kuleuven.be

@wuytski

@kimw@mastodon.social

https://www.linkedin.com/in/kwuyts/

A Taste of Privacy Threat Modeling



Why?

What?

How?

PRIVACY

WHY PRIVACY MATTERS?

```
0 1 0 1 1 1 0 0 1 0 1 1 0 0 1 0 0 0 1 1 1 0 0 1 0 1 0 1 1 1 0 0 1 1
1 1 0 0 0 1 0 1 1 0 0 0 1 1 0 1 0 1 1 0 0 1 1 1 1 0 0 1 0 1 0 1 1 0
1 0 0 1 1 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 1 1 0 0 1 0 1 0 0 1 0
0 1 0 1 1 1 0 0 1 0 1 1 0 0 1 0 0 0 1 1 1 0 0 1 0 1 0 1 1 1 0 0 1 1
1 1 0 0 0 1 0 1 1 0 0 0 1 1 0 1 0 1 1 0 0 1 1 1 1 0 0 1 0 1 0 1 1 0
1 0 0 1 1 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 1 1 0 0 1 0 1 0 0 1 0
0 1 0 1 1 1 0 0 1 0 1 1 0 0 1 0 0 0 1 1 1 0 0 1 0 1 0 1 1 1 0 0 1 1
1 1 0 0 0 1 0 1 1 0 0 0 1 1 0 1 0 1 1 0 0 1 1 1 1 0 0 1 0 1 0 1 1 0
1 0 0 1 1 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 1 1 0 0 1 0 1 0 0 1 0
0 1 0 1 1 1 0 0 1 0 1 1 0 0 1 0 0 0 1 1 1 0 0 1 0 1 0 1 1 1 0 0 1 1
1 1 0 0 0 1 0 1 1 0 0 0 1 1 0 1 0 1 1 0 0 1 1 1 1 0 0 1 0 1 0 1 1 0
1 0 0 1 1 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 1 1 0 0 1 0 1 0 0 1 0
0 1 0 1 1 1 0 0 1 0 1 1 0 0 1 0 0 0 1 1 1 0 0 1 0 1 0 1 1 1 0 0 1 1
1 1 0 0 0 1 0 1 1 0 0 0 1 1 0 1 0 1 1 0 0 1 1 1 1 0 0 1 0 1 0 1 1 0
1 0 0 1 1 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 1 1 0 0 1 0 1 0 0 1 0
0 1 0 1 1 1 0 0 1 0 1 1 0 0 1 0 0 0 1 1 1 0 0 1 0 1 0 1 1 1 0 0 1 1
1 1 0 0 0 1 0 1 1 0 0 0 1 1 0 1 0 1 1 0 0 1 1 1 1 0 0 1 0 1 0 1 1 0
1 0 0 1 1 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 1 1 0 0 1 0 1 0 0 1 0
0 1 0 1 1 1 0 0 1 0 1 1 0 0 1 0 0 0 1 1 1 0 0 1 0 1 0 1 1 1 0 0 1 1
1 1 0 0 0 1 0 1 1 0 0 0 1 1 0 1 0 1 1 0 0 1 1 1 1 0 0 1 0 1 0 1 1 0
1 0 0 1 1 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 1 1 0 0 1 0 1 0 0 1 0
0 1 0 1 1 1 0 0 1 0 1 1 0 0 1 0 0 0 1 1 1 0 0 1 0 1 0 1 1 1 0 0 1 1
1 1 0 0 0 1 0 1 1 0 0 0 1 1 0 1 0 1 1 0 0 1 1 1 1 0 0 1 0 1 0 1 1 0
1 0 0 1 1 1 0 1 0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 1 1 0 0 1 0 1 0 0 1 0
```

I HAVE DONE NOTHING WRONG,
SO I HAVE NOTHING TO HIDE

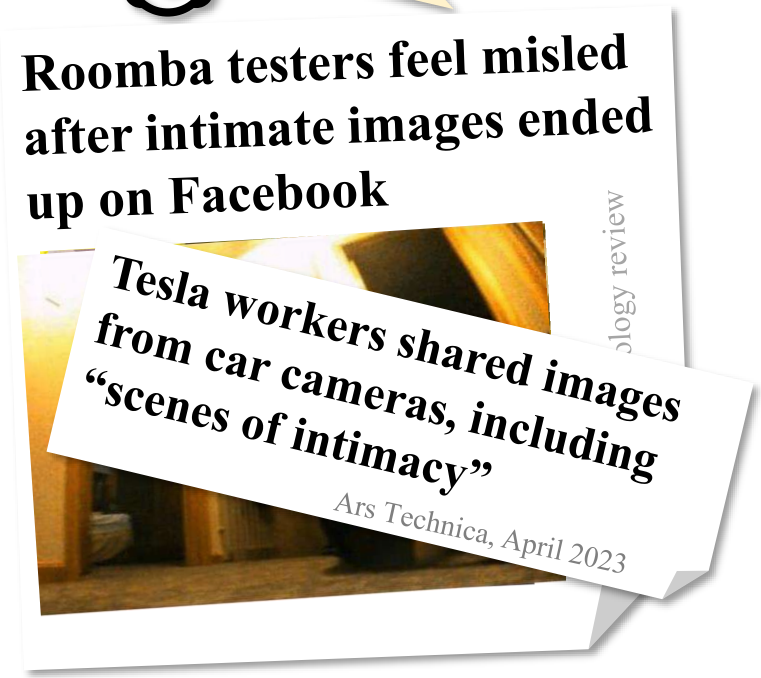
MISCONCEPTION

WHY PRIVACY MATTERS?

WHY PRIVACY MATTERS?

I HAVE DONE NOTHING WRONG, SO I HAVE NOTHING TO HIDE

MISCONCEPTION

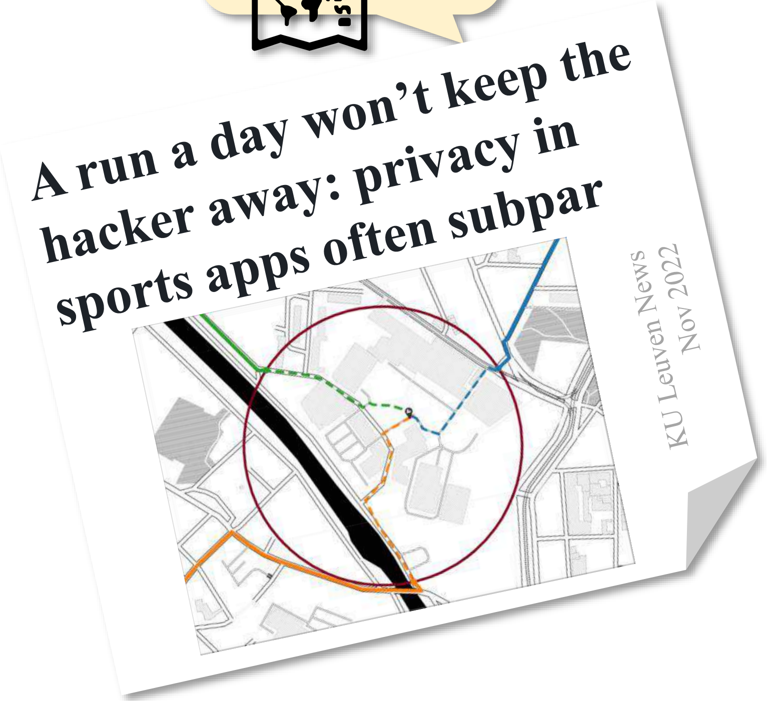


Roomba testers feel misled after intimate images ended up on Facebook

ology review

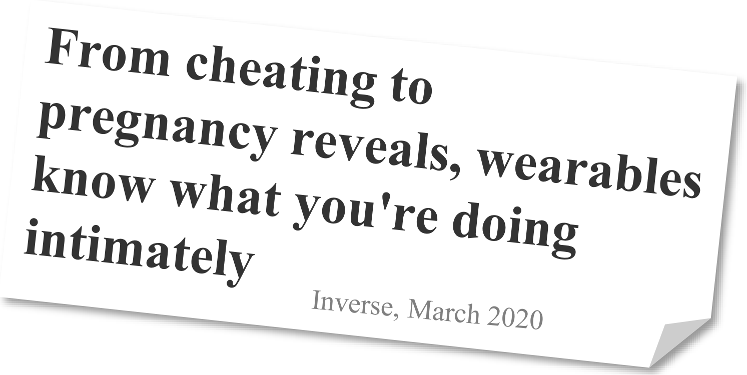
Tesla workers shared images from car cameras, including “scenes of intimacy”

Ars Technica, April 2023



A run a day won’t keep the hacker away: privacy in sports apps often subpar

KU Leuven News Nov 2022



From cheating to pregnancy reveals, wearables know what you're doing intimately

Inverse, March 2020

WHY SHOULD PRIVACY MATTER FOR COMPANIES?

