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

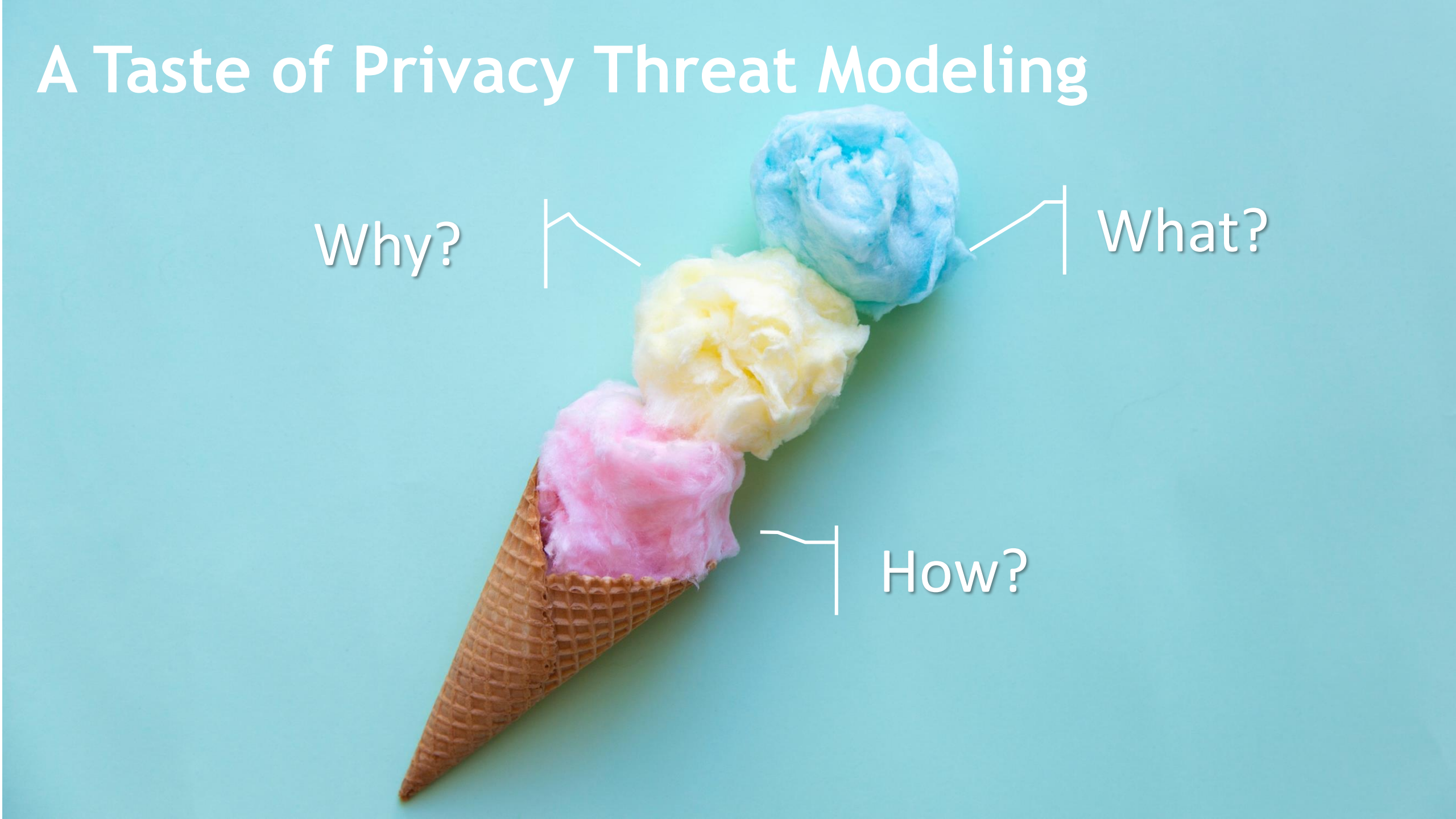
Kim.Wuyts@kuleuven.be

@wuytski

@kimw@mastodon.social

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

A Taste of Privacy Threat Modeling




PRIVACY

WHY PRIVACY MATTERS?

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

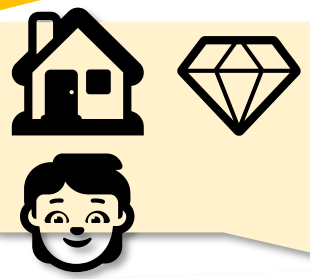
MISCONCEPTION

WHY PRIVACY MATTERS?

WHY PRIVACY MATTERS?

