# Chapter 2: Definitions and threat models

**Lecture PETs4DS: Privacy Enhancing Technologies for Data Science**

Parts of this slide set (slides 3 – 15) are based on work from Thibaud René Kehler, RWTH Aachen University.

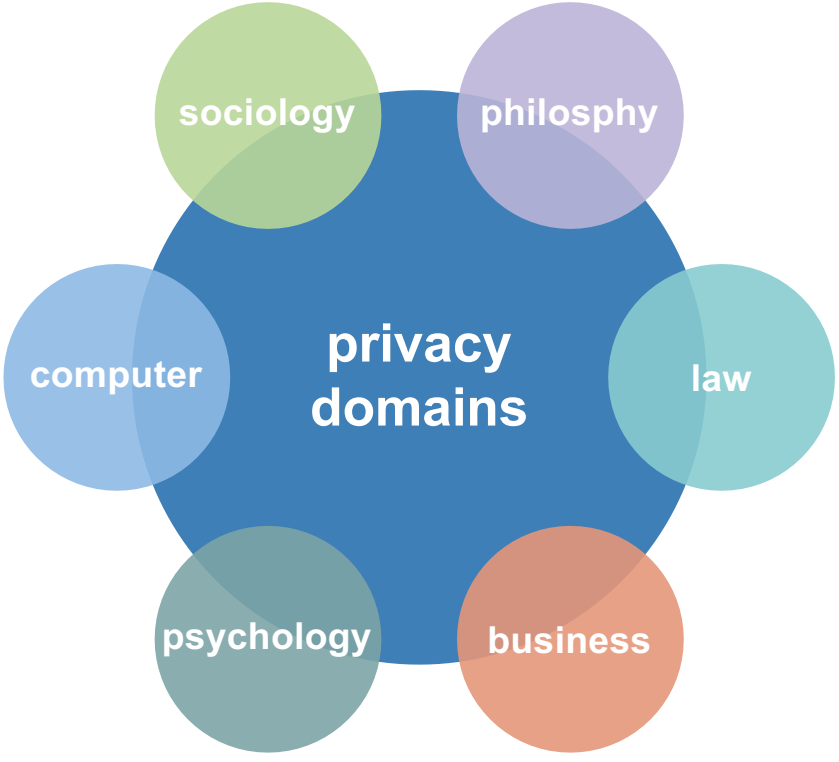
Dr. Benjamin Heitmann and Prof. Dr. Stefan Decker
Informatik 5
Lehrstuhl Prof. Decker


RWTH AACHEN UNIVERSITY

# Overview of chapter

- Privacy definitions
- LINDDUN privacy threat analysis methodology
  - categorisation of privacy threats
  - description of 6 step methodology
- Example showing how to apply LINDDUN to a real world example

# The Term “Privacy” is used in many Domains




Cooley (1888), Warren and Brandeis (1890)[15]

They defined privacy as the “right to be let alone.”

There is no single common and clear definition of privacy.

# Physical Privacy vs. Information Privacy

## Physical Privacy

Violation of the private space, e.g.