MISCONCEPTION

NO WORRIES! WE ALREADY HAVE SECURITY MEASURES IN PLACE.

SECURITY vs. PRIVACY

MISCONCEPTION

WE VALUE SECURITY SO WE CAN'T SUPPORT PRIVACY!

PRIVACY ENGINEERING

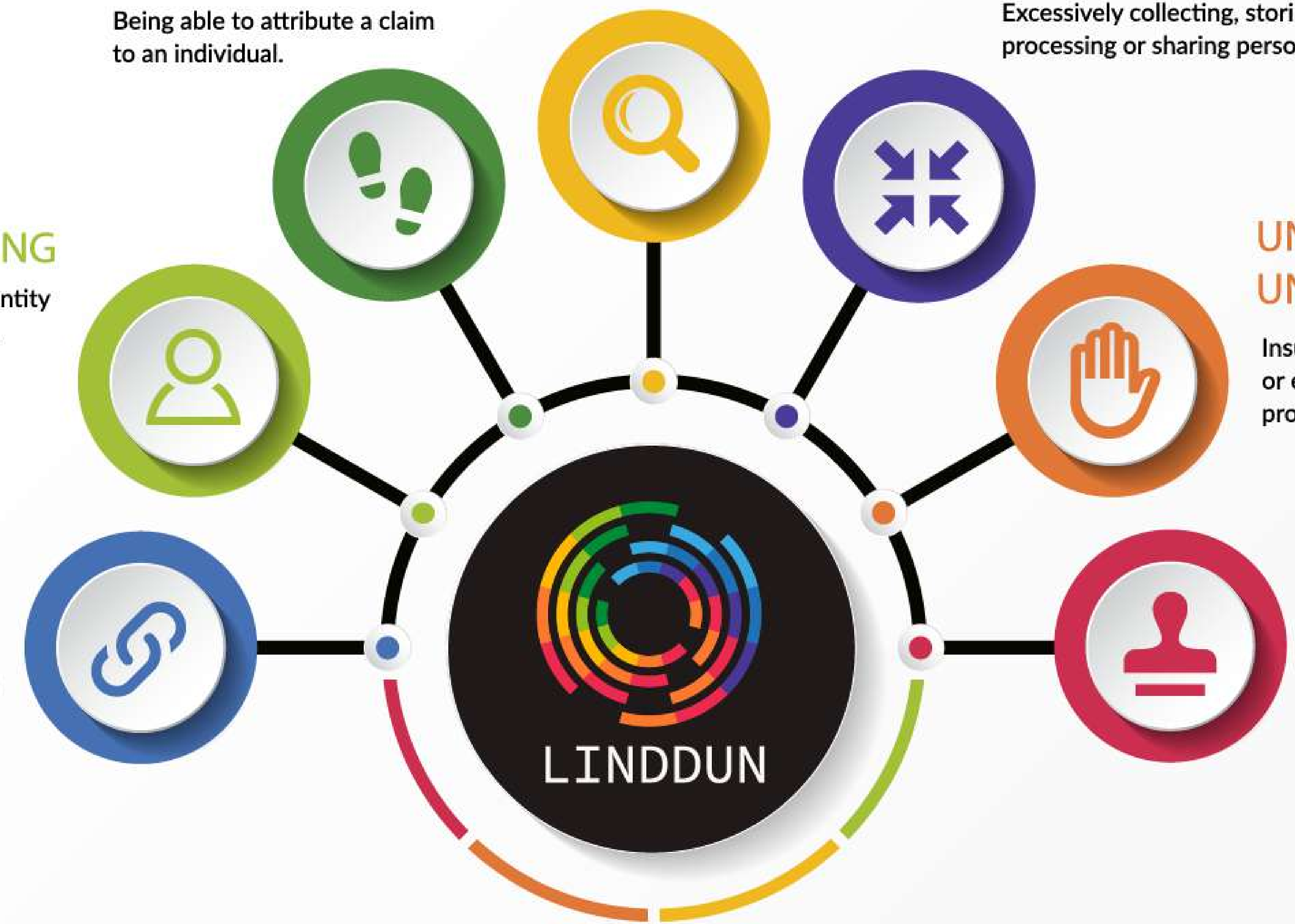
INTERVENABILITY
MANAGEABILITY

TRANSPARENCY
PREDICTABILITY

UNLINKABILITY
DISASSOCIABILITY

M. Hansen, M. Jensen and M. Rost, "Protection Goals for Privacy Engineering," *2015 IEEE Security and Privacy Workshops*, 2015

NISTIR 8062 An Introduction to Privacy Engineering and Risk Management in Federal Systems, 2017



LINKING

Associating data items or user actions to learn more about an individual or group.

IDENTIFYING

Learning the identity of an individual.

NON-REPUDIATION

Being able to attribute a claim to an individual.

DETECTING

Deducing the involvement of an individual through observation.

DATA DISCLOSURE

Excessively collecting, storing, processing or sharing personal data.

UNAWARENESS & UNINTERVENABILITY

Insufficiently informing, involving or empowering individuals in the processing of personal data.

NON-COMPLIANCE

Deviating from security and data management best practices, standards and legislation.