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

MISCONCEPTION



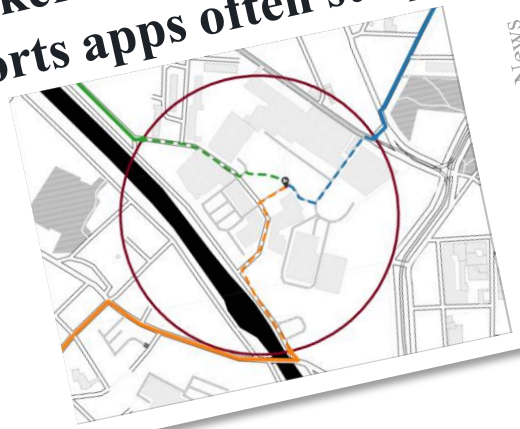
Roomba testers feel misled after intimate images ended up on Facebook

...ology review

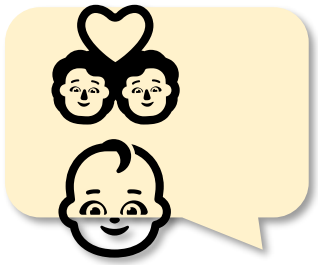
Tesla workers shared images from car cameras, including "scenes of intimacy"

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!

INTERVENABILITY
MANAGEABILITY

TRANSPARENCY
PREDICTABILITY

UNLINKABILITY
DISASSOCIABILITY

PRIVACY ENGINEERING

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

DETECTING

Deducing the involvement of an individual through observation.

NON-REPUDIATION

Being able to attribute a claim to an individual.

DATA DISCLOSURE

Excessively collecting, storing, processing or sharing personal data.

IDENTIFYING

Learning the identity of an individual.

UNAWARENESS & UNINTERVENABILITY

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

LINKING

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

NON-COMPLIANCE

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

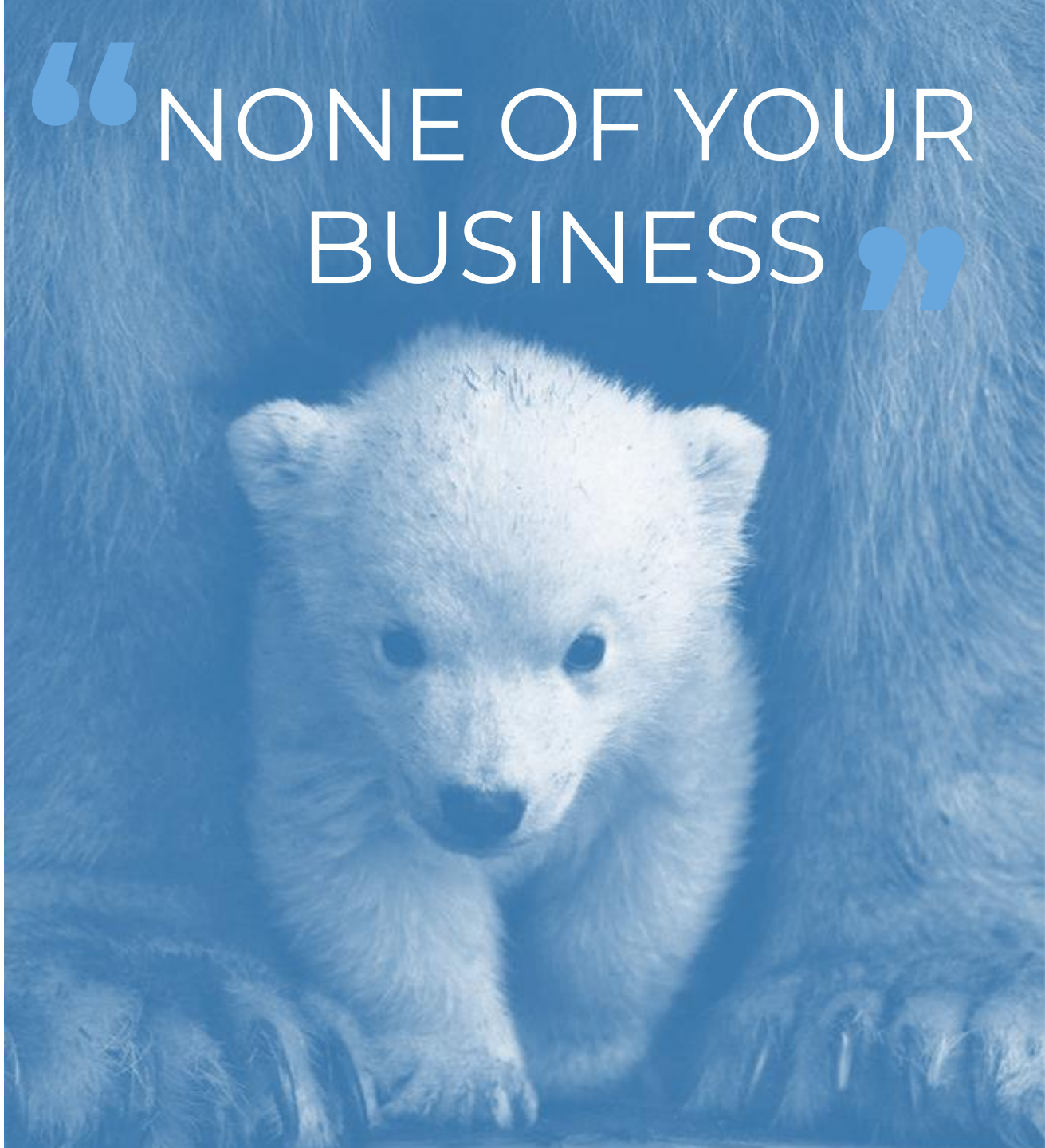
DATA DISCLOSURE

UNNECESSARY USE

OF DATA

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

- collection
- storage
- processing
- sharing



LINKING

PLAYING “GUESS WHO”

Linking multiple properties to
the same individual

vs.

