Embracing Privacy Engineering

Going Beyond Checkbox Compliance

Kim Wuyts

Manager Cyber & Privacy

pwc

Compliance is Overrated

We need Privacy Engineering

Kim Wuyts

Privacy engineer | Threat modeling enthusiast | privacy-by-design advocate

PhD in privacy engineering

Cyber & Privacy Manager at PwC Belgium

Kim.Wuyts@pwc.com

@wuytski

@kimw@mastodon.social

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

LINDDUN Privacy Threat Modeling Pioneer

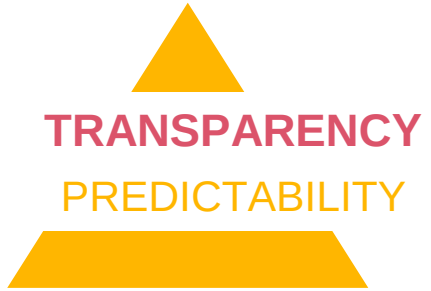
Threat Modeling Manifesto Co-Author

International Workshop of Privacy Engineering **(IWPE**) Program Co-Chair

ENISA ad-hoc **Working Group** on Data Protection by Design Member

Institute of Privacy Design (IOPD) Advisor

Privacy Engineering: Goals



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

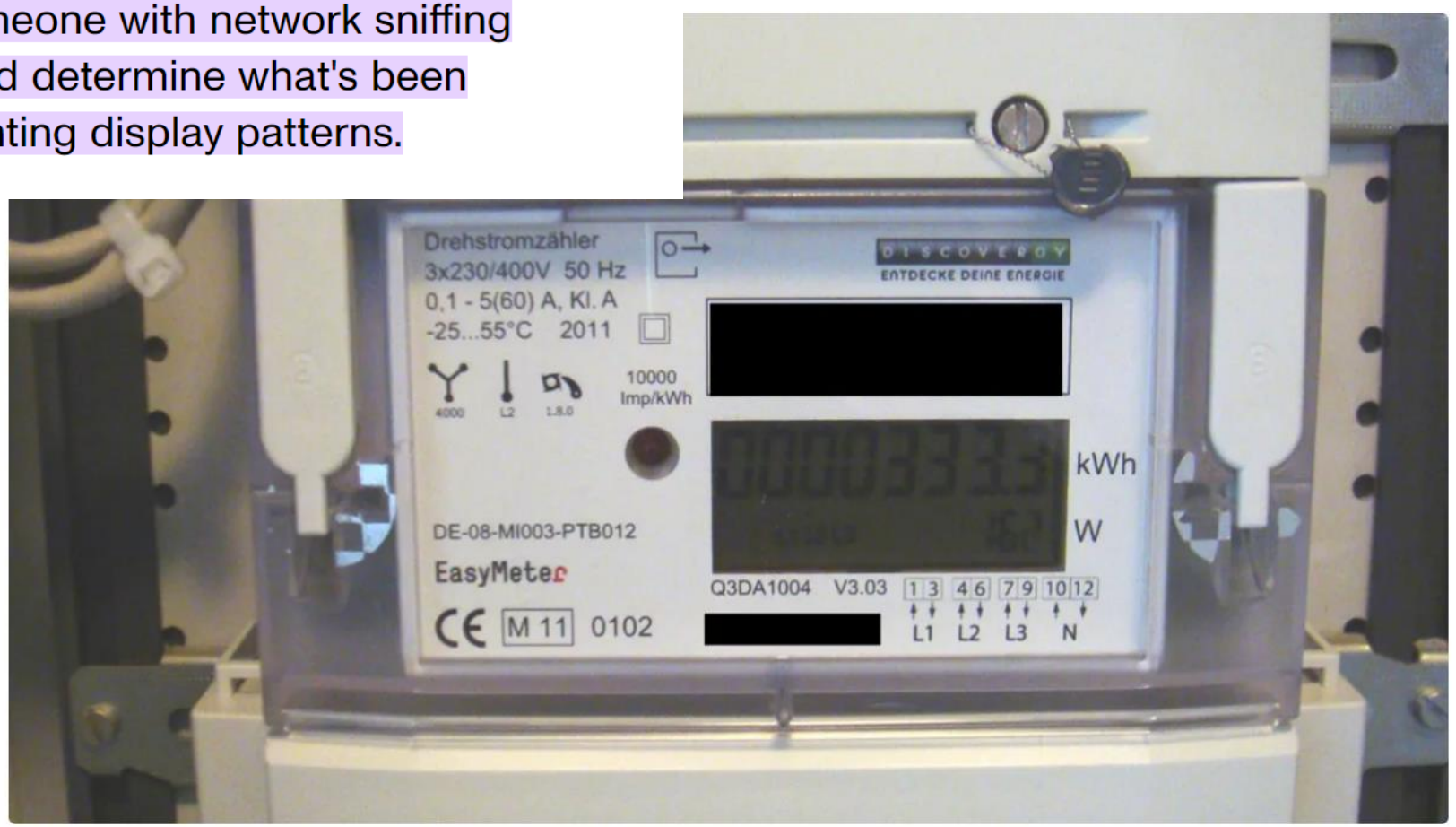
UNLINKABILITY

CONNECTING
THE DOTS

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.

https://www.cnet.com/news/privacy/researchers-find-smart-meters-could-reveal-favorite-tv-shows/



A Discovergy smart meter used for testing by researchers who found that they could snoop on some of the data transmitted over the Internet to figure out what specific content was being viewed on the digital TV.

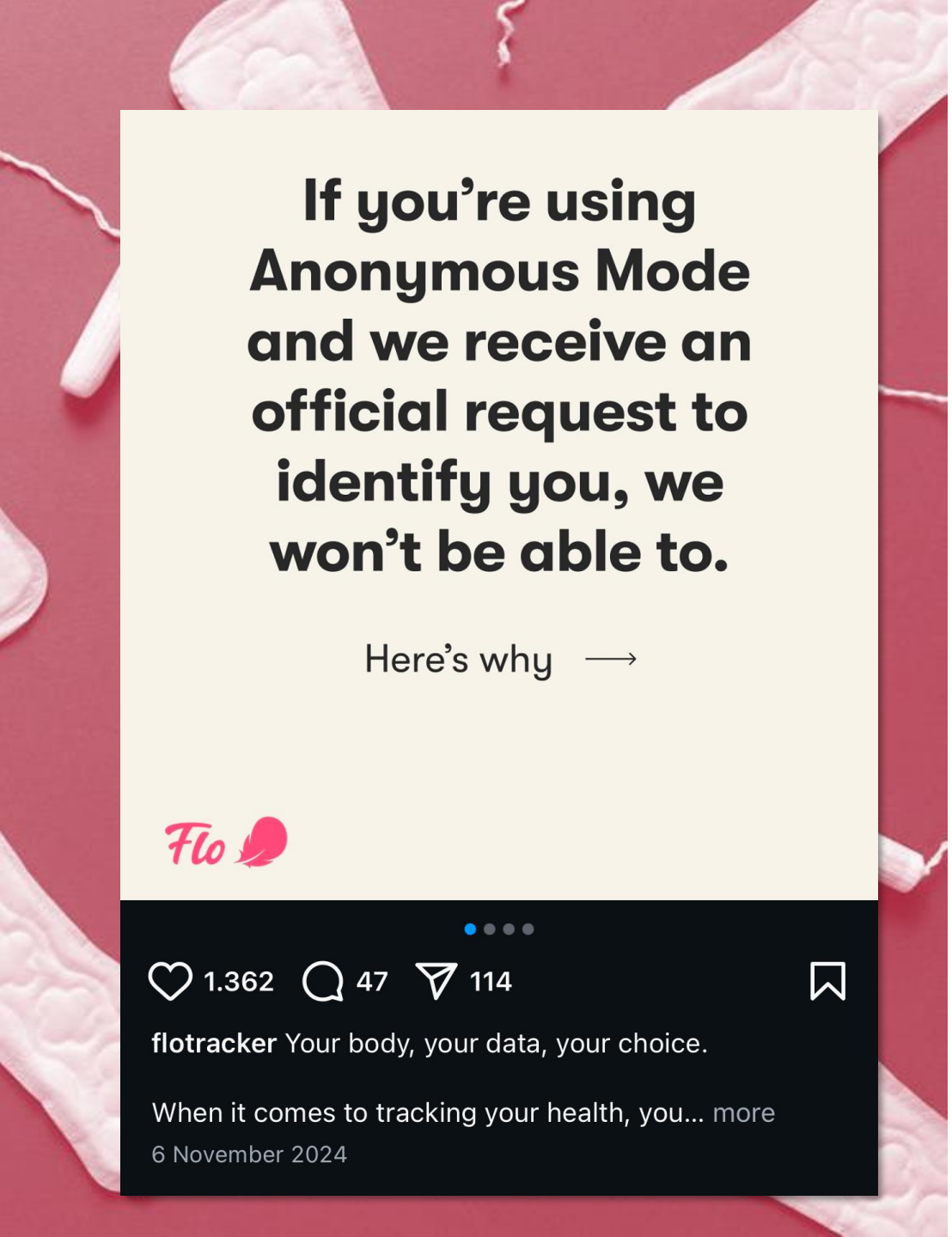
Muenster University of Applied Sciences,Ulrich Greveler, Benjamin Justus, and Dennis Loehr