- home
- rest rooms
- car
- property

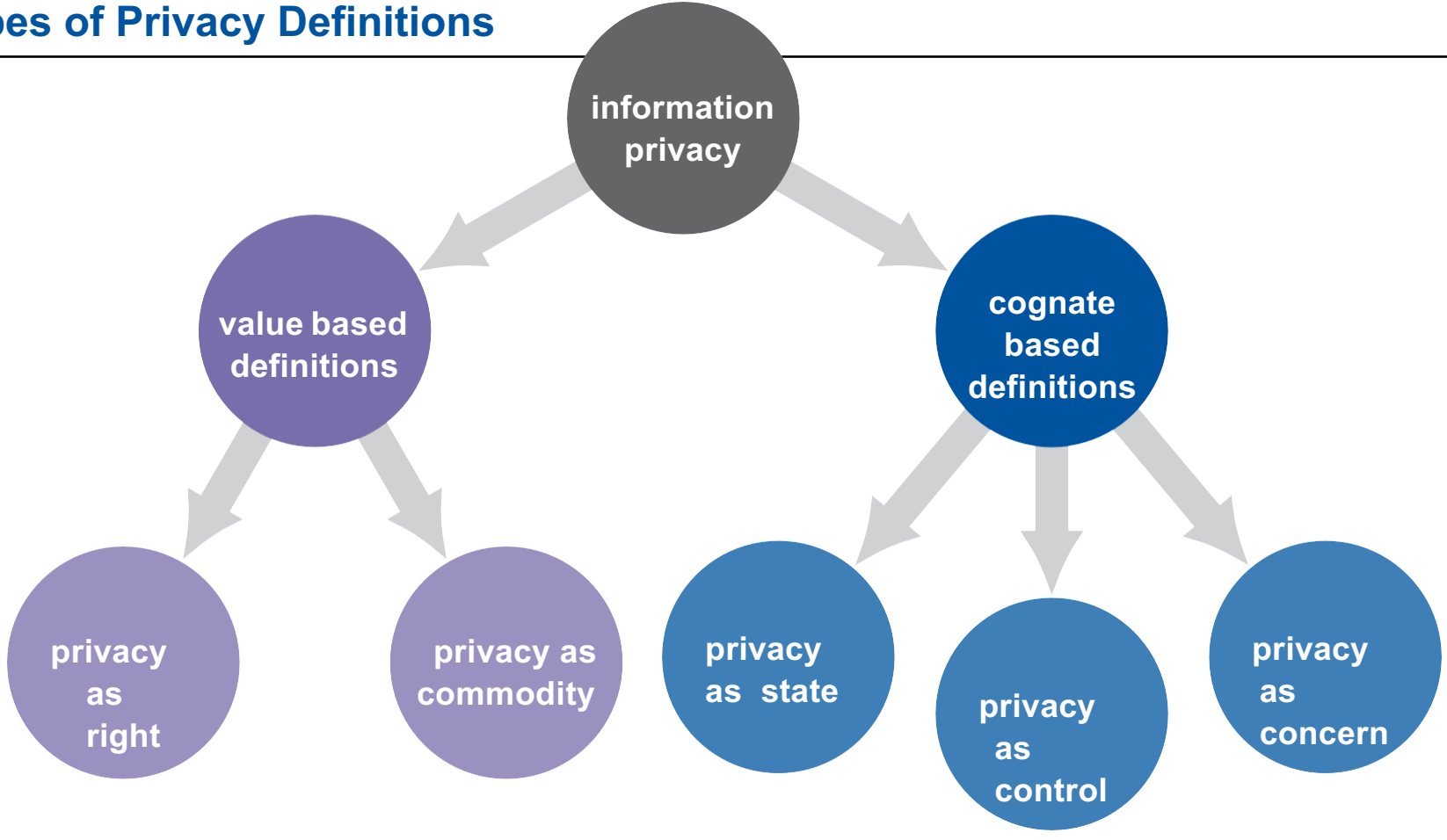
## Information Privacy

Leak of sensitive information, e.g.

- messages
- medical records
- purchasing behavior
- photographs
- personal interests

Relevant for computer science and information science.

# Types of Privacy Definitions



# Privacy as a Right

- Normative definition
- Depending on the states legislation

## United States of America

- Mostly omitted from laws and regulations
- Evolved in court cases, e.g. about
  - Law enforcement
  - Press
  - Workplace
  - Voyeurism

