
THREAT MODELING
CONNECT
THREAT MODCON 2023
THREAT MODELING IS FOR EVERYONE

THREAT MODCON 2023

Shifting Privacy In

The one where privacy and security become F·R·I·E·N·D·S

Kim Wuyts

@wuytski

@kimw@mastodon.social

Kim Wuyts

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

- Has ***PhD in privacy engineering***
- Was ***Senior Researcher at DistriNet, KU Leuven, Belgium***

Kim.Wuyts@kuleuven.be

@wuytski

@kimw@mastodon.social

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

THREAT MODCON 2023

What to take away?

- Privacy is important
- Threat modeling can be used to implement privacy
- Privacy and security threat modeling are F·R·I·E·N·D·S
  - They strengthen each other
  - They require different mindsets
  - Combined analysis is more efficient than separate

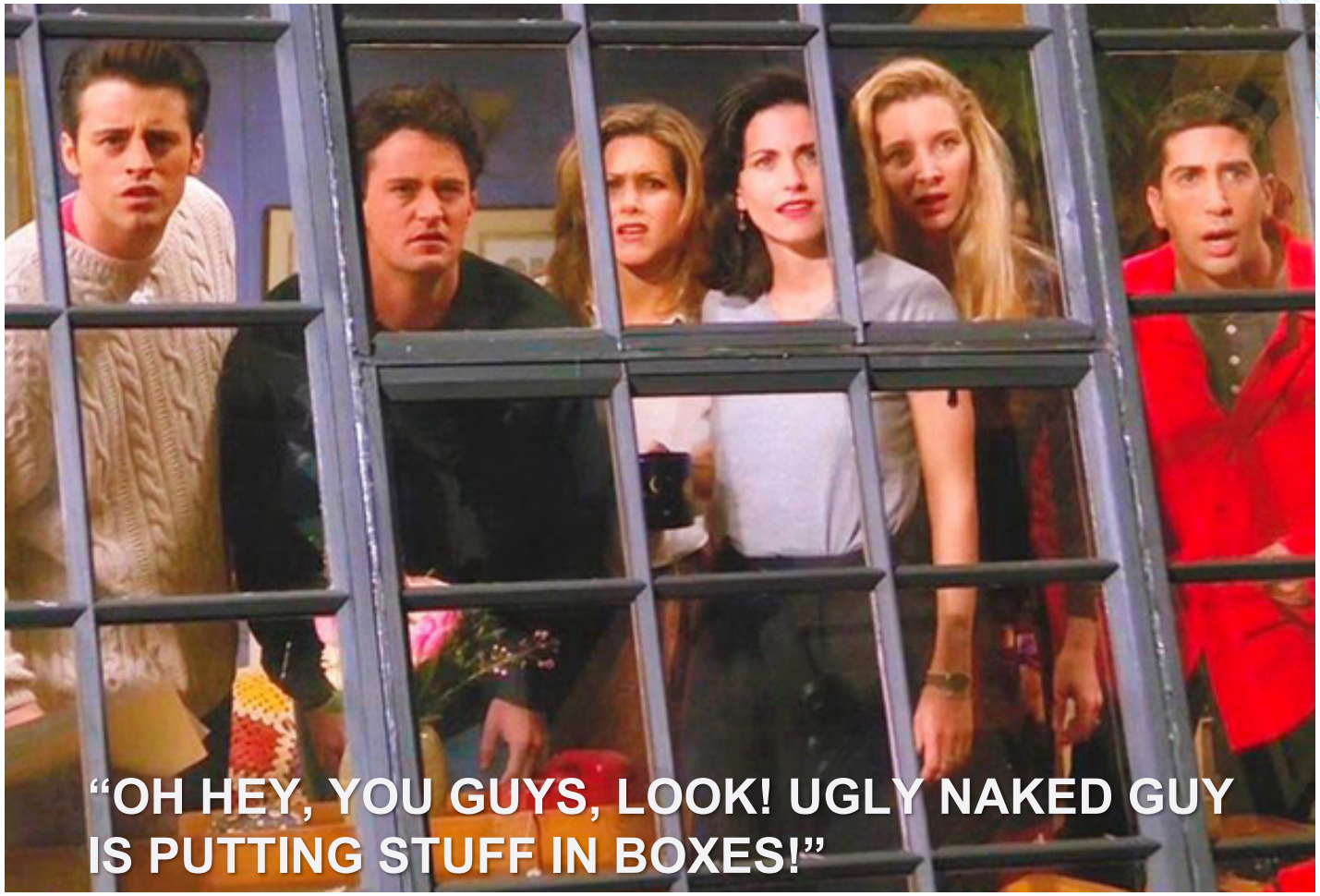
THREAT MODCON 2023

Privacy

It matters!

THREAT MODCON 2023

Privacy matters



© Friends, NBC

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

Ars Technica, April 2023

What your car (company) can collect about you

- Name
- Address
- Phone number
- Email
- Date of birth
- your credit card number social security number
- Driving habit and style
- Use of accelerator
- Location history
- Marital status
- Race
- Education
- Medical information
- Health insurance information
- genetic information
- Facial templates
- Keystroke
- Physical or mental disability
- Voiceprints
- audio recordings of vehicle occupants
- Pictures
- Iris or retina scans
- Gait
- Sleep data
- Sexual activity
- Religion or creed
- Philosophical beliefs
- …

Mozilla's Privacy Not Included study,Sept 2023

https://foundation.mozilla.org/en/privacynotincluded/articles/what-data-does-my-car-collect-about-me-and-where-does-it-go/

*Privacy Not Included

moz://a

THREAT MODCON 2023

WE NEED PRIVACY BY DESIGN!

THREAT MODCON 2023

But... we already do security

Align and integrate privacy in secure development lifecyle

THREAT MODCON 2023

Privacy