IDENTIFYING

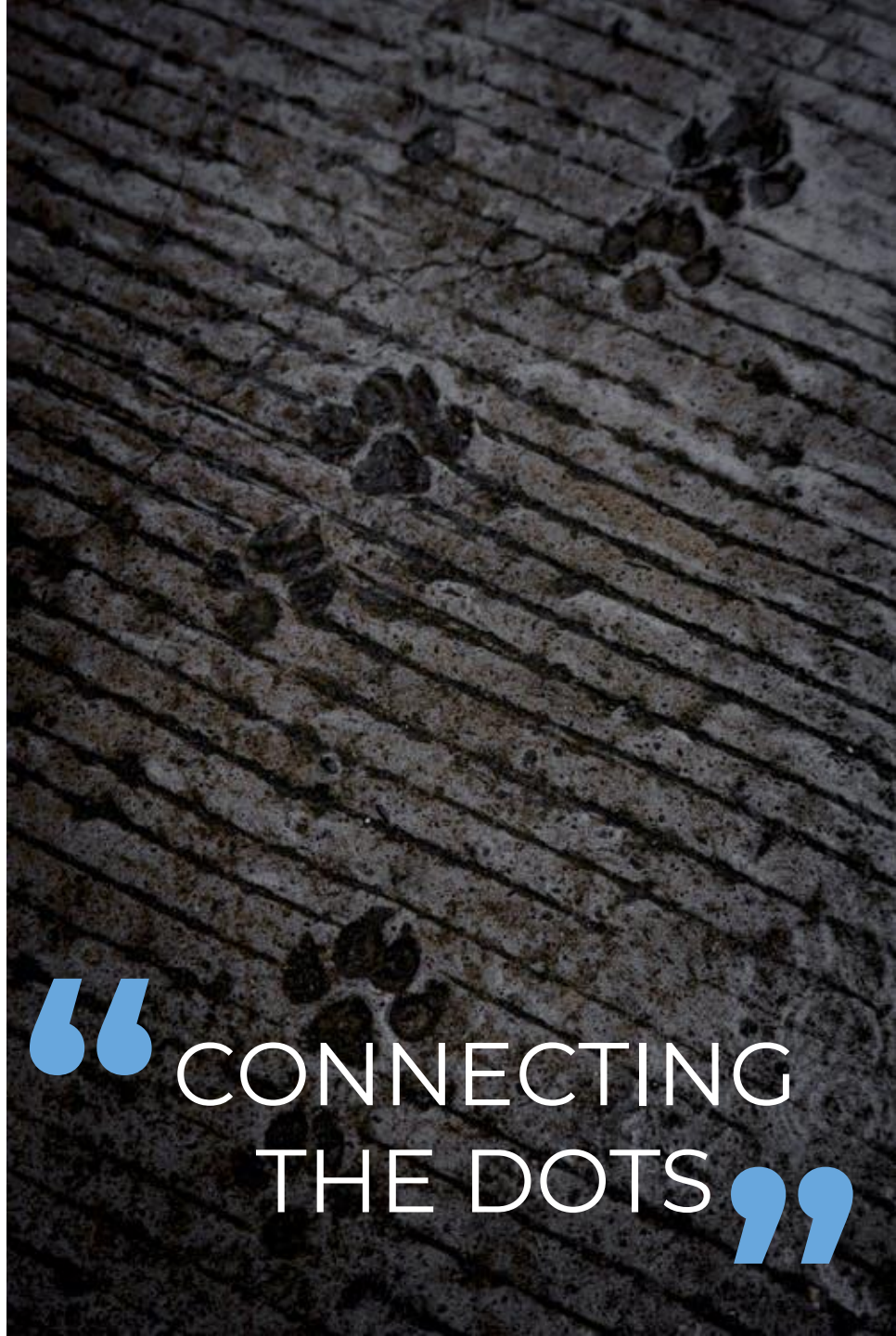
WINNING “GUESS WHO”