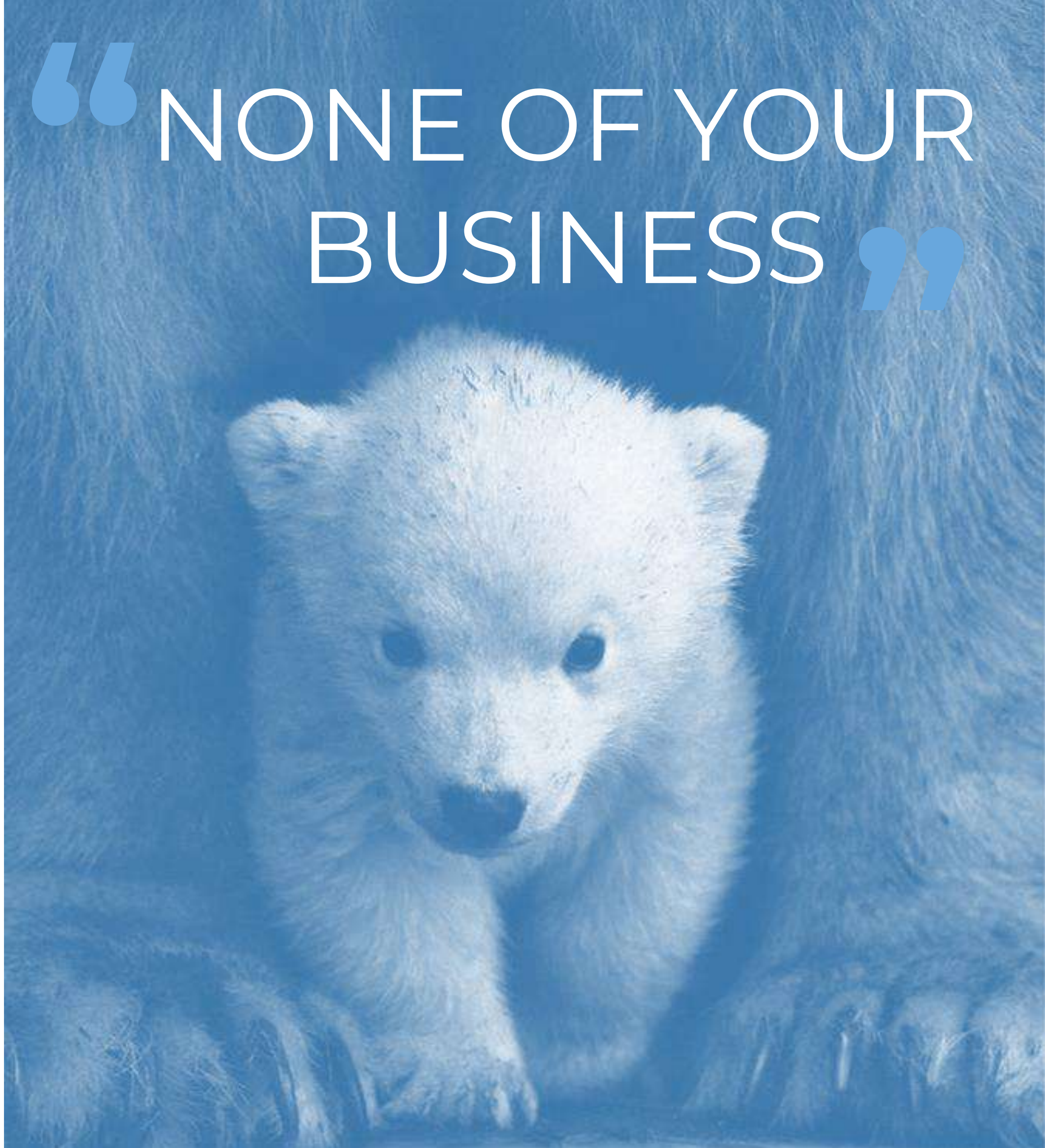
DATA DISCLOSURE

UNNECESSARY USE

OF DATA

- Excessive data types
- Excessive volume
- Excessive processing
- Excessive exposure

- collection
- storage
- processing
- sharing



“NONE OF YOUR BUSINESS”

LINKING

PLAYING “GUESS WHO”

Linking multiple properties to
the same individual

vs.

IDENTIFYING

WINNING “GUESS WHO”

Reducing the set of individuals
to one.

LINKING

LEARNING MORE ABOUT AN INDIVIDUAL (OR GROUP) BY MATCHING DATA ITEMS TOGETHER

- Through identifiers
- Through combination
- Through profiling/derivation/inference

“CONNECTING THE DOTS”

IDENTIFYING

LEARNING THE IDENTITY

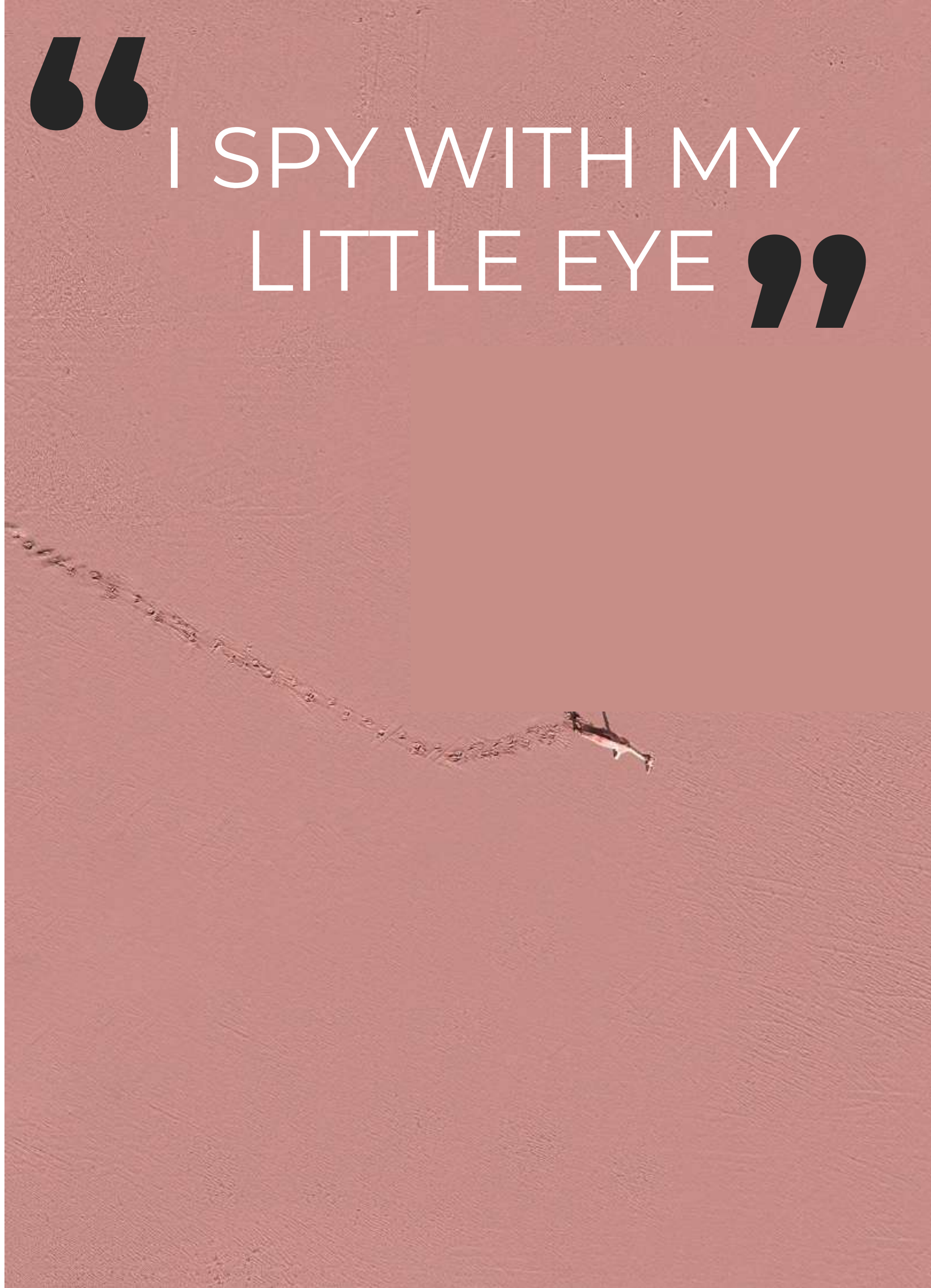
- Through direct identifiers
- Through identifiable information
  - Pseudonyms
  - Revealing content
  - Small anonymity set (set of individuals)

“IF IT WALKS AND TALKS LIKE A DUCK, IT IS A DUCK.”