Not a synonym for security!

Privacy is NOT confidentiality

Unlinkability

Disassociability

Transparency

Predictability

Intervenability

Manageability

M. Hansen, M. Jensen and M. Rost, "Protection Goals for Privacy Engineering," 2015
NISTIR 8062 An Introduction to Privacy Engineering and Risk Management in Federal Systems, 2017

THREAT MODCON 2023

Unlinkability

- Can data items be tied together?
- What extra information could be extracted from this?

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

Researchers find smart meters could reveal favorite TV shows

Tests on smart meters made by German company Discovergy show that someone with network sniffing skills and equipment could determine what's been watched by looking at lighting display patterns.

Transparency and intervenability

THREAT MODCON 2023

WANT TO KNOW MORE?

We hope you will not read this part because when you click on this link you will sell us your soul.

YES!

SHOW ME THE COOL STUFF

No. I am a boring person

Security

AND

Privacy

THREAT MODCON 2023

Varied viewpoints

Diverse team for cross-functional collaboration 

Security strengthens privacy

Technical details & attacks

Asset-focused

Confidentiality is essential for privacy

Privacy strengthens security

Logical business flows

Data-centric & user-focused

Minimization to reduce breach impact

From Security Heroes vs. the Power of Privacy, by Avi D & Kim Wuyts, at Troopers 2023

THREAT MODCON 2023

Privacy

In Security Threat Modeling

What are we working on?

What could go wrong?

What are we going to do about it?

Did we do a good enough job?

What are we working on?

	Security	Privacy
Assets	Kinds of data, Storage technology	More fine-grained, Data purpose
Controls	Protocols, encryption authentication	Access control, consent flows, PETs
Actors	Users, roles, attackers	Individuals, outsiders, organization itself

From Security Heroes vs. the Power of Privacy, by Avi D & Kim Wuyts, at Troopers 2023