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



IDENTIFYING

LEARNING

THE IDENTITY

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

DETECTING

DEDUCING SUBJECT INVOLVEMENT BY OBSERVING EXISTENCE OF RELEVANT INFORMATION

- Observed communication
- Application side-effects
- System responses

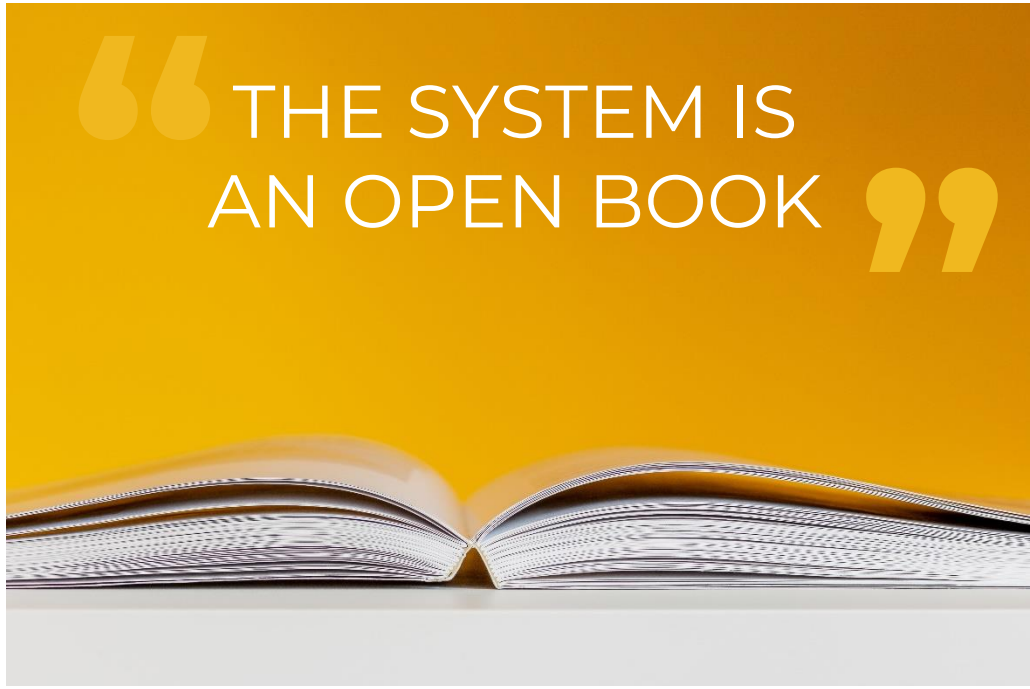
NON-REPUDIATION

PROOF OF A CLAIM ABOUT AN INDIVIDUAL

- Evidence of the claim / action
- Attribution 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

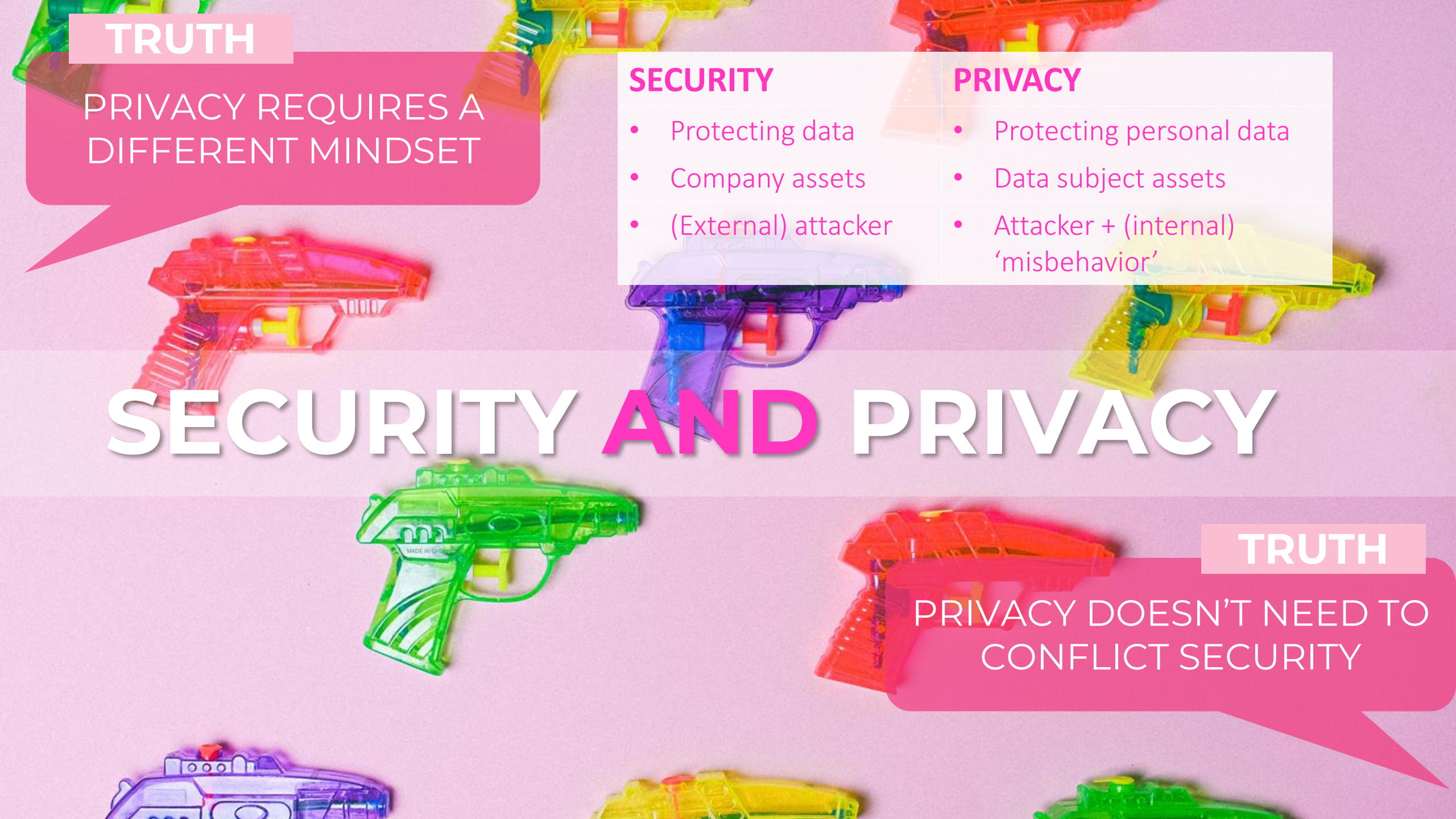
- Lack of preferences control
- Lack of access
- Lack of rectification/erasure