DETECTING

DEDUCING SUBJECT INVOLVEMENT BY OBSERVING EXISTENCE OF RELEVANT INFORMATION

- Observed communication
- Application side-effects
- System responses



"I SPY WITH MY LITTLE EYE"

NON-REPUDIATION

PROOF OF A CLAIM ABOUT AN INDIVIDUAL

- Evidence of the claim / action
- Attribution to the individual

“I KNOW WHAT YOU DID LAST SUMMER”
Evidence of action
Attributed to the individual

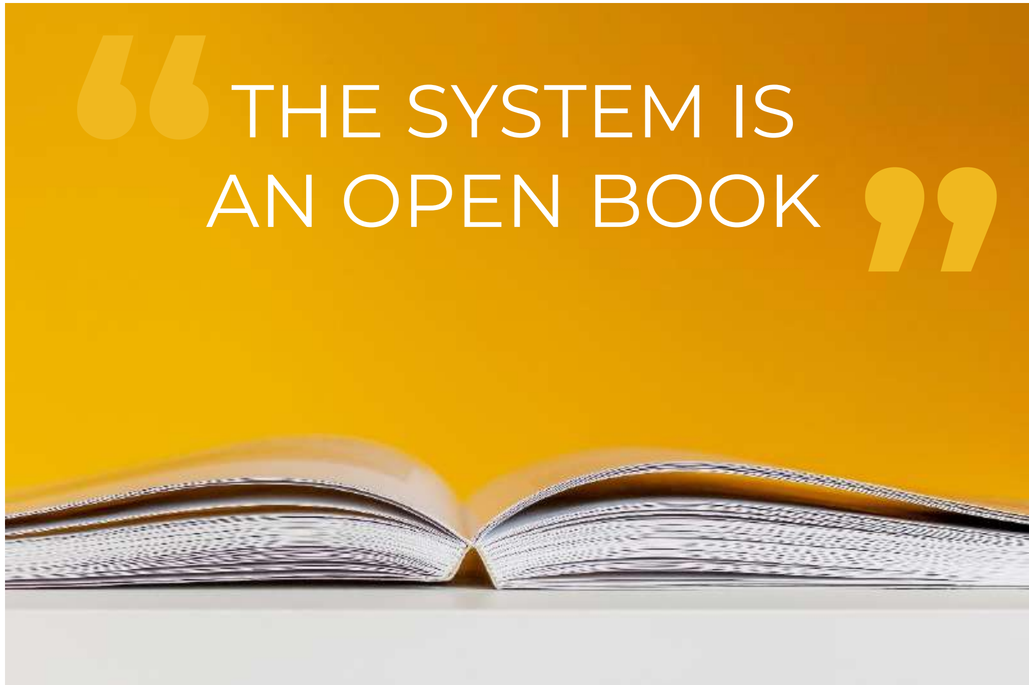
- Unawareness of data subject
- Unawareness of user sharing personal data (about others or themselves)

INSUFFICIENTLY INFORMING ABOUT THE PROCESSING OF PERSONAL DATA

UNAWARENESS

LACK OF DATA SUBJECT CONTROL

- Lack of preferences control
- Lack of access
- Lack of rectification/erasure



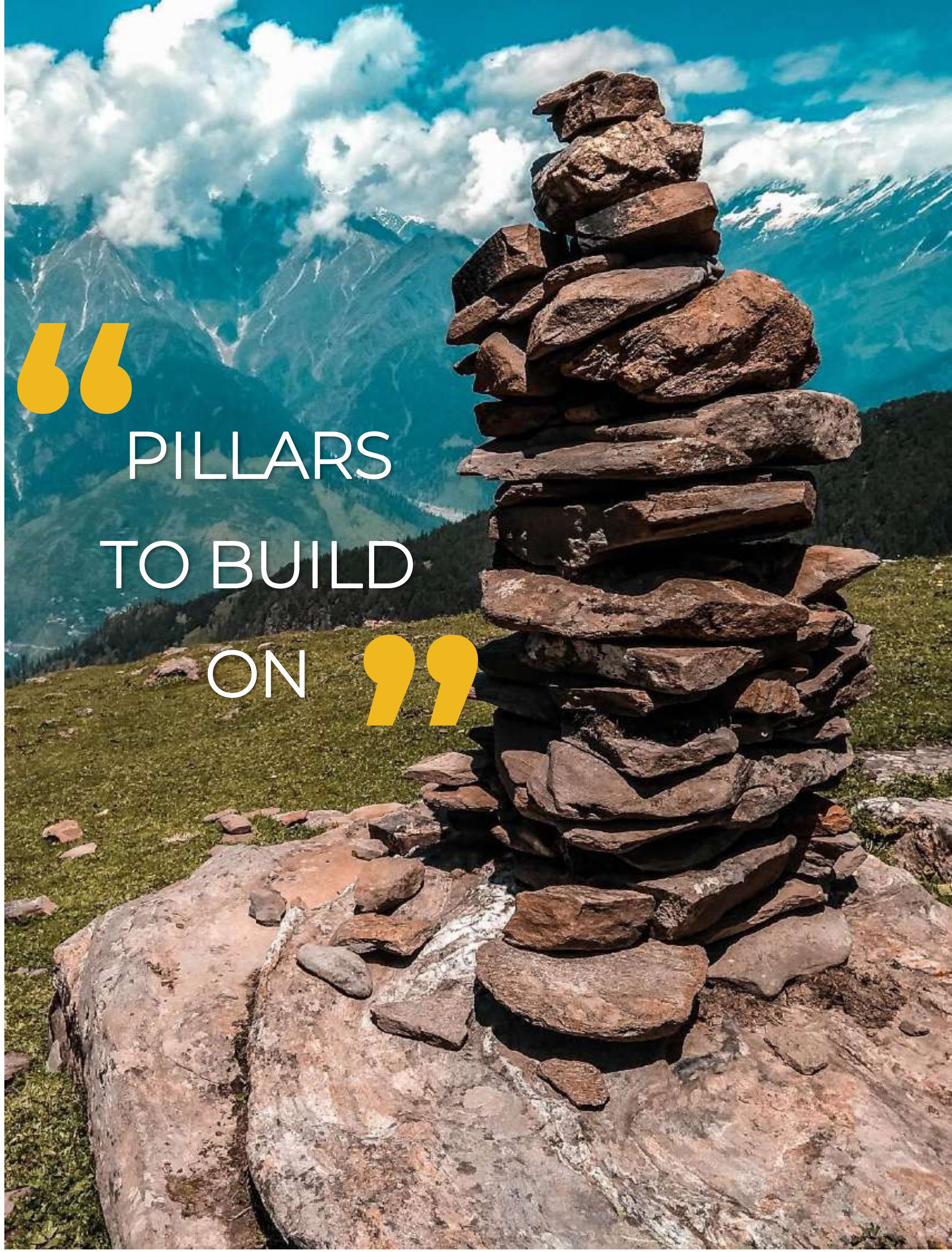
“THE SYSTEM IS AN OPEN BOOK”

“THE INDIVIDUAL SHOULD BE IN THE DRIVER’S SEAT”

