

A close-up photograph of a metal tray filled with various flavors of soft-serve ice cream. The colors include yellow, blue, orange, and light green. Each flavor has a small wooden stick or spatula sticking out of it. The background is slightly blurred, showing more of the ice cream display.

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

TOO MUCH TO FINISH

STARTS EATING THE CONE



DOESN'T LIKE THE FLAVOR

IT STARTS MELTING AND MAKE A MESS

3. WHAT TO DO ABOUT IT?



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](https://twitter.com/wuytski)

 [@kimw@mastodon.social](https://mstdn.social/@kimw)

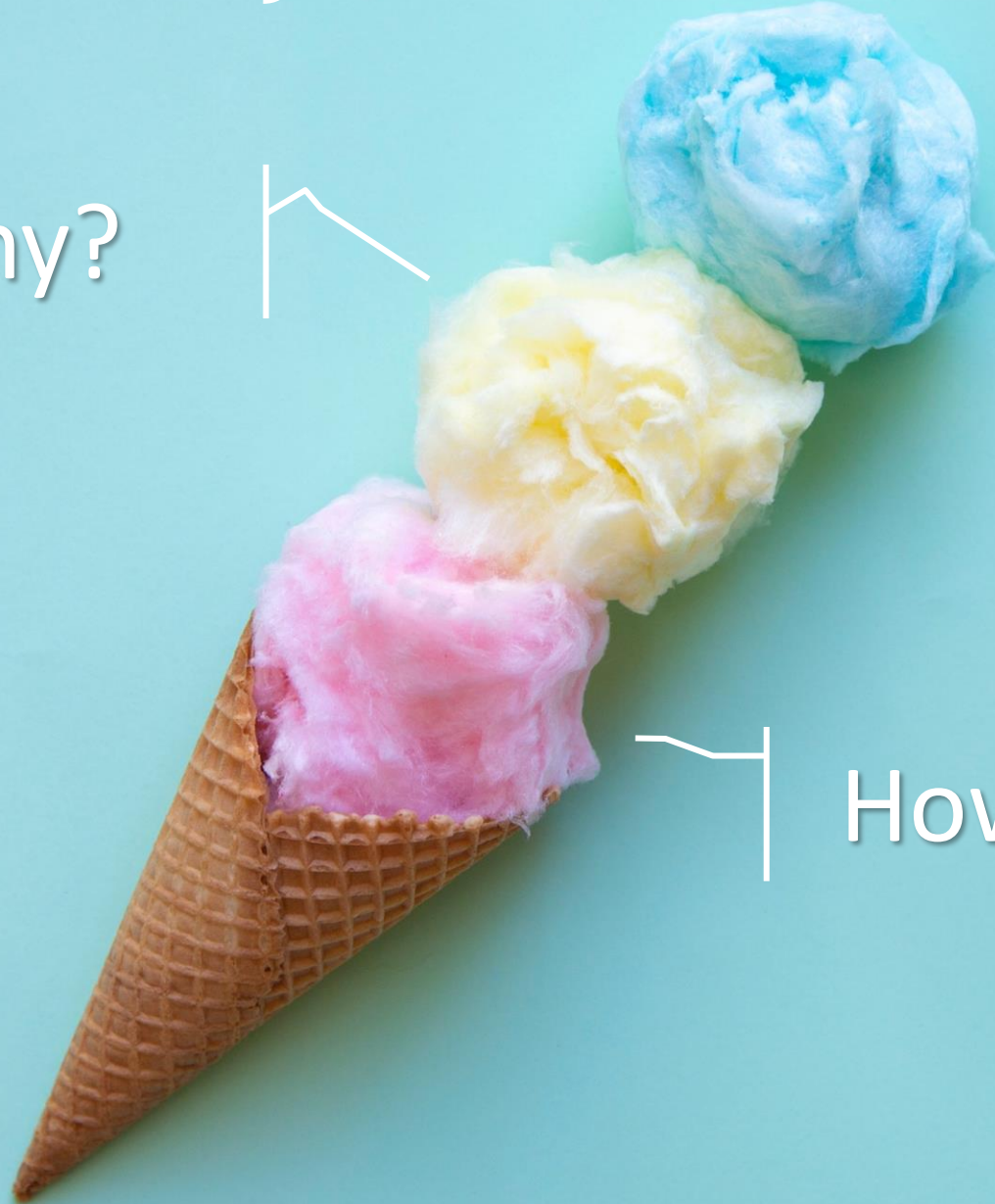
 <https://www.linkedin.com/in/kwuyts/>

A Taste of Privacy Threat Modeling

Why?

What?

How?



A background of numerous rainbow-striped popsicles scattered across a light pink surface. The popsicles are arranged in a dense, overlapping pattern, with some showing the wooden sticks. The colors of the stripes are purple, blue, green, yellow, orange, and red.

PRIVACY

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

MISCONCEPTION

WHY PRIVACY MATTERS?

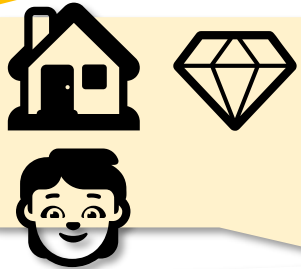
```
1001 01110
010110 011001
110101 101010
1001 01110

11101010 10101010
01111001011 10001110010
100010110001 101011001111
001110101001010101010111
0101110010110010001110010
110001011001100110011110
10011101010101 0101 1010101110
0101110010 1001 0011100101
110010110 0110 10110011 10010
101110101 10001010101 10001100
01110010 00011100110 1100
001 10 0101100111 01 101
111 01 1010101011 10100
111 10 00 100 111001
001 10 01 011 010110
111 01 10 101 01000
111 10 00 100 11001
001 10 01 011 011
111 01 10 101 0110
```

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

MISCONCEPTION

WHY PRIVACY MATTERS?



Roomba testers feel misled
after intimate images ended
up on Facebook

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

Ars Technica, April 2023

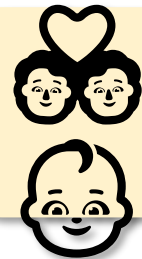
Technology review



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

DETECTING

Deducing the involvement of an individual through observation.

DATA DISCLOSURE

Excessively collecting, storing, processing or sharing personal data.

UNAWAWARENESS & 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.

NON-REPUDIATION

Being able to attribute a claim to an individual.

IDENTIFYING

Learning the identity of an individual.