## European Union

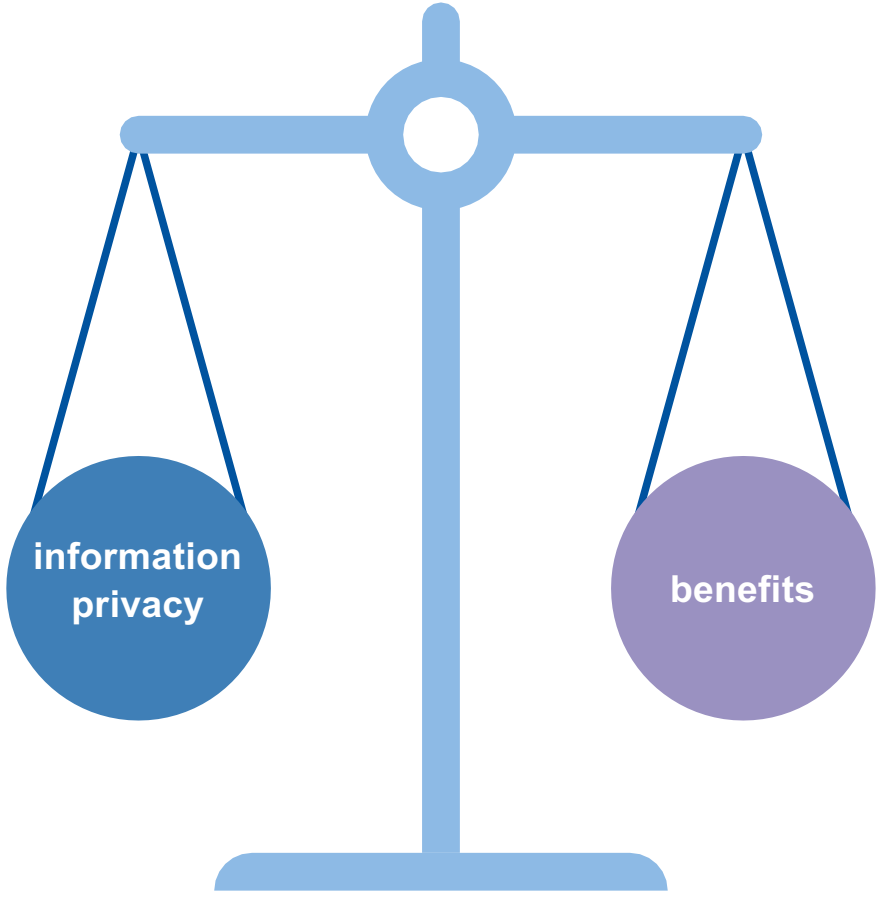
- E. U. directive (1995)
  - The “consent of the data subject” is required for data processing.
  - Implemented into the BDSG.
- Charter of fundamental rights (2010)
- E. U regulation (2016)
  - Is binding for all member states.

No precise and absolute definition of privacy

# Privacy as an Economic Commodity

- Market-based perspective
- Individuals provide information in exchange for benefits:
  - personalized advertising
  - social networking
  - interest-based proposals
- Privacy is difficult to quantify

User: Is a contract appropriate?