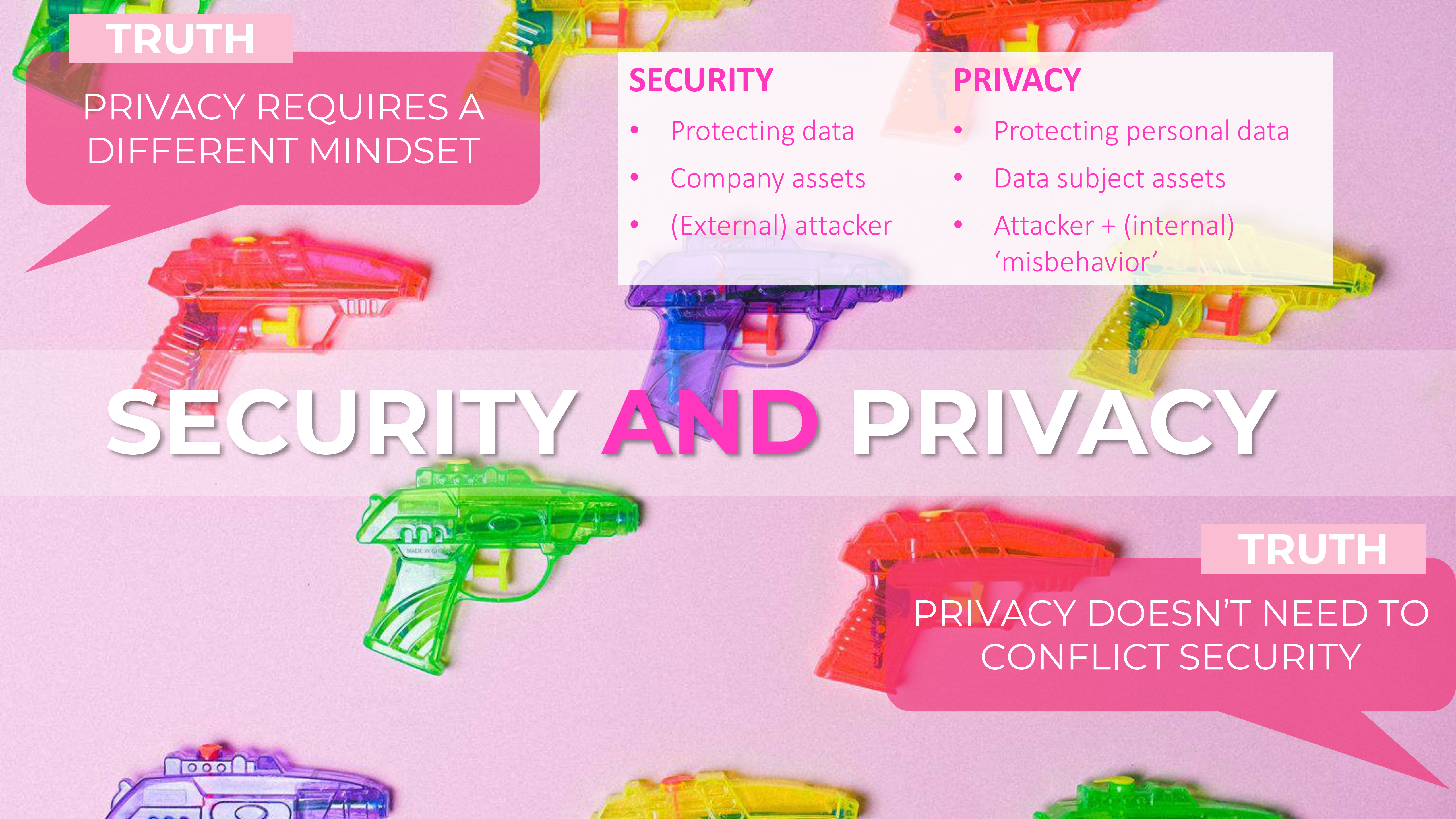
NON-COMPLIANCE

LACK OF ADHERENCE TO LEGISLATION, REGULATION, STANDARDS AND BEST PRACTICES

- Lawfulness
- Data lifecycle management
- Cybersecurity risk management



“PILLARS TO BUILD ON”



SECURITY AND PRIVACY

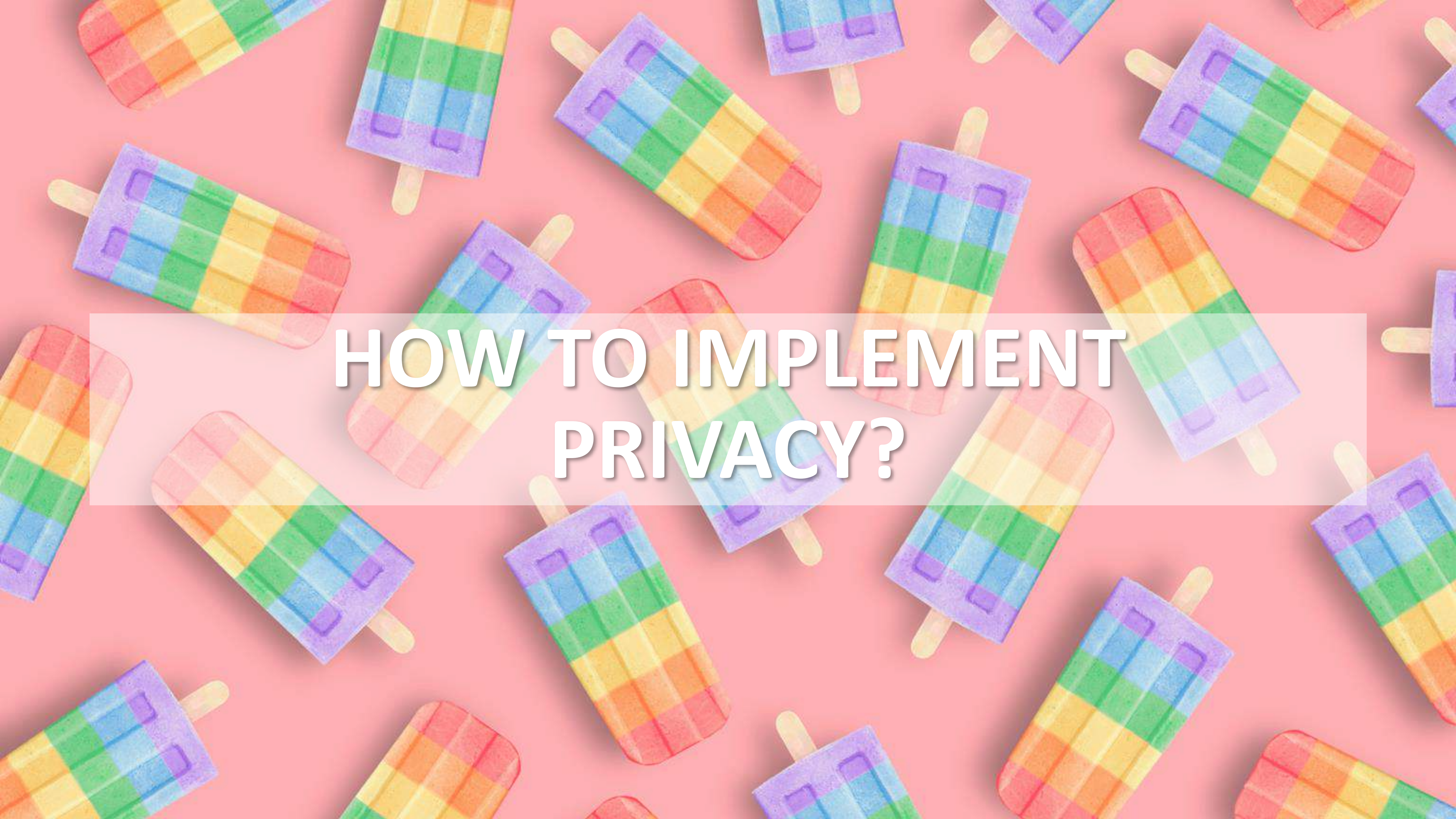
TRUTH

PRIVACY REQUIRES A DIFFERENT MINDSET

SECURITY	PRIVACY
• Protecting data	• Protecting personal data
• Company assets	• Data subject assets
• (External) attacker	• Attacker + (internal) ‘misbehavior’

TRUTH

PRIVACY DOESN’T NEED TO CONFLICT SECURITY



HOW TO IMPLEMENT PRIVACY?

HOW TO IMPLEMENT PRIVACY?

How to draw an owl?

1. Draw some circles

2. Draw the rest of the f***ing owl

PRIVACY BY DESIGN

Tackled **proactively**

Systematically analyzed

Integrated in the development lifecycle

Have an **impact on design** decisions

WHAT IS THREAT MODELING?

Analyzing representations of a system to highlight concerns about security and privacy characteristics

- Threat Modeling Manifesto

- Tackled **proactively**
- **Systematically** analyzed
- **Integrated** in the development lifecycle
- Have an **impact on design** decisions

WHAT IS THREAT MODELING?

Think about what can go wrong
so you can fix it before it actually happens

Something we do in our day-to-day lives

Used in security community >20 years

Equally useful for privacy engineering

Threat modeling is HOT

HOW TO THREAT MODEL?