LINKING

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



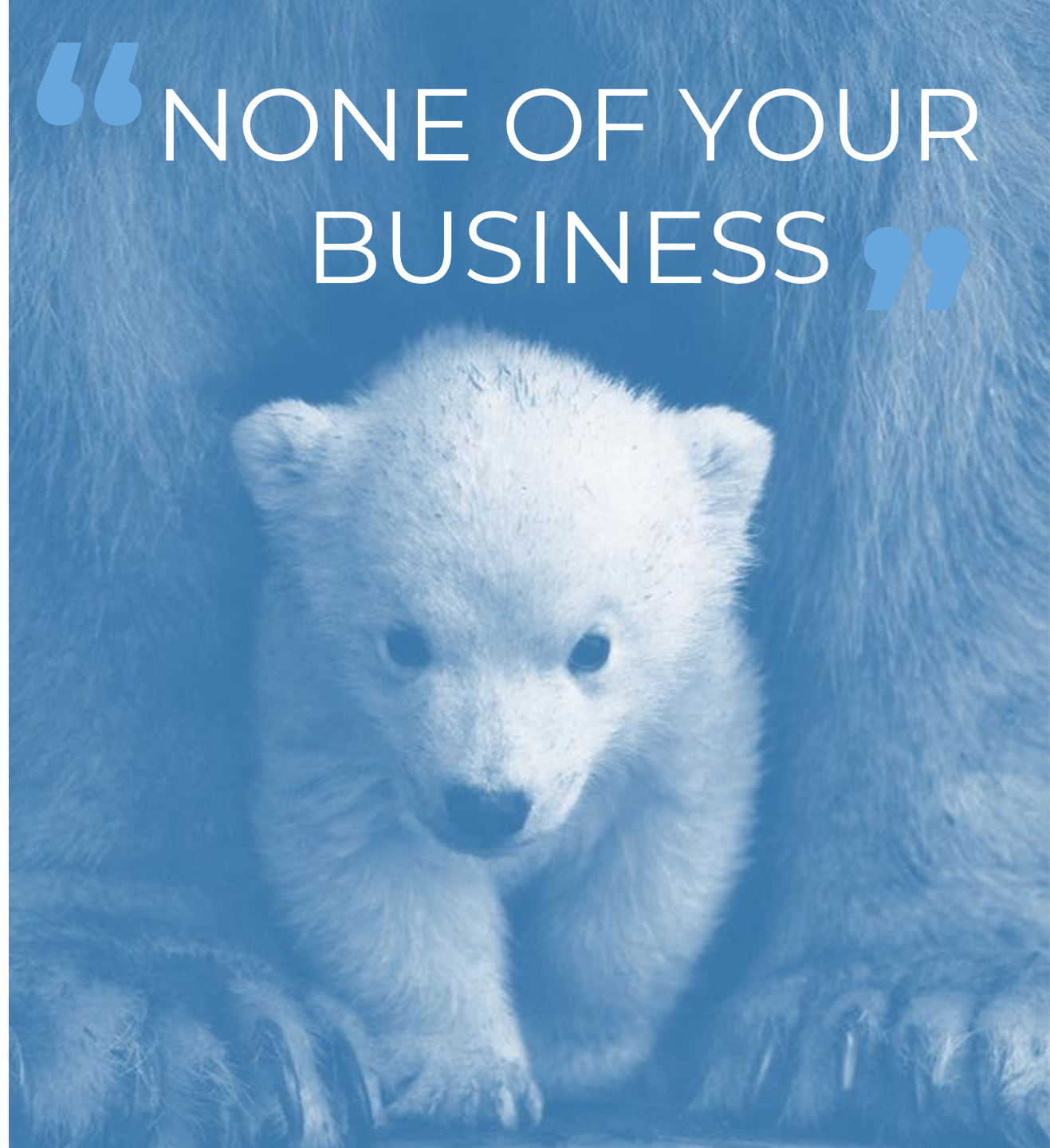
DATA DISCLOSURE

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