NON-COMPLIANCE

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

4

- Lawfulness
- Data lifecycle management
- Cybersecurity risk management



TRUTH

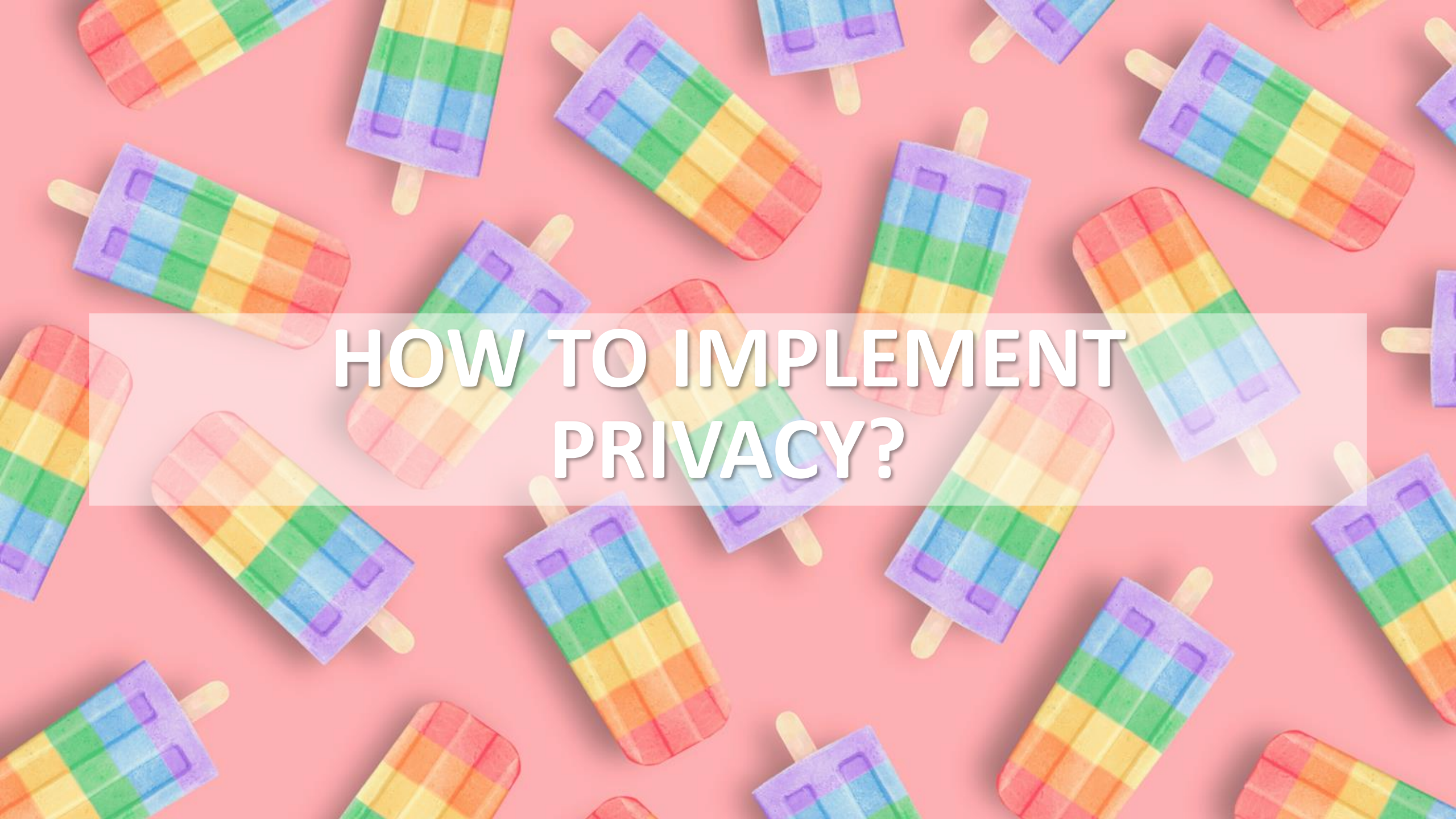
PRIVACY REQUIRES A DIFFERENT MINDSET

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

SECURITY AND PRIVACY

TRUTH

PRIVACY DOESN’T NEED TO CONFLICT SECURITY


HOW TO IMPLEMENT
PRIVACY?

HOW TO IMPLEMENT PRIVACY?