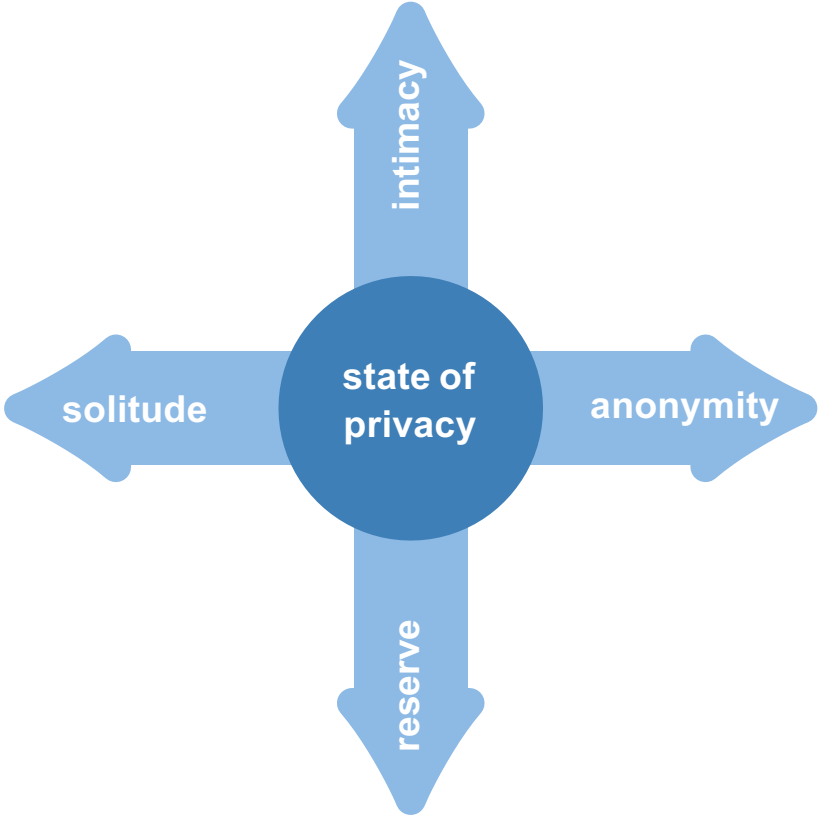


# Privacy as a State

## Schoeman (1984)

Privacy is the “state of limited access” to information.

- Various interpretations
  - e.g. four sub-states[16]
- Degree of privacy
- Individual’s goal to attend a state of privacy



# Privacy as a Form of Control

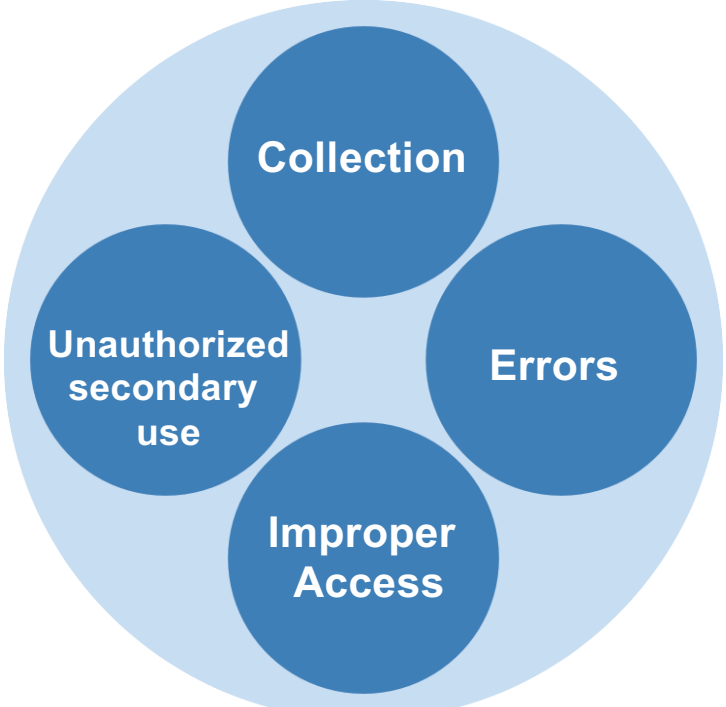
## Margulis (1977)

"Privacy, as a whole or in part, represents the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability."

- Variant: Ability to control
- Technologies which empower user with control?