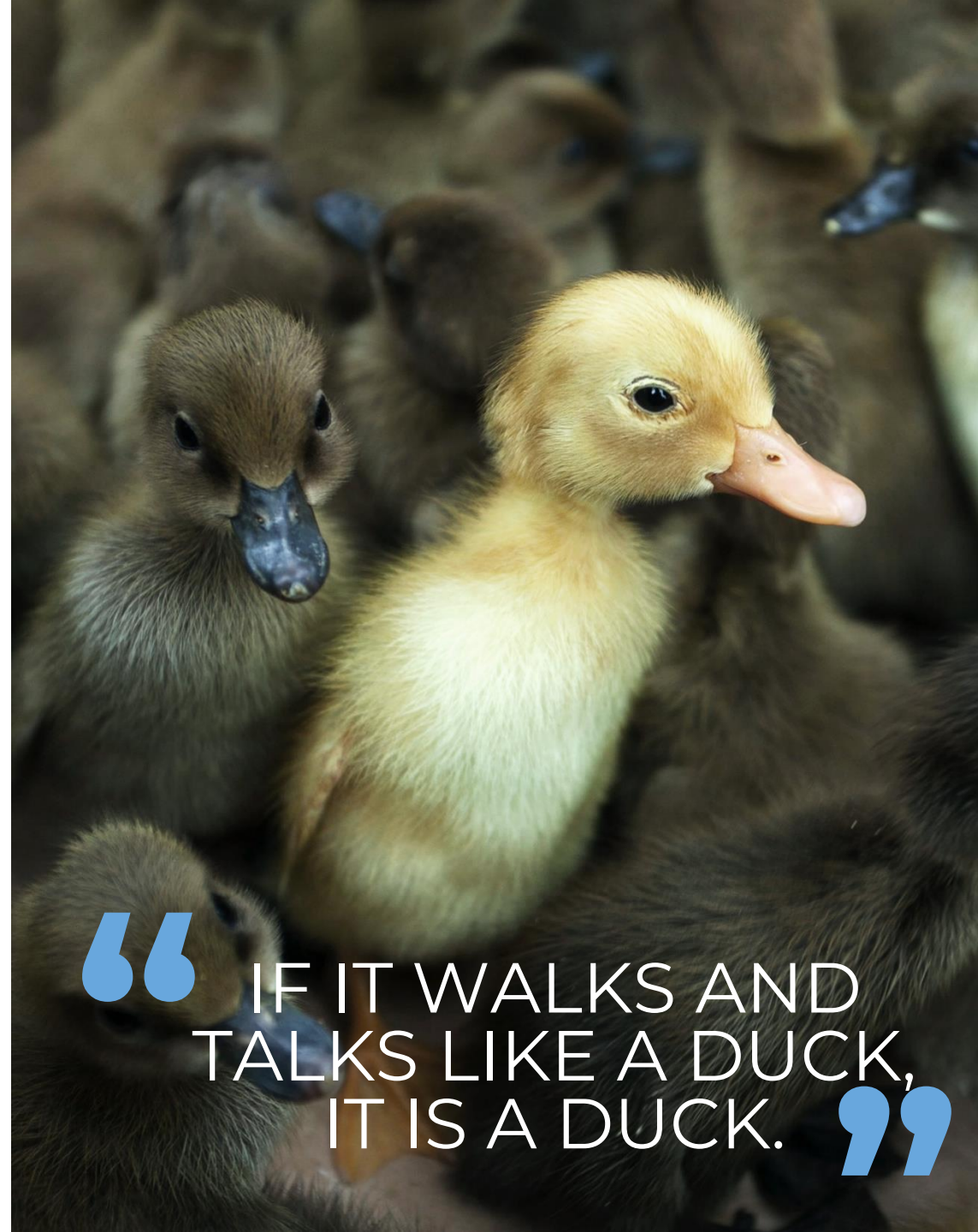
- Through identifiers
- Through combination
- Through profiling/derivation/inference

“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 ”