PERIOD TRACKING APPS

Roe v. Wade

The US Supreme Court overruled Roe in 2022 ending the constitutional right to abortion.

PERIOD TRACKING APPS



TRANSPARENCY

INFORM

CONTROL

INTERVENABILITY

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

WHAT ARE WE GOING TO DO ABOUT IT?

PRIVACY MITIGATIONS & CONTROLS

Going beyond compliance and security

Unlinkability

Minimality

Minimize personal data being collected, processed, stored, and shared

- De-identification techniques
- Data deletion (retention period)

Limit processing to intended purposes

Transparency

Inform

Privacy notices

(e.g. transparency enhancing technologies (TETs) to align with implementation)

UI/UX avoiding deceptive patterns

Intervenability

Control / Empower

Consent management

Support for data subject requests

(e.g. data subject access request (DSAR), deletion, updating)

Privacy Engineering > PETs

(Privacy Enhancing Technologies)

Privacy Engineering

"Conceptions range from the design and implementation of anonymity-preserving algorithms and protocols to **higher-order ones taking up methods and practices** from software engineering, physical architecture, human-computer-interaction, or socio-technical systems design."

Pallas et al. IEEE Security & Privacy (Vol 22, issue 2, March-April 2024)

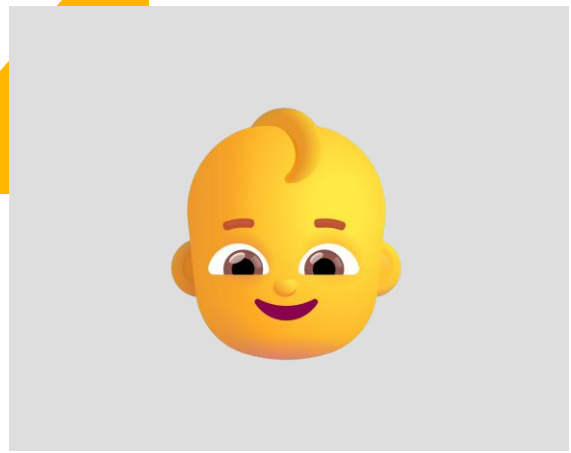
“It is evident **that proper and timely** development and **integration** of technical and organizational **measures into the data processing activities** play a big role in the practical implementation of different data protection principles. […] Data Protection Engineering aims to support the selection, deployment and configuration of appropriate technical and organizational measures in order to satisfy specific data protection principles.

ENISA, Data Protection Engineering report, Jan 2022

No worries… We have acronyms!

Data Protection Impact Assessment

PIA	Privacy Impact Assessment
LIA	Legitimate Interests Assessment
TIA	Transfer Impact Assessment
ROPA	Record Of Processing Activities



We can do better!

SECURITY CAN HELP

Yay!

But… we already do security

Privacy and security by design share the same foundation.

Align and integrate privacy in secure development lifecyle!