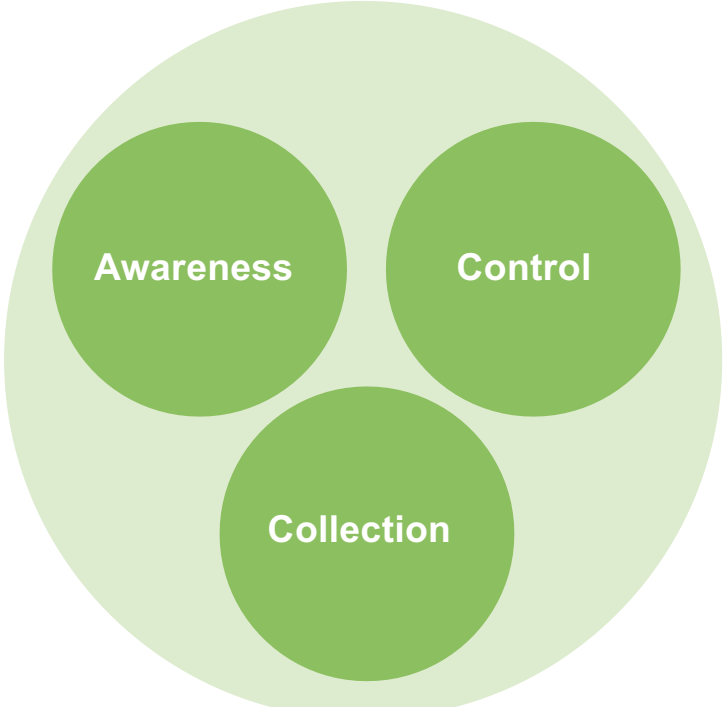
# Privacy as a Concern

## Concern for Information Privacy (CFIP)




15 items

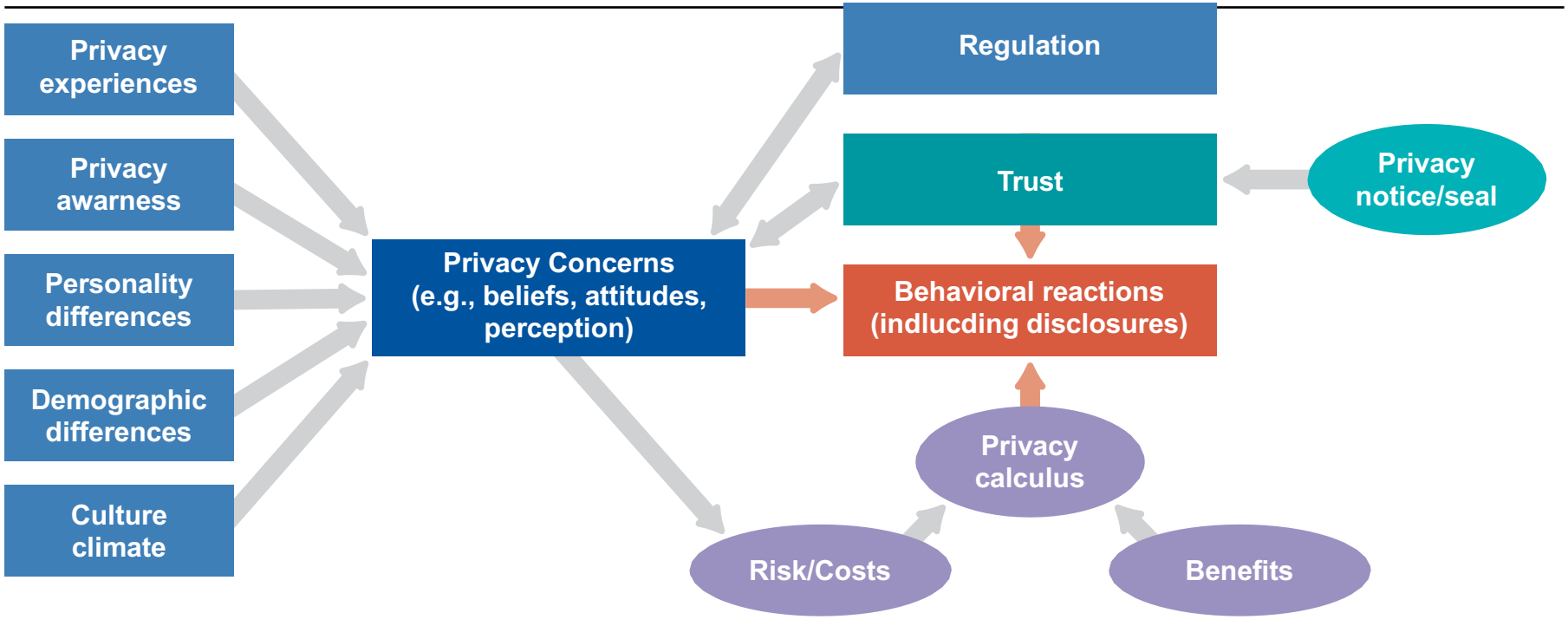
## Internet User's Information Privacy Concerns (IUIPC)




10 items

## APCO Maco Model

# Antecedents → Privacy Concerns → Outcomes




## Behavioral Paradox

The user externalizes significantly more information than he intends to do.