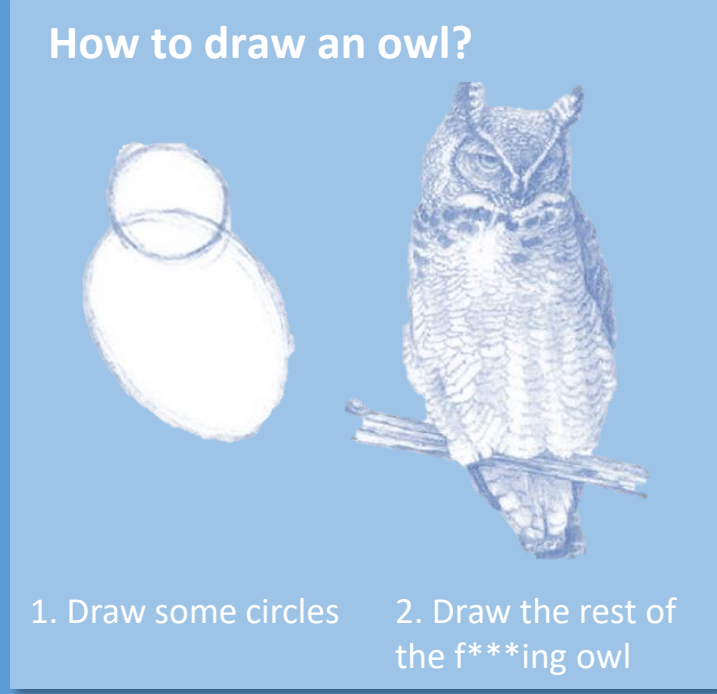
PRIVACY BY DESIGN

Tackled **proactively**

Systematically analyzed

Integrated in the development lifecycle

Have an **impact on design** decisions



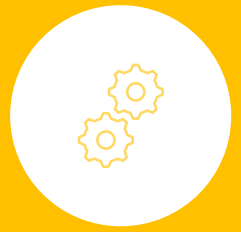
WHAT IS THREAT MODELING?