Threat modeling

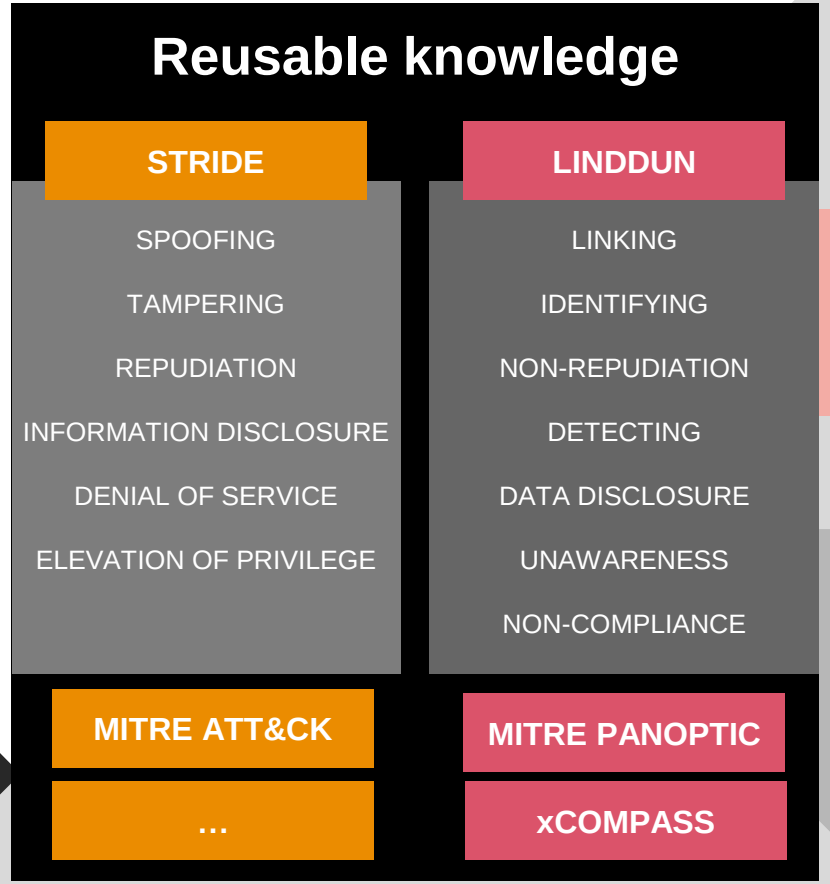
Analyzing representations of a system to highlight concerns about security and privacy characteristics.

Threat Modeling Manifesto

1. **What are we working on?**
2. **What can go wrong?**
3. **What are we going to do about it?**
4. **Did we do a good enough job?**

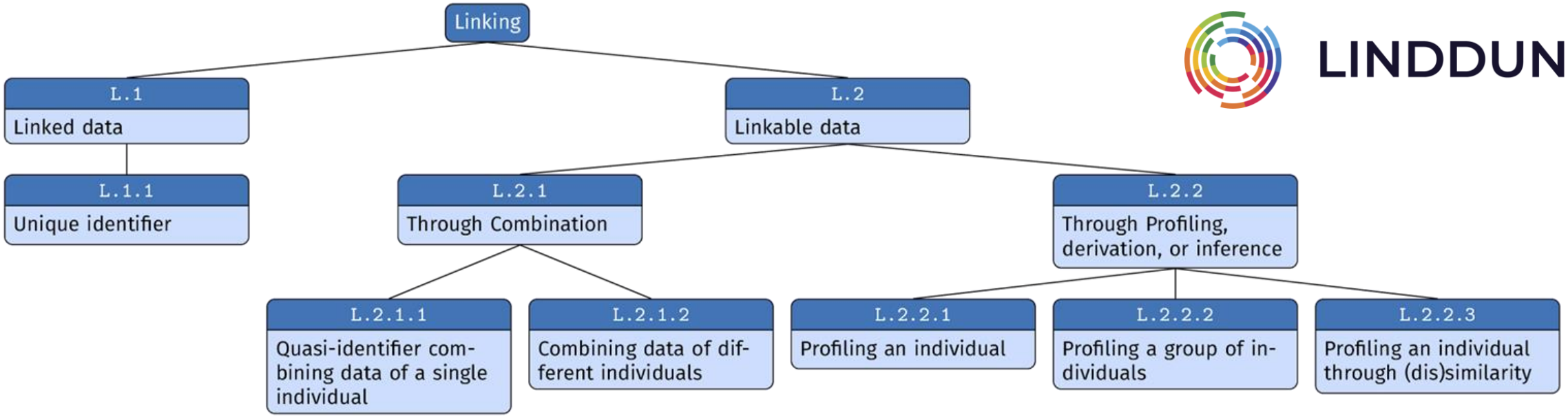
© Adam Shostack /
Threat Modeling Manifesto

Threat modeling



1. What are we working on?
2. What can go wrong?
3. What are we going to do about it?
4. Did we do a good enough job?

© Adam Shostack /
Threat Modeling Manifesto



LINDDUN PRO

LINDDUN GO

WWW.LINDDUN.ORG

Threat Modeling as Swiss Army Knife

- Approach to **structured (D)PIA**
- Driver for all **S&PDLC steps**
- Means to bring privacy back into engineering
  - Bring **security & privacy** closer together

Privacy Engineering

Are we there yet?