1. MODEL THE SYSTEM

- Create DFD / white board sketch / …

2. ELICIT THREATS

- Map model components
- Identify threats

3. MITIGATE THREATS

- Assess & prioritize
- Mitigate

4. REFLECT

- Reflect & repeat

All models are wrong, some are useful - *G. Box*

1. MODEL THE SYSTEM

- Create DFD / white board sketch / …

2. ELICIT THREATS

- Map model components
- Identify threats

3. MITIGATE THREATS

- Assess & prioritize
- Mitigate

4. REFLECT

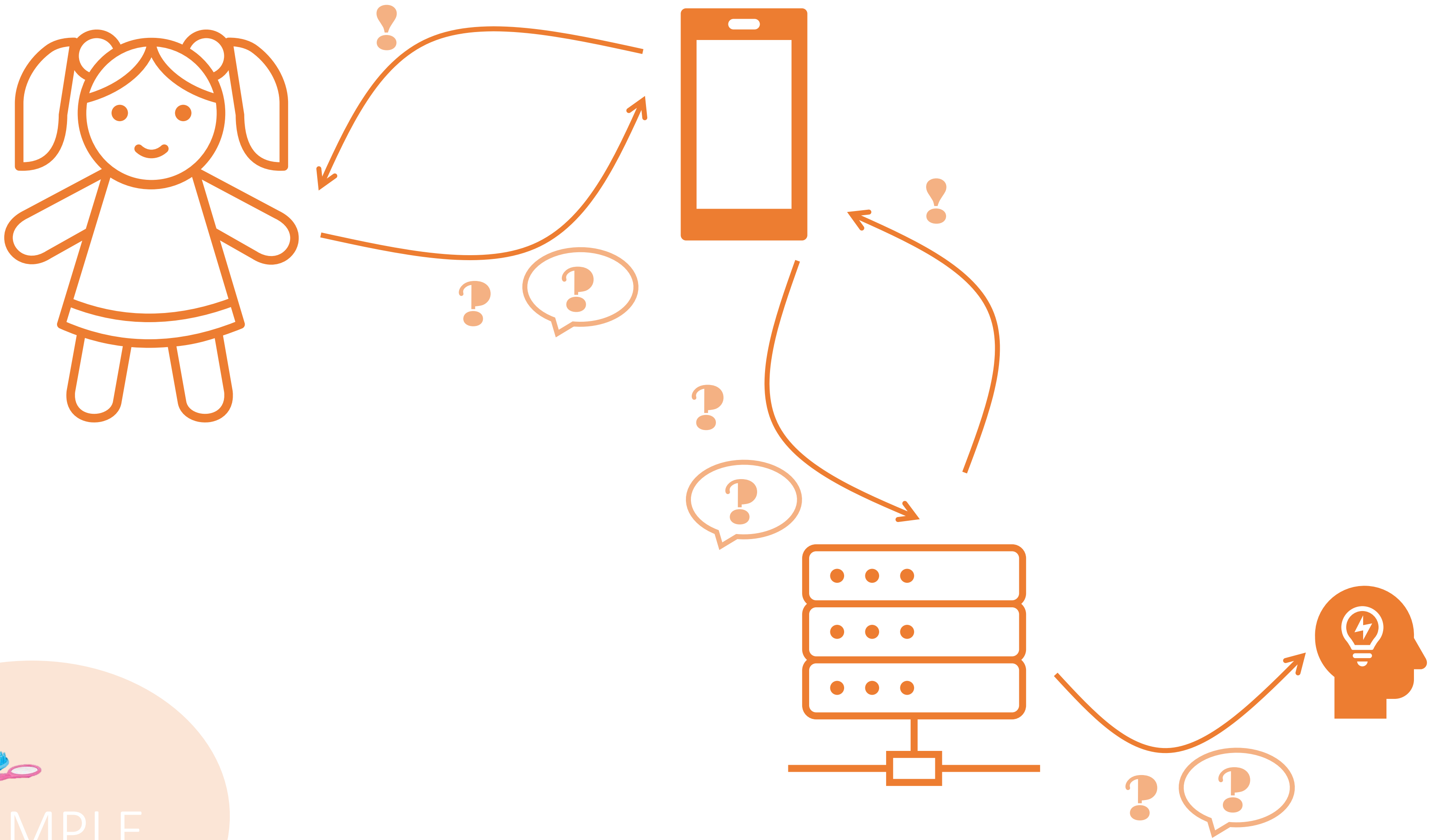
- Reflect & repeat

1. MODEL THE SYSTEM

2. ELICIT THREATS

3. MITIGATE THREATS

4. REFLECT



?	Question(s)
💬	Voice recordings
!	Response

EXAMPLE

NOW WHAT?