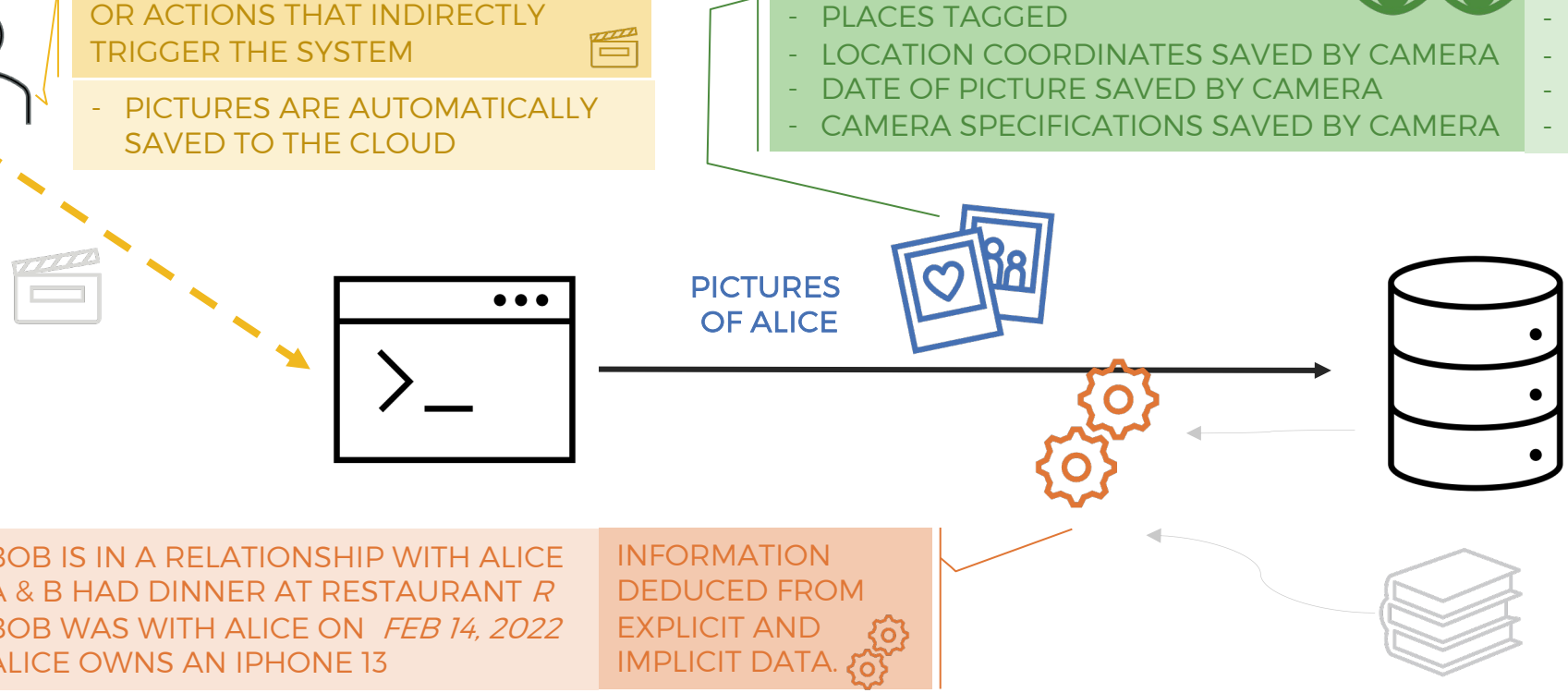
It's all about the data

INTERACTIONS WITH THE SYSTEM OR ACTIONS THAT INDIRECTLY TRIGGER THE SYSTEM

- PICTURES ARE AUTOMATICALLY SAVED TO THE CLOUD

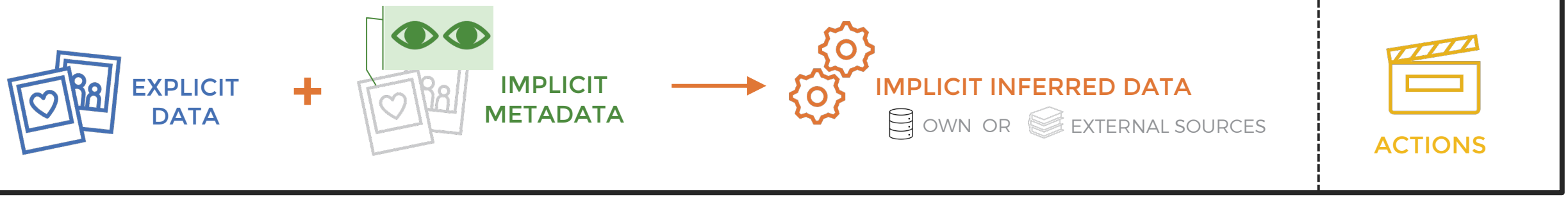
- PEOPLE TAGGED
- PLACES TAGGED
- LOCATION COORDINATES SAVED BY CAMERA
- DATE OF PICTURE SAVED BY CAMERA
- CAMERA SPECIFICATIONS SAVED BY CAMERA

- BOB TAGGED BY ALICE
- AT RESTAURANT *R*
- IN BRUSSELS
- ON FEBRUARY 14, 2022 AT 20h
- PICTURE TAKEN WITH IPHONE 13



- BOB IS IN A RELATIONSHIP WITH ALICE
- A & B HAD DINNER AT RESTAURANT *R*
- BOB WAS WITH ALICE ON *FEB 14, 2022*
- ALICE OWNS AN IPHONE 13

INFORMATION DEDUCED FROM EXPLICIT AND IMPLICIT DATA.



THREAT MODCON 2023

What can go wrong?

- Security threats
- Privacy threats

What can go wrong?

- **Security threats**
- **Privacy threats**

- **Reusable knowledge base**
  - STRIDE SECURITY
  - LINDDUN PRIVACY
  - EoP SECURITY
  - INCLUDES NO DIRT SECURITY PRIVACY
  - PLOT4AI PRIVACY
  - TRIM PRIVACY
  - STRIPED SECURITY PRIVACY
  - CTM SECURITY

> Allow for creativity by including both craft and science.
>
> *- Threat Modeling Manifesto*

Privacy threats on the individual

THREAT MODCON 2023

L

Linking

Personal data can be **combined** and more information can be extracted.

I

Identifying

Data can be **tied to** a natural **person**.

N

Non Repudiation

Impossible to **deny** involvement.

D

Detecting

Based on **observations**, additional information can be **assumed**.

D

Data Disclosure

Processing of personal data **beyond proportion**.