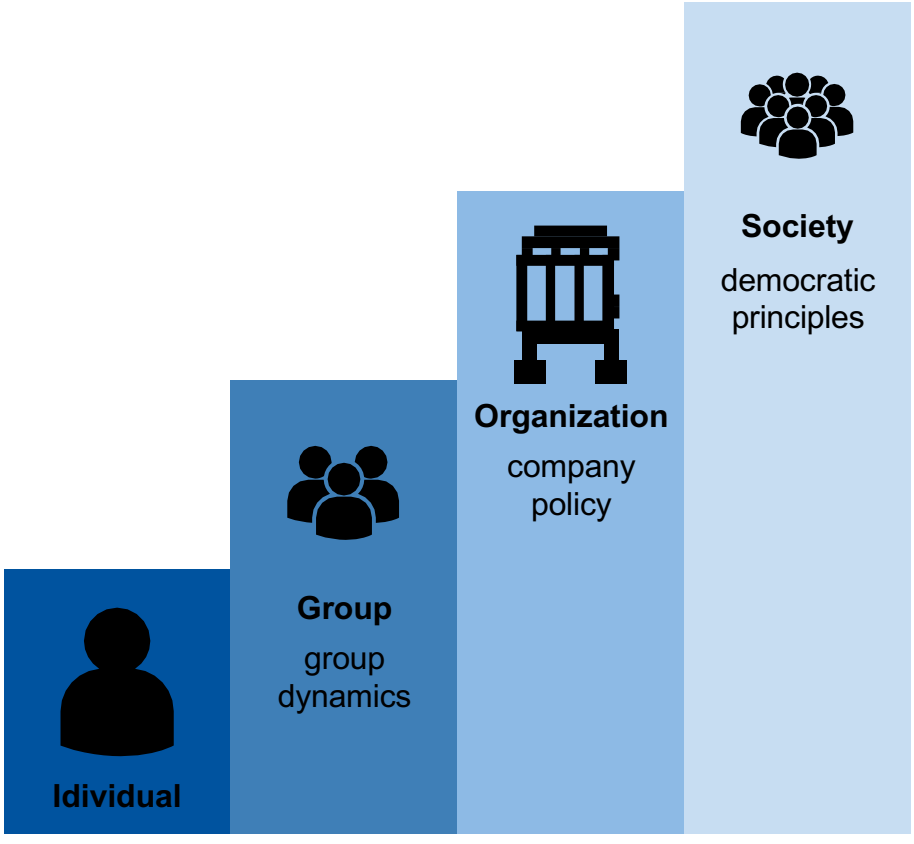
# Levels of Privacy

- Information is a shared property
- Concern appears at different levels
- May differ from individuals one