TRUTH

PRIVACY REQUIRES A DIFFERENT MINDSET

SECURITY

- Protecting data
- Company assets
- (External) attacker

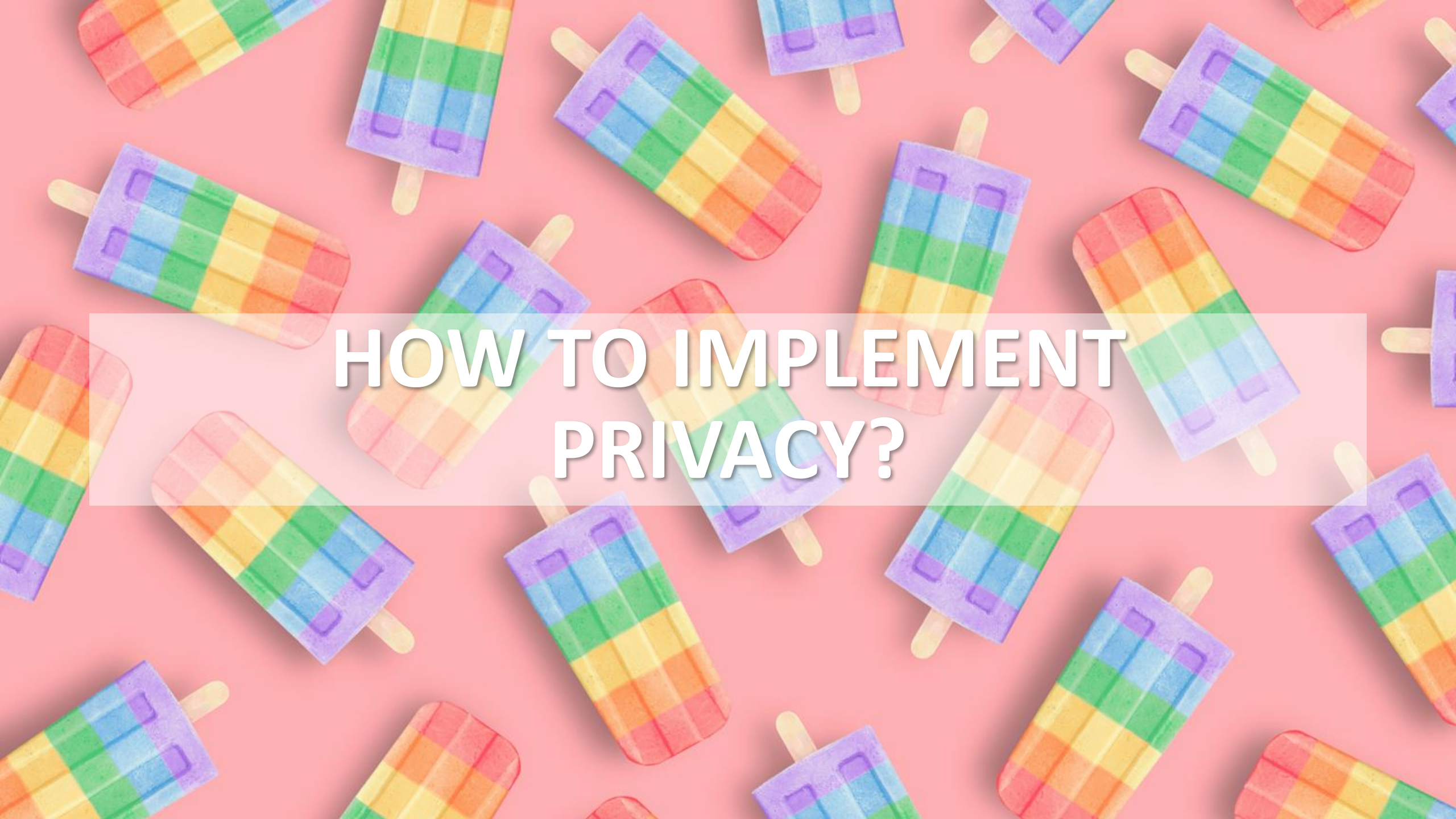
PRIVACY

- Protecting personal data
- Data subject assets
- Attacker + (internal) 'misbehavior'

SECURITY AND PRIVACY

TRUTH

PRIVACY DOESN'T NEED TO CONFLICT SECURITY

A background of numerous rainbow-striped popsicles scattered across a light pink surface. The popsicles are arranged in various orientations, creating a vibrant and playful pattern. The colors of the stripes include purple, blue, green, yellow, orange, and red.

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

How to draw an owl?