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

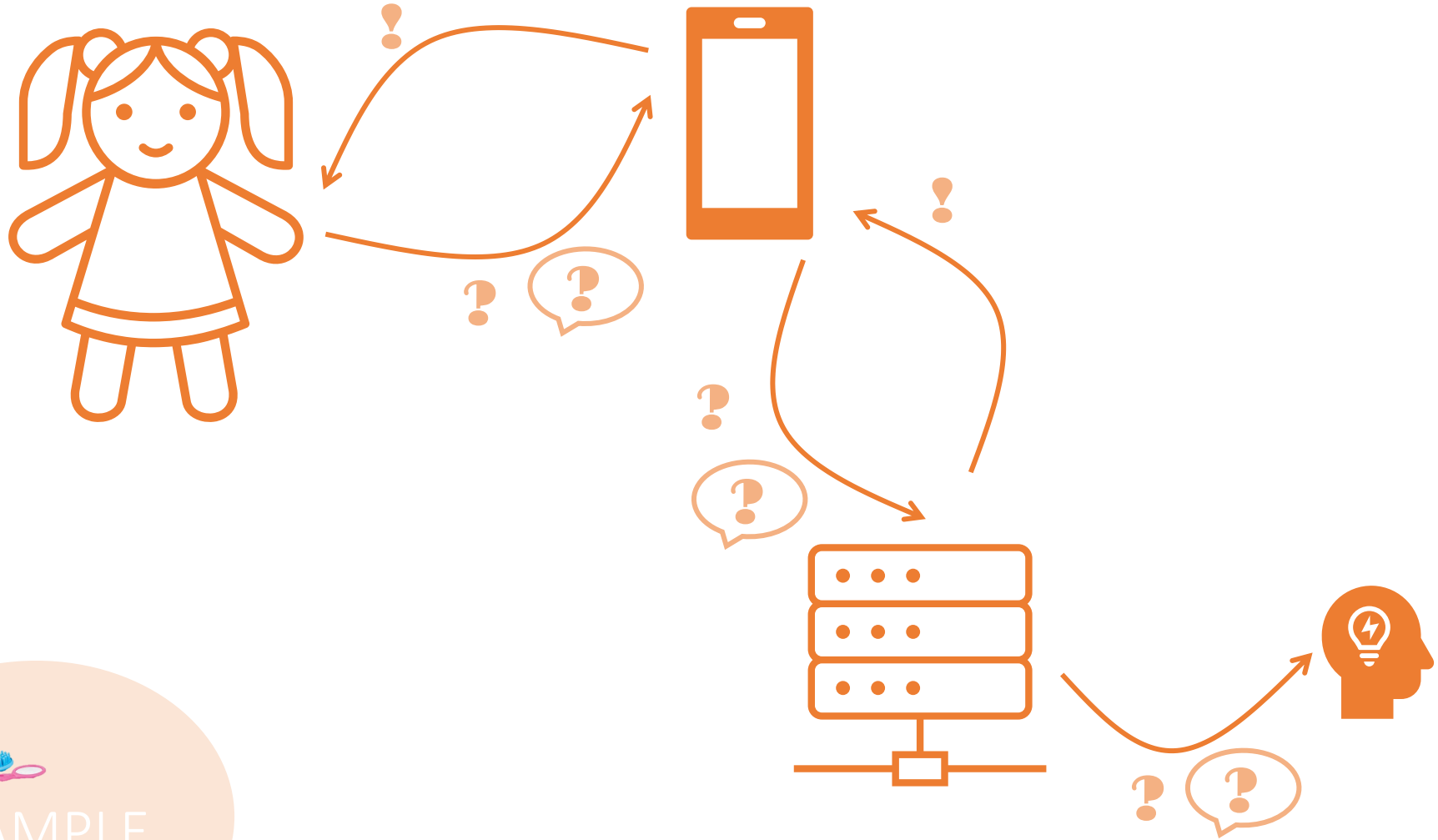
- Reflect & repeat

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

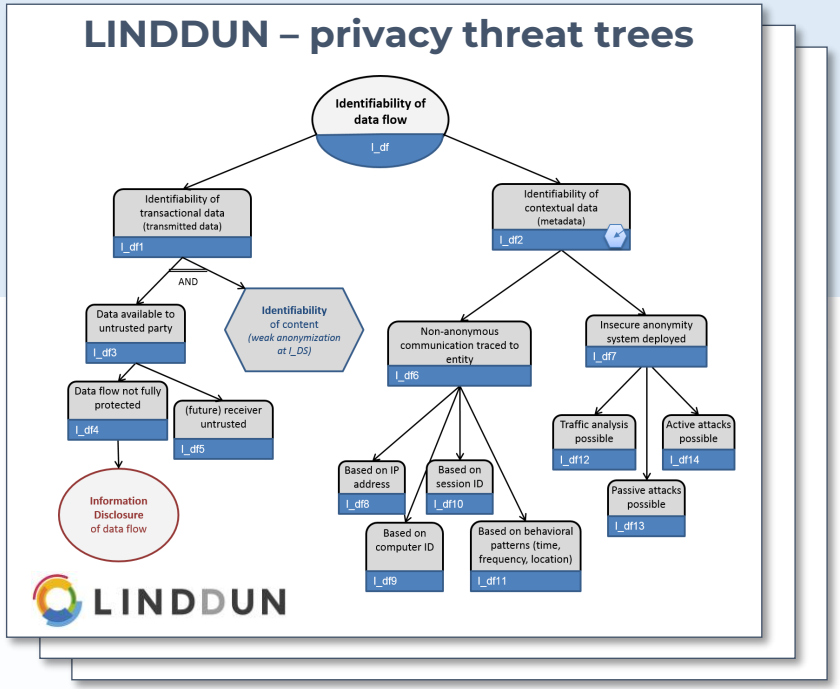
3. MITIGATE THREATS

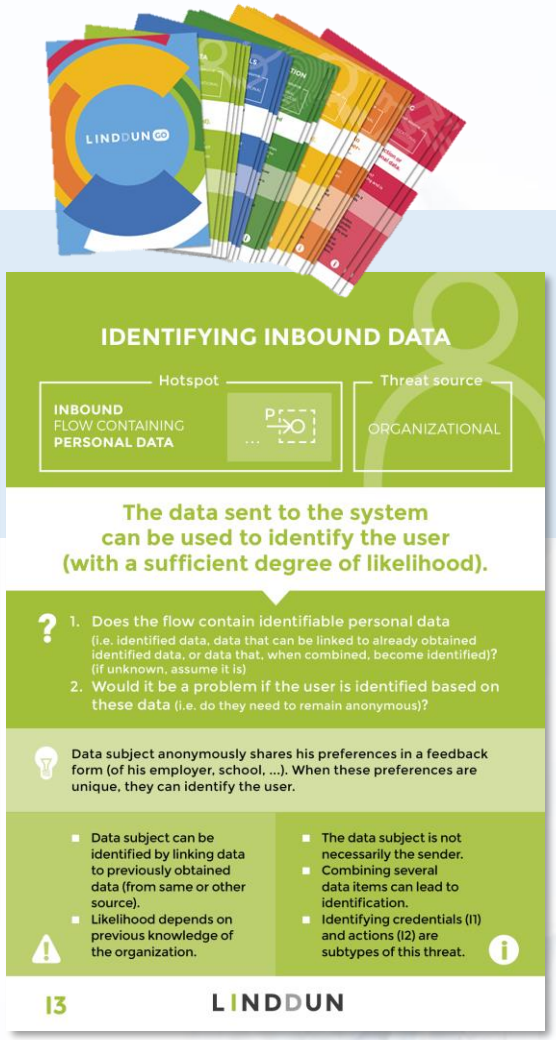
- Assess & prioritize
- Mitigate

4. REFLECT

- Reflect & repeat

REUSABLE KNOWLEDGE





LINDDUN GO cards

WWW.LINDDUN.ORG

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

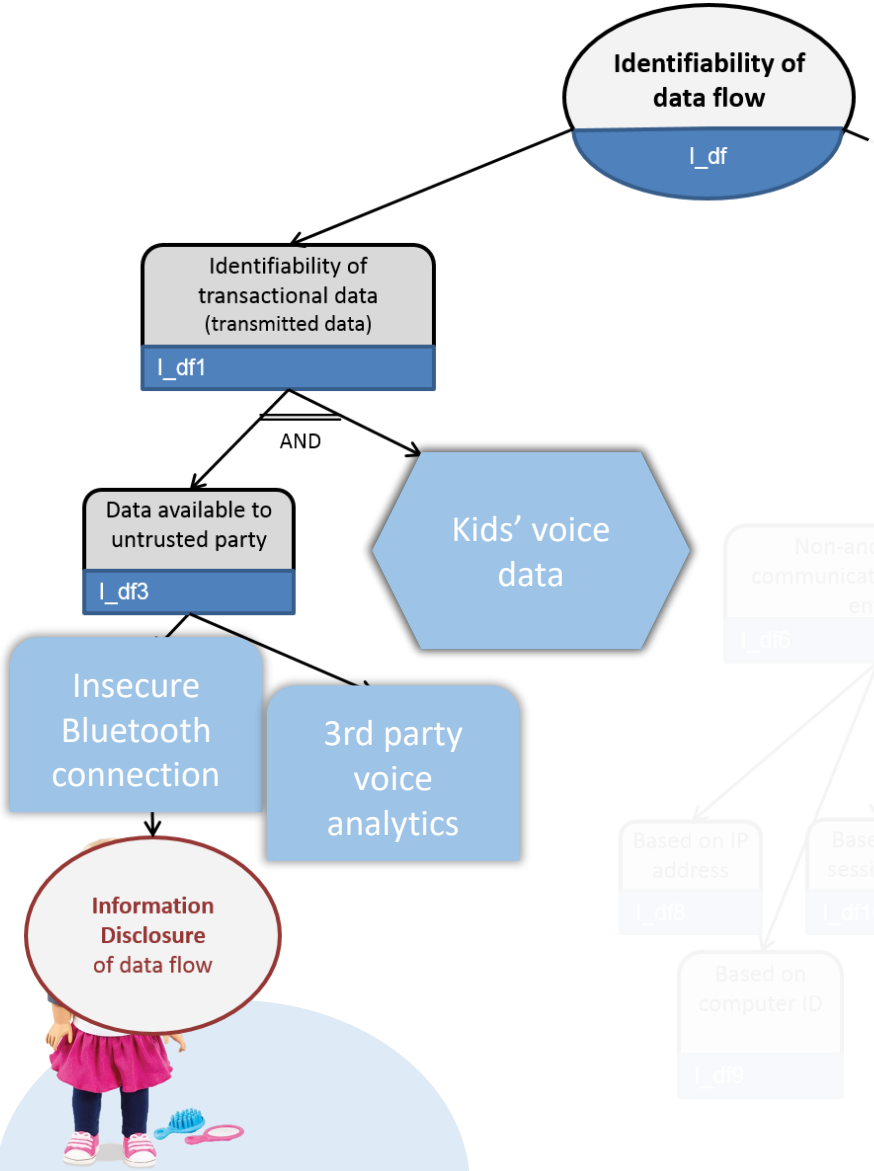
- Reflect & repeat

1. MODEL THE SYSTEM

2. ELICIT THREATS

3. MITIGATE THREATS

4. REFLECT