Choose

reasonable privacy

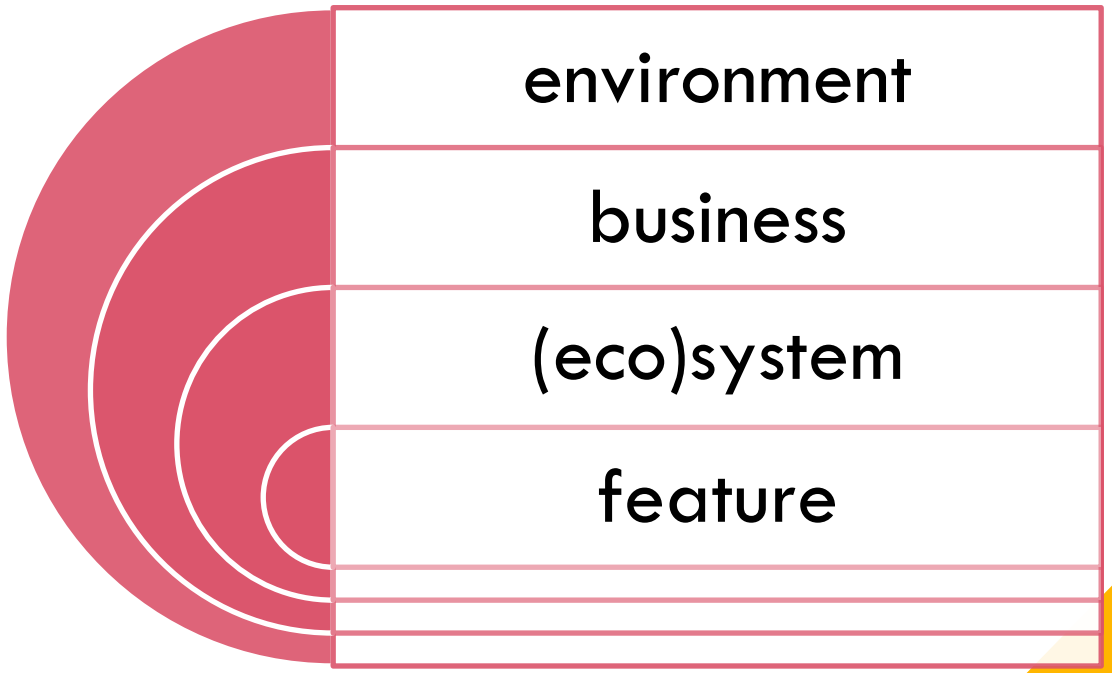
over perfect privacy

(Izar Tarandach (sort of))