U

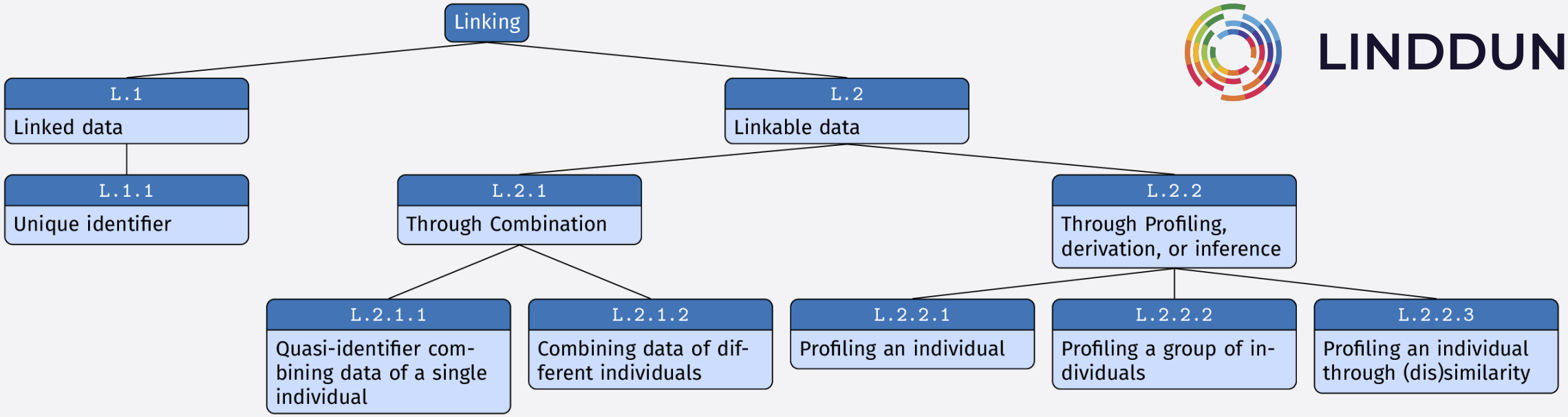
Unawareness

Lack of **transparency** & **control**

N

Non Compliance

Lack of **best practices** integration



LINDDUN PRO

LINDDUN GO

WWW.LINDDUN.ORG

What could go wrong?

Privacy threats

THREAT MODCON 2023

DOES THIS PRIVACY THREAT APPLY?

What could go wrong?

Privacy threats

Question 1

CAN IT HAPPEN?

DOES THIS PRIVACY THREAT APPLY?

What could go wrong?

Privacy threats

DOES THIS PRIVACY THREAT APPLY?

Question 1

CAN IT HAPPEN?

Question 2

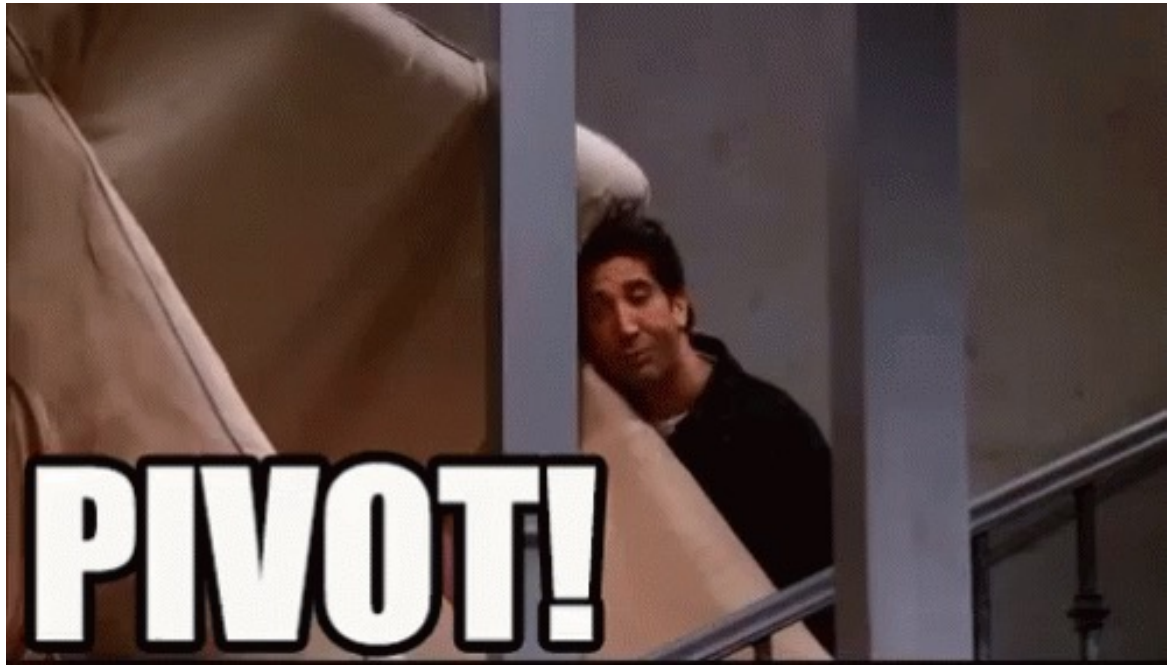
WOULD IT BE A PROBLEM?