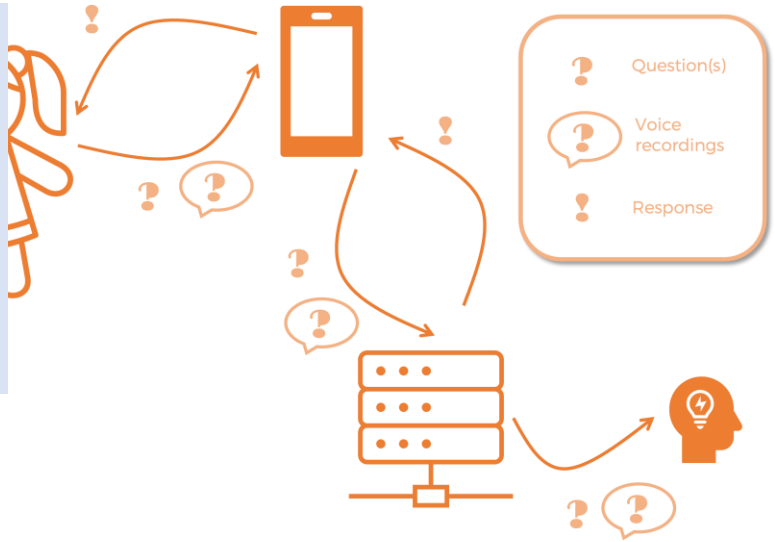
EXAMPLE

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



- 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

EXAMPLE

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.

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

DID I DO A GOOD ENOUGH JOB?

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

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

AVOID A BRAIN FREEZE

DON’T GET GREEDY

TRY DIFFERENT FLAVORS

TO DECIDE WHAT YOU LIKE BEST

A Taste of Privacy Threat Modeling

Kim Wuyts

@wuytski

@kimw@mastodon.social