PROCESS

1. MODEL THE SYSTEM

- Create DFD / white board sketch / …

2. ELICIT THREATS

- Map model components
- Identify threats

3. MITIGATE THREATS

- Assess & prioritize
- Mitigate

4. REFLECT

- Reflect & repeat

REUSABLE KNOWLEDGE

STRIDE

- SPOOFING
- TAMPERING
- REPUDIATION
- INFORMATION DISCLOSURE
- DENIAL OF SERVICE
- ELEVATION OF PRIVILEGE

LINDDUN

- LINKING
- IDENTIFYING
- NON-REPUDIATION
- DETECTING
- DATA DISCLOSURE
- UNAWARENESS
- NON-COMPLIANCE

PROCESS

1. MODEL THE SYSTEM

- Create DFD / white board sketch / …

2. ELICIT THREATS

- Map model components
- Identify threats

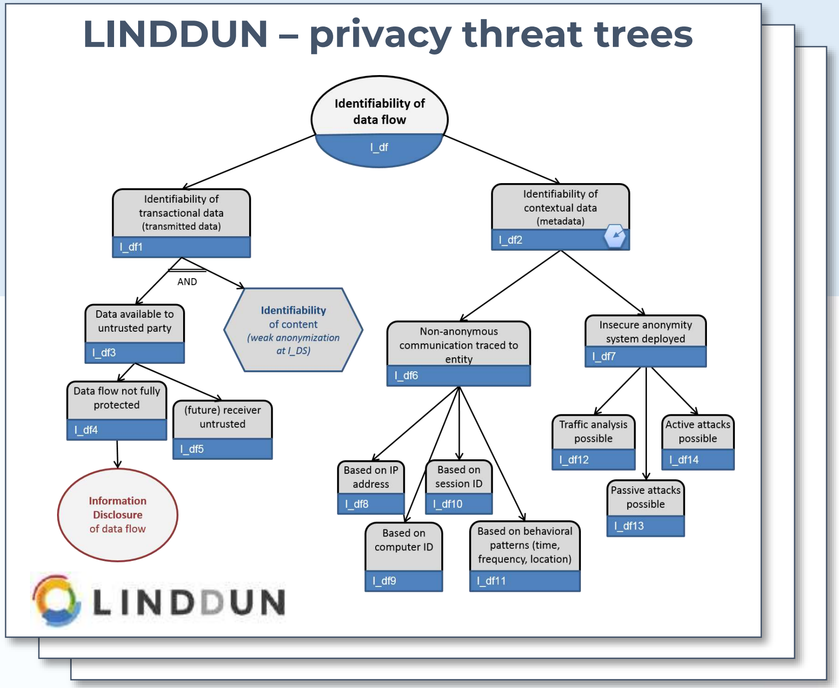
3. MITIGATE THREATS

- Assess & prioritize
- Mitigate

4. REFLECT

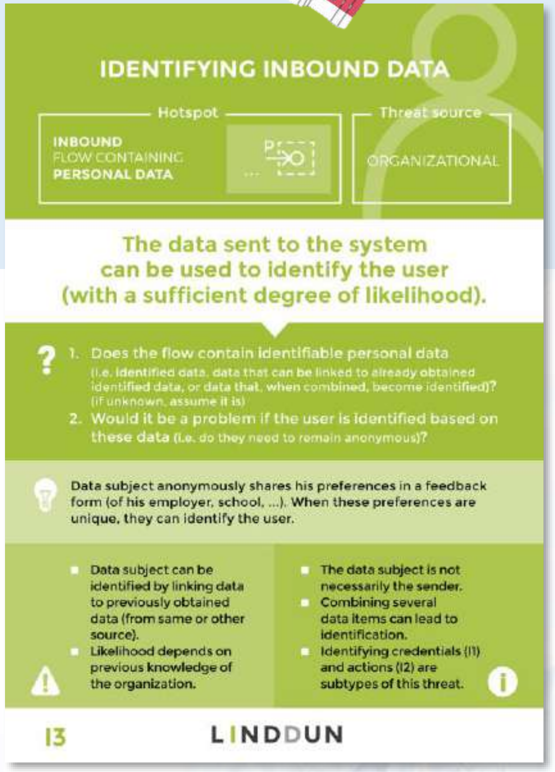
- Reflect & repeat

REUSABLE KNOWLEDGE



LINDDUN – privacy threat trees

Identifiability of data flow
I_df
Identifiability of transactional data (transmitted data)
I_df1
AND
Identifiability of content (weak anonymization at I_DS)
Data available to untrusted party
I_df3
Data flow not fully protected
I_df4
(future) receiver untrusted
I_df5
Information Disclosure of data flow
Identifiability of contextual data (metadata)
I_df2
Non-anonymous communication traced to entity
I_df6
Based on IP address
I_df8
Based on session ID
I_df10
Based on computer ID
I_df9
Based on behavioral patterns (time, frequency, location)
I_df11
Insecure anonymity system deployed
I_df7
Traffic analysis possible
I_df12
Active attacks possible
I_df14
Passive attacks possible
I_df13
LINDDUN



IDENTIFYING INBOUND DATA

Hotspot: INBOUND FLOW CONTAINING PERSONAL DATA

Threat source: ORGANIZATIONAL

The data sent to the system can be used to identify the user (with a sufficient degree of likelihood).

?
1. Does the flow contain identifiable personal data (i.e. identified data, data that can be linked to already obtained identified data, or data that, when combined, become identified)? (if unknown, assume it is)
2. Would it be a problem if the user is identified based on these data (i.e. do they need to remain anonymous)?

Data subject anonymously shares his preferences in a feedback form (of his employer, school, ...). When these preferences are unique, they can identify the user.

- Data subject can be identified by linking data to previously obtained data (from same or other source).
- Likelihood depends on previous knowledge of the organization.

- The data subject is not necessarily the sender.
- Combining several data items can lead to identification.
- Identifying credentials (I1) and actions (I2) are subtypes of this threat.

I3 LINDDUN

WWW.LINDDUN.ORG

LINDDUN GO cards

PROCESS

1. MODEL THE SYSTEM

- Create DFD / white board sketch / ...

2. ELICIT THREATS

- Map model components
- Identify threats

3. MITIGATE THREATS

- Assess & prioritize
- Mitigate

4. REFLECT

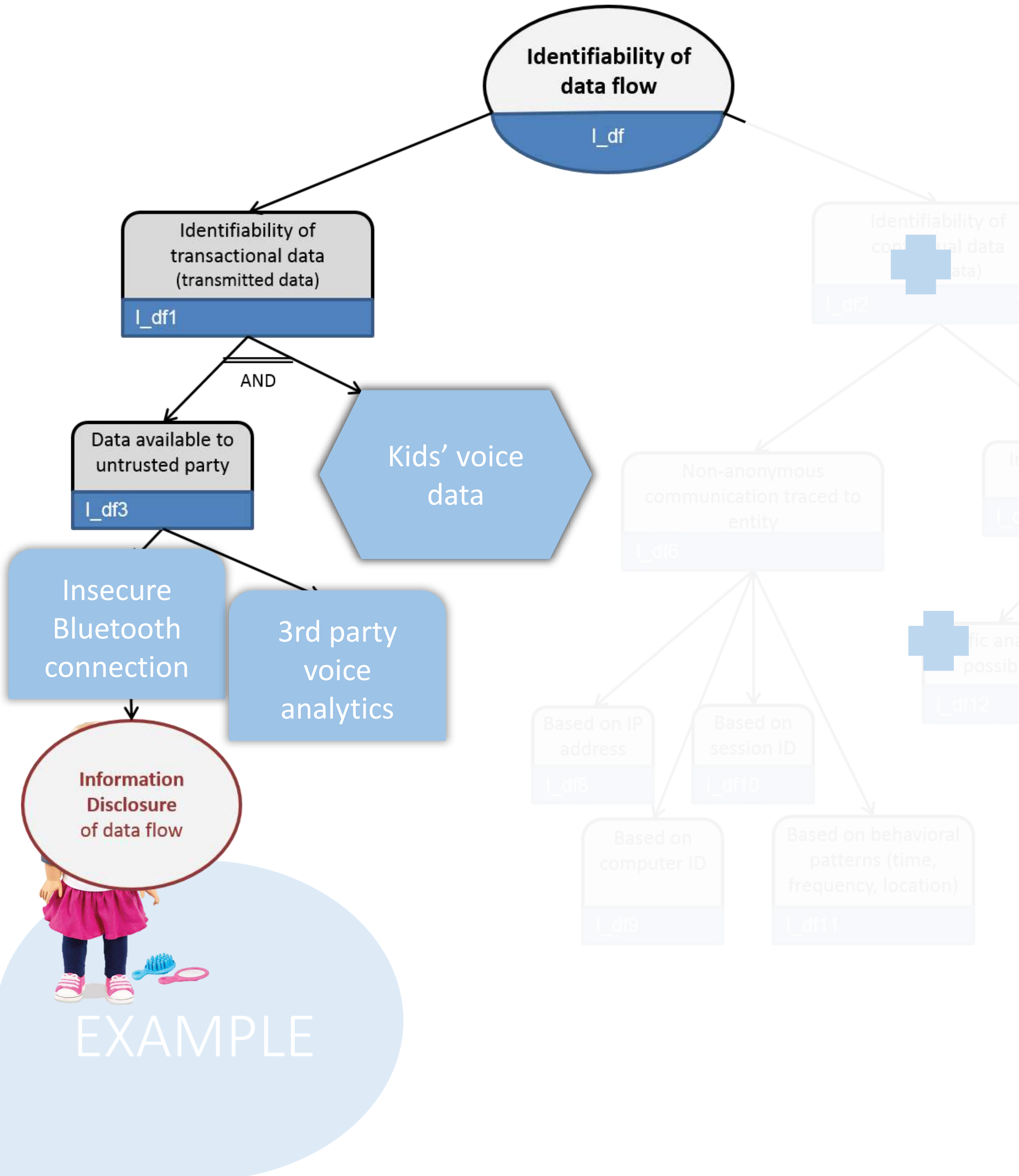
- Reflect & repeat

1. MODEL THE SYSTEM

2. ELICIT THREATS

3. MITIGATE THREATS

4. REFLECT



Identifiability of data flow
I_df
Identifiability of transactional data (transmitted data)
I_df1
AND
Data available to untrusted party
I_df3
Kids' voice data
Insecure Bluetooth connection
3rd party voice analytics
Information Disclosure of data flow
Non-anonymous communication traced to entity
I_df6
Based on IP address
I_df8
Based on session ID
I_df10
Based on computer ID
I_df9
Based on behavioral patterns (time, frequency, location)
I_df11