1. Draw some circles

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

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

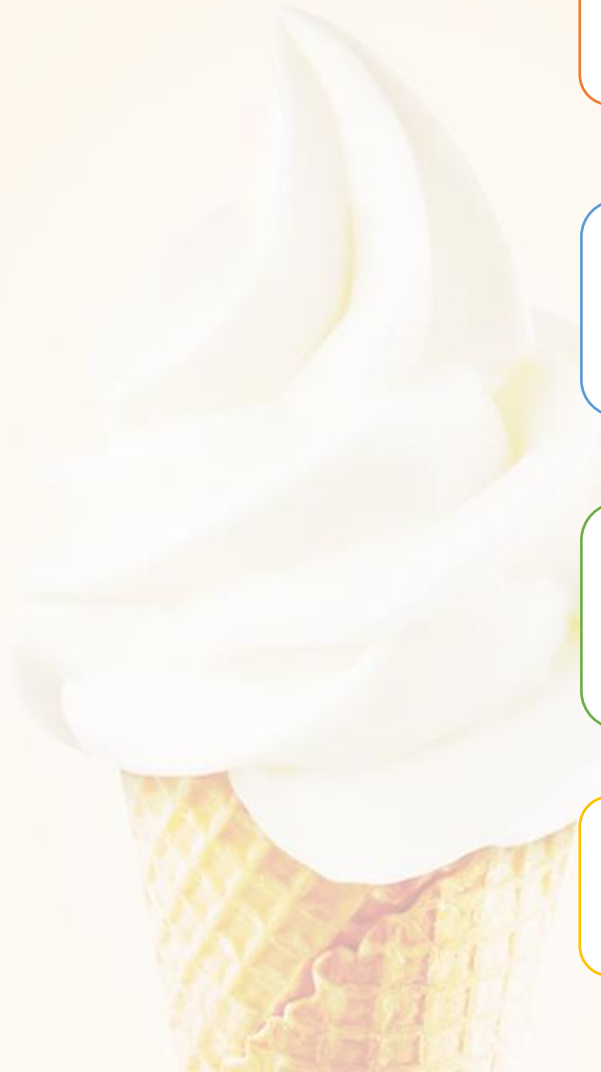


Have an **impact** on
design decisions

The background features a repeating pattern of bright red chili peppers on a vibrant green surface. A semi-transparent white rectangular box is centered over the image, containing the text "Threat modeling is HOT". The word "Threat modeling" is in green, "is" is in green, and "HOT" is in red. Below the text, a red line graph with a jagged, upward-trending path is visible.