FOR THE INDIVIDUALS INVOLVED

What can go wrong?
Looking for threats

- Security and privacy perspective required

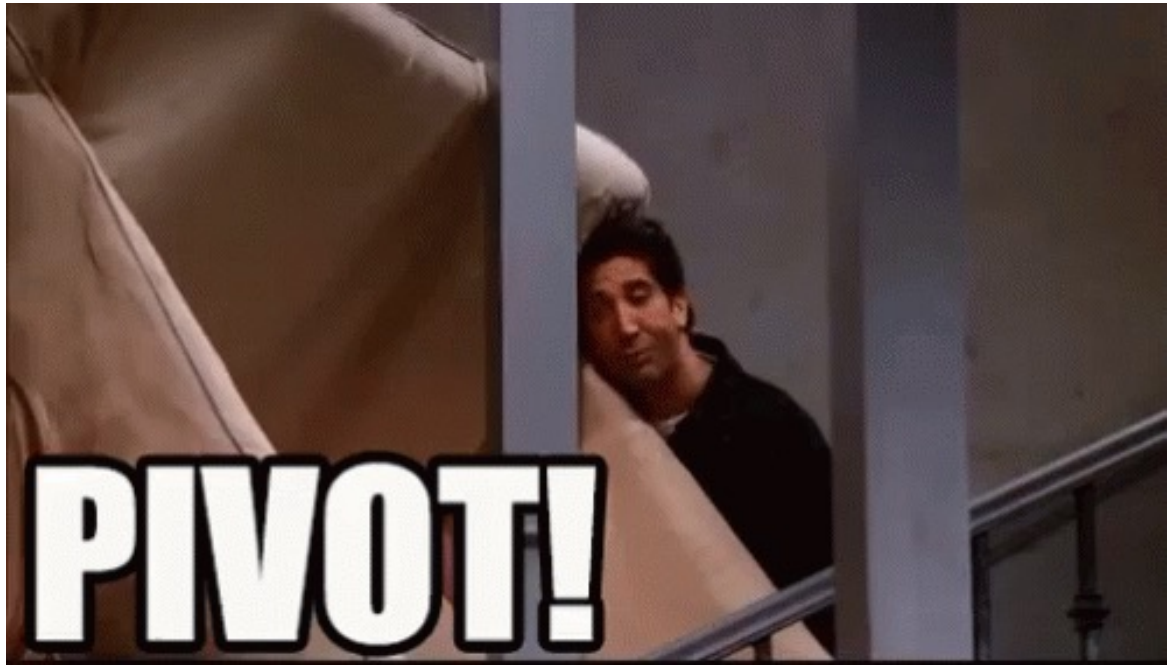
- How?
  - Combined analysis
  - Separate scoped security and privacy analyses



What can go wrong?
Looking for threats

- Security and privacy perspective required

- How?
  - Combined analysis for ad-hoc brainstorming
  - Separate scoped systematic security and privacy analysis
    - First security, then privacy focus



What can go wrong?
Documentation

Threats & Assumptions

- To the point
- Relevant
- Up to date

What are we going to do about it?

Privacy strategies & tactics

Minimize – Abstract – Separate – Hide
Inform – Control - Demonstrate – Enforce

Privacy patterns

Privacypatterns.org – privacypatterns.eu

PETS

Privacy Enhancing Technologies

© Friends, NBC

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

What are we going to do about it?

Align privacy with security, functionality, …

Full functionality - “Positive sum” approach

- No add-ons. Integrate early.
- Don’t go for separate solutions but aim for combined mitigation.

Did we do a good enough job?
Are we done yet?

- **Data protection / compliance requires a risk-based approach.**
  - Is residual risk acceptable for the individuals at stake?
- **Cover all aspects of the system?**
- **Cover all threat knowledge?**

Continuous refinement over a single delivery.

Threat Modeling Manifesto

THREAT MODCON 2023

What to take away?

- Privacy is important
- Threat modeling can be used to implement privacy
- Privacy and security threat modeling are F·R·I·E·N·D·S
  - They strengthen each other
  - They require different mindsets
  - Combined analysis is more efficient than separate

THREAT MODCON 2023

Shifting Privacy In

The one where privacy and security become F·R·I·E·N·D·S

Kim Wuyts

@wuytski

@kimw@mastodon.social


THREAT MODELING
CONNECT
THREAT MODCON 2023
THREAT MODELING IS FOR EVERYONE