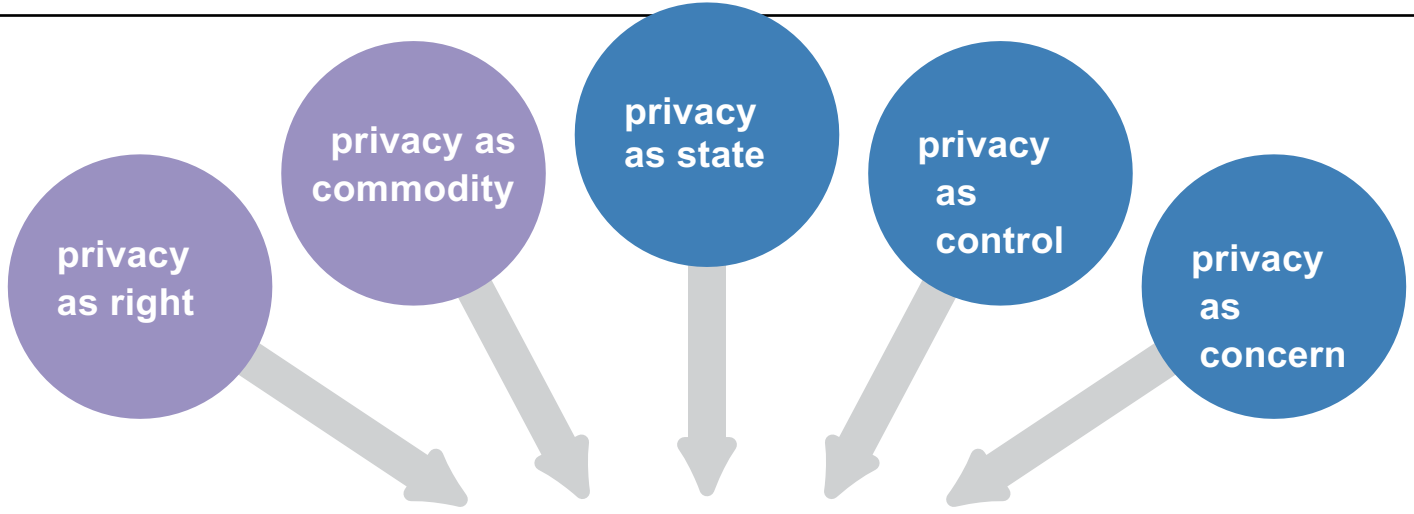
## Example: Society

Voting behavior in democratic elections, should not be released to the public.

Privacy is mostly investigated on the individual level.



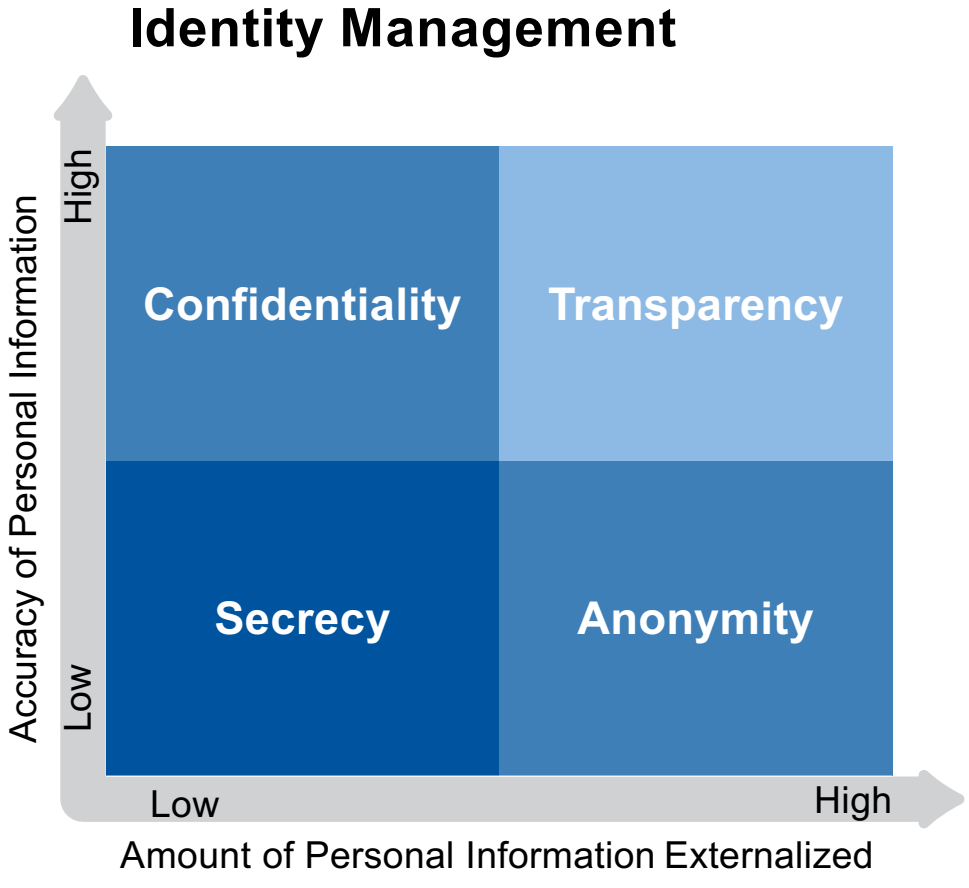
# The Challenge of Privacy for new Technologies