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

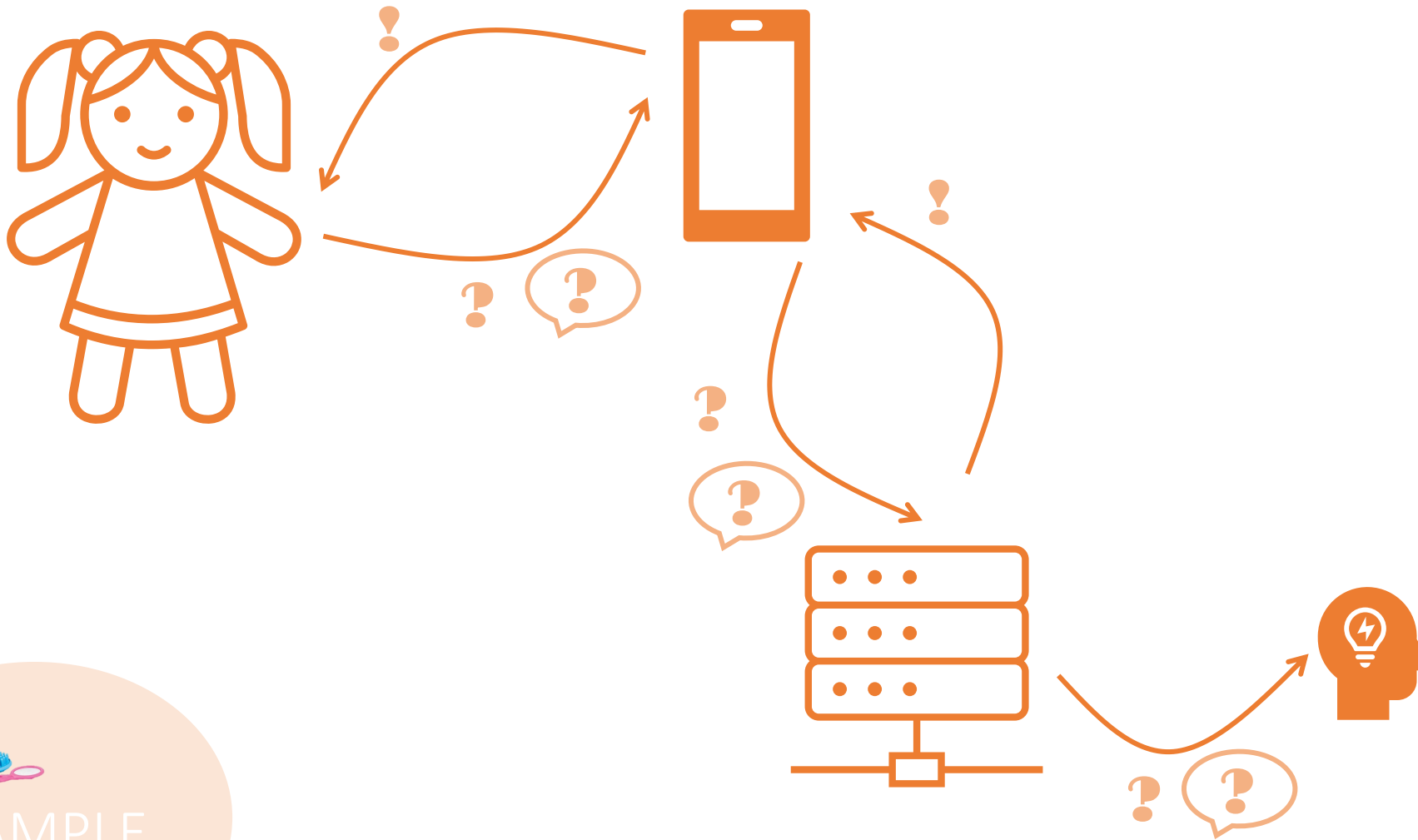
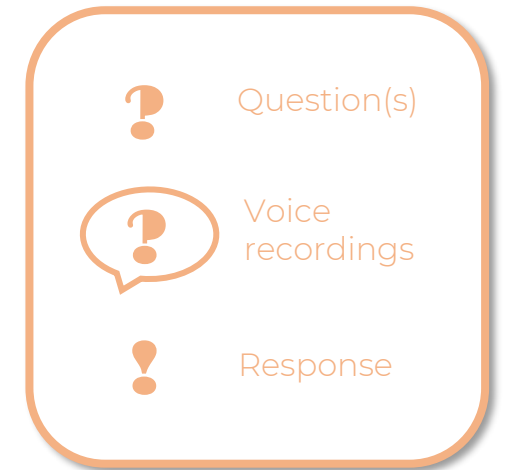