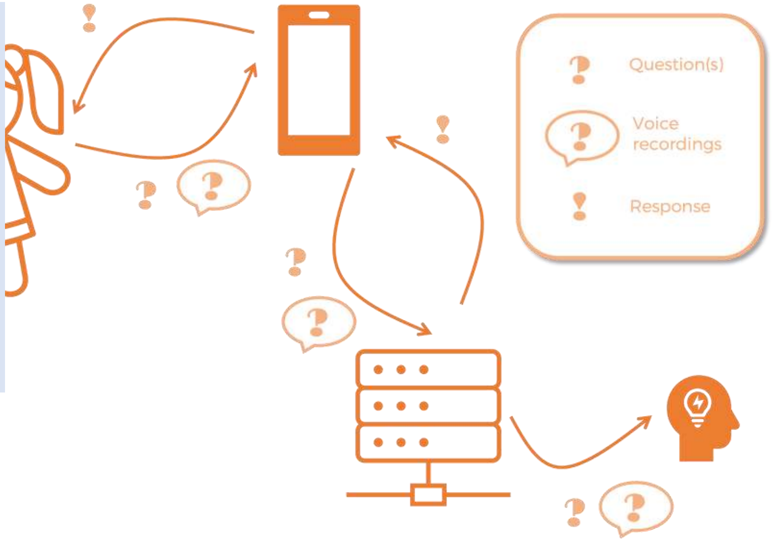
EXAMPLE

THREAT 01

Identifiable kids' voice data is being sent over an insecure communication channel

THREAT 02

Identifiable kids' voice data is being being shared with an untrusted 3rd party

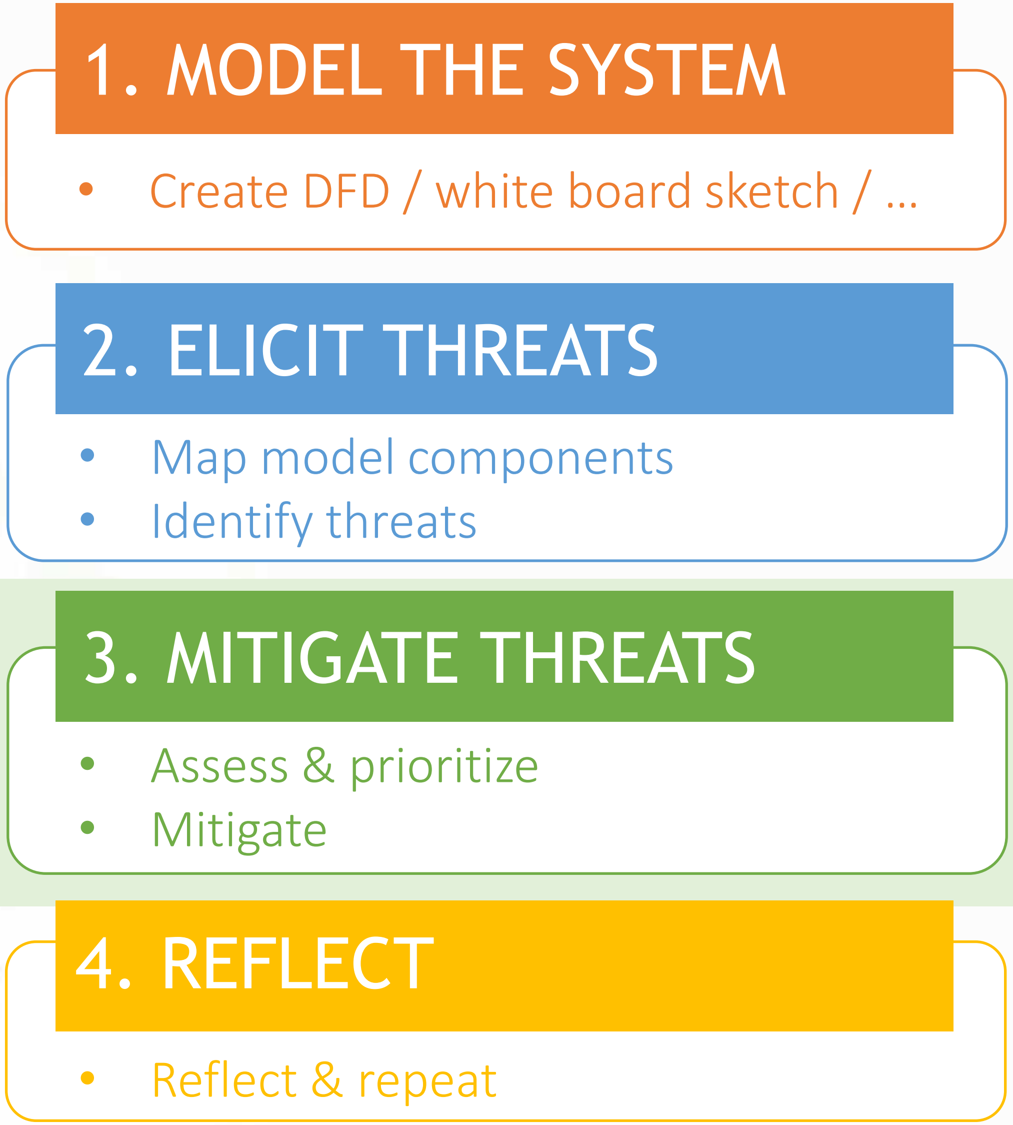


- Prioritize threats
  - assess risk (impact & likelihood)

- Mitigate threats
  - Tactics & strategies
  - Privacy patterns
  - PETs

THEN WHAT?

PROCESS



1. MODEL THE SYSTEM

- Create DFD / white board sketch / ...

2. ELICIT THREATS

- Map model components
- Identify threats

3. MITIGATE THREATS

- Assess & prioritize
- Mitigate

4. REFLECT

- Reflect & repeat

1. MODEL THE SYSTEM

2. ELICIT THREATS

3. MITIGATE THREATS

4. REFLECT

THREAT 01

Identifiable kids’ voice data is being sent over an insecure communication channel

THREAT 02

Identifiable kids’ voice data is being shared with an untrusted 3rd party

Before sharing

- **Hide** – Restrict access. Secure communication between doll and phone.
- **Separate** – Distribute processing. Local speech to text translation (no sharing of voice to the back-end).

When shared to back-end

- **Abstract** – summarize/group/perturb recordings. When share to external party, aggregate data, scramble recordings, etc.
- **Minimize** – select/exclude/strip/destroy data. Don’t store recordings. Delete once speech is translated to text. Don’t link questions to user profiles.

EXAMPLE

Strategies and tactics from:
Jaap-Henk Hoepman, Privacy design strategies (little blue book) https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf

PROCESS

1. MODEL THE SYSTEM

- Create DFD / white board sketch / …

2. ELICIT THREATS

- Map model components
- Identify threats

3. MITIGATE THREATS

- Assess & prioritize
- Mitigate

4. REFLECT

- Reflect & repeat

DID I DO A GOOD ENOUGH JOB?

HOW TO DO THREAT MODELING?

SUCCESSFULLY

USE SUCCESSFULLY FIELD-TESTED TECHNIQUES
ALIGNED TO LOCAL NEEDS,
THAT ARE INFORMED BY THE LATEST THINKING
ON THE BENEFITS AND LIMITS OF THOSE
TECHNIQUES.

USEFUL RESOURCES

- *Threat modeling. Designing for security.* By Adam Shostack, 2014.
- *Threat Modeling – A Practical Guide for Development Teams* by Izar Tarandach & Matthew J. Coles, 2020
- *Securing systems. Applied security architectures and threat models* by Brook Schoenfield, 2015.
- Threat Modeling Manifesto *www.threatmodelingmanifesto.org*
- Threat Modeling Connect community *www.threatmodelingconnect.com*

THREAT MODELING APPROACHES

- **STRIDE**
- **LINDDUN** PRIVACY

Tool support

- OWASP Threat Dragon
- SPARTA (DistriNet)

- EoP
- PASTA
- TRIKE
- TARA
- Continuous Threat Modeling

- INCLUDES NO DIRT PRIVACY
- PLOT4AI PRIVACY
- TRIM PRIVACY
- STRIPED PRIVACY

https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/

A TASTE OF PRIVACY THREAT MODELING

TRY DIFFERENT FLAVORS

TO DECIDE WHAT YOU LIKE BEST

AVOID A BRAIN FREEZE

DON’T GET GREEDY

A Taste of Privacy Threat Modeling

Kim Wuyts

@wuytski

@kimw@mastodon.social