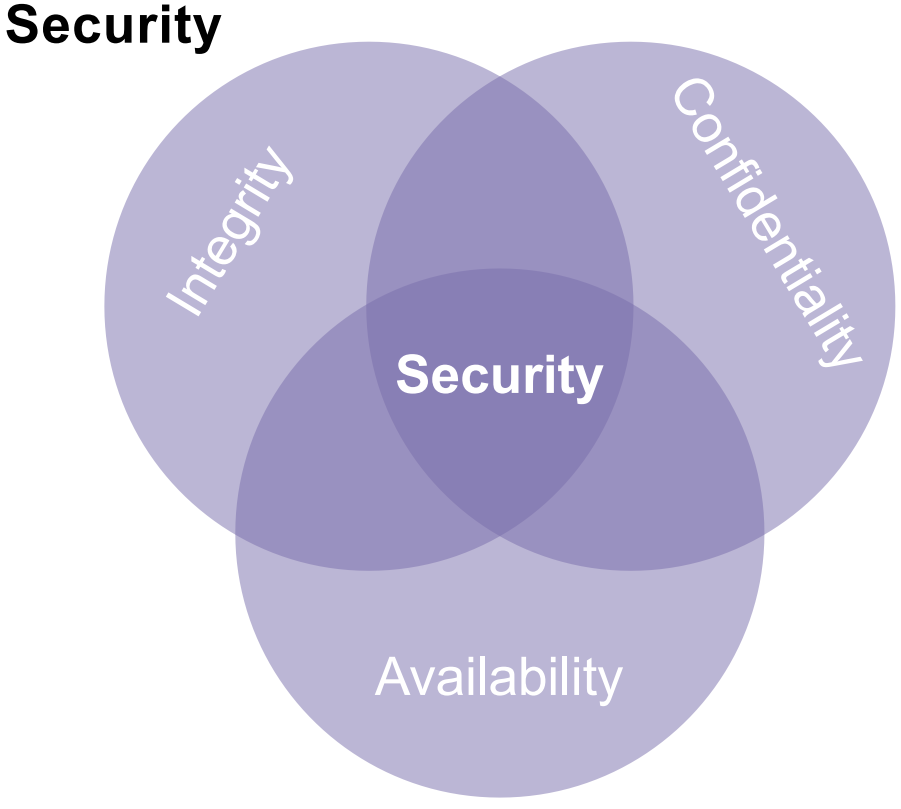

## New technological challenge

- Satisfy law
- Features for consumer protection
- Empower user with control
- Adress concerns on all levels

# Privacy is not the same as Identity Management



# Privacy is not the Same as Security




**Important:**

In most privacy scenarios:
Recipient = Attacker

# Threat Models

**Microsoft** (security context) :

“Threat modeling allows you to apply a structured approach to security and to address the top threats that have the greatest potential impact to your application first.”

**Wikipedia** (general) :

- Process to identify, enumerate and prioritize potential threats from a hypothetical attackers point of view

- Goal : Provide defenders with systematic analysis of
  - Potential attacker profiles
  - Attack vectors
  - Desired assets

# Examples of Threat Analysis in Daily Life

- Where should I park my bicycle ?
  - Parking rack available
  - Street light available
  - Better secured parking spot in the next street
- Should I walk outside after dark ?
  - Which Country/City am I in
  - Part of the City
  - Hide valuable things
  - How to prepare