1. MODEL THE SYSTEM

2. ELICIT THREATS

3. MITIGATE THREATS

4. REFLECT



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

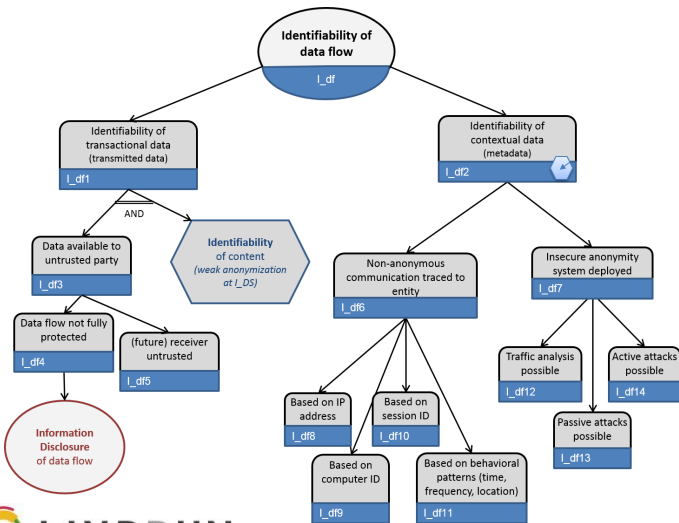
- Reflect & repeat

REUSABLE KNOWLEDGE

PROCESS



LINDDUN – privacy threat trees



IDENTIFYING INBOUND DATA



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

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

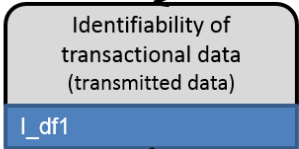
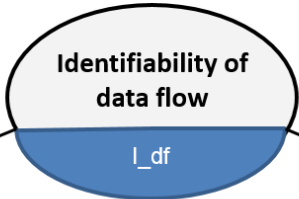
- Reflect & repeat

1. MODEL THE SYSTEM

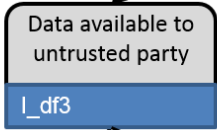
2. ELICIT THREATS

3. MITIGATE THREATS

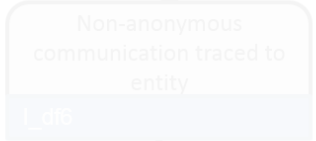
4. REFLECT



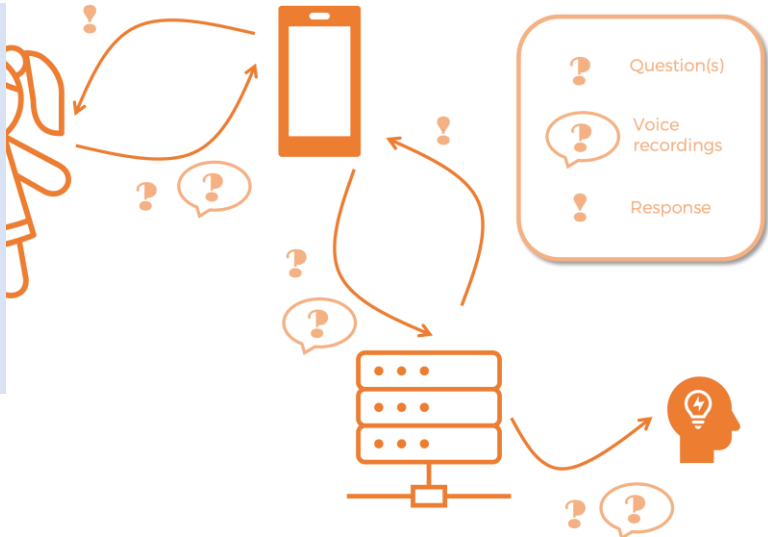
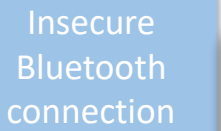
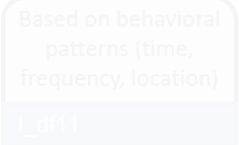
AND



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

CAN WE FIX IT?
YES, WE CAN!



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 background of numerous rainbow-colored popsicles scattered across a light pink surface. The popsicles are arranged in a dense, overlapping pattern, with some showing the wooden sticks. The colors of the popsicles transition from purple at the top to red at the bottom, following the rainbow spectrum.

A TASTE OF PRIVACY THREAT MODELING

AVOID A BRAIN FREEZE

**DON'T GET
GREEDY**



**TRY DIFFERENT FLAVORS
TO DECIDE WHAT YOU LIKE BEST**

A close-up photograph of a metal display case filled with various flavors of soft-serve ice cream. The flavors include yellow, blue, orange, and light green. Each flavor is served in a white plastic cup with a wooden stick. The background is slightly blurred, showing more of the display case.

A Taste of Privacy Threat Modeling

Kim Wuyts



@wuytski



@kimw@mastodon.social