Privacy Analysis needs to be more applicable

Privacy is **complex**

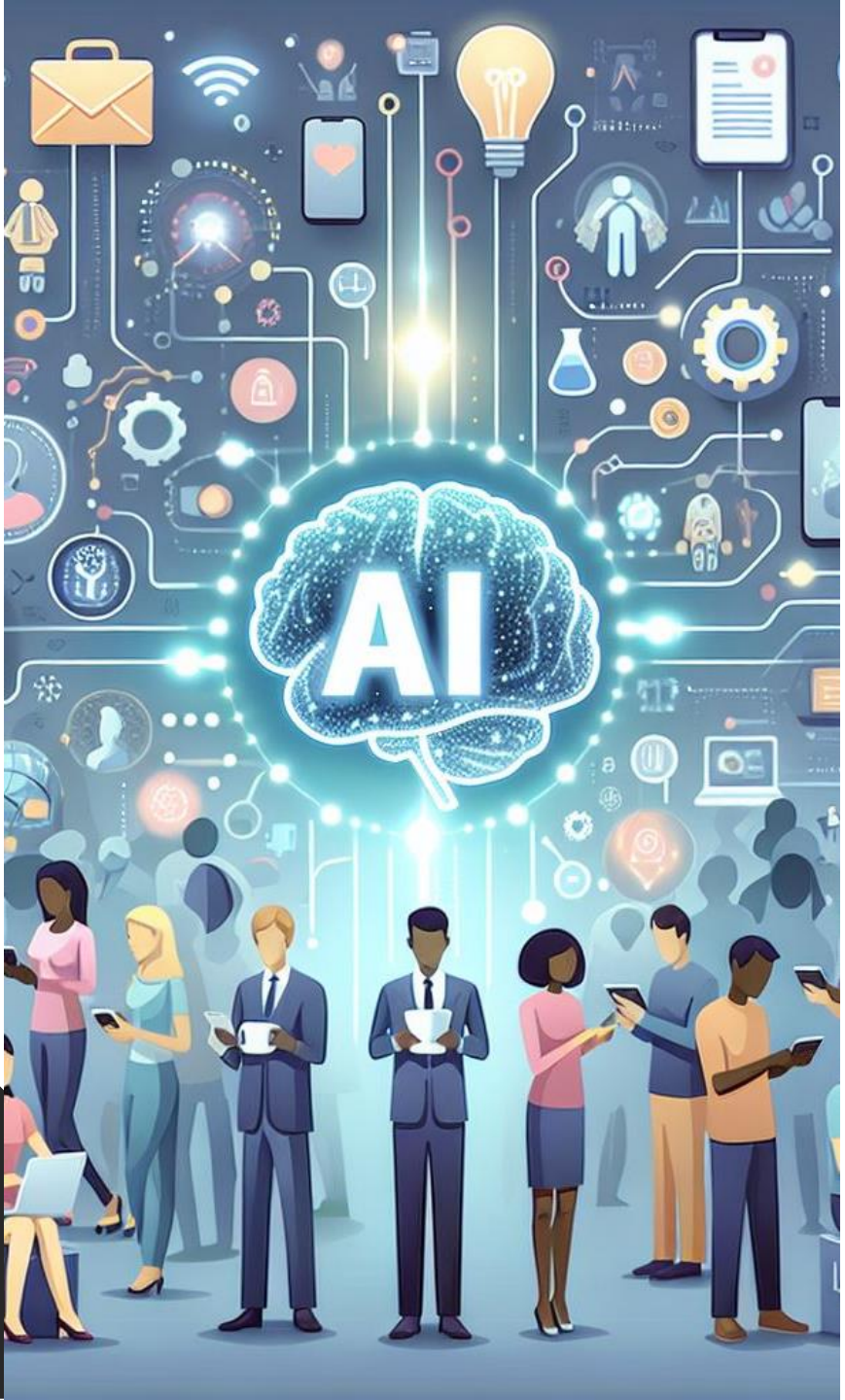
Multiple **layers** that need to be analyzed



Unraveling Privacy Threat Modeling Complexity: Conceptual Privacy Analysis Layers, *Kim Wuyts & Avi Douglen (August 2024, https://www.arxiv.org/abs/2408.03578)*

Privacy at the expense of **usability** is at the expense of privacy

(Avi Douglen (sort of))



AI. Oh my.

- AI can help, but…
  - Assistance over automation

Allow for **creativity** by including both craft and science
(Informed creativity, TM Manifesto)

- AI is awesome, but…
  - If you had bad security or privacy practices, the use of AI will amplify these issues.

AI can turn a small privacy leak into a flood of personal data

Privacy Controls!

Beyond threat elicitation

- What is out there?
  - ? Catalogs of solutions (patterns, PETs,…)
- What to use?
  - ? Selection support for solutions
- How to apply it?
  - ? Guidelines and guardrails for developers
  - ? Red team guidance
  - ? …

You...

...can help too

STRONGER TOGETHER

CALL TO ACTION

Leverage your security expertise and approaches

Threat model every story

DEV

Verify privacy protections

PENTESTING

Hunt for privacy violations

BUG BOUNTY

CALL TO ACTION

Leverage your security expertise and approaches

Be a privacy champion

OWASP GLOBAL APPSEC BARCELONA (MAY 25)
BLACKHAT LAS VEGAS (AUGUST 25)

Practical Privacy by Design Training

KIM WUYTS

AVI DOUGLEN

OUTLINE

- Privacy engineering **essentials**
- Privacy **architecture** & **feature** analysis
- **Data** inventory, mapping, and tagging
- Privacy **threats** (e.g. LINDDUN)
- Privacy **controls**, mitigations, and technologies
- **Full** privacy **process**

PRIVACY BY DESIGN TRAINING
KIM WUYTS & AVI DOUGLEN

Compliance is overrated

Kim Wuyts

Manager Cyber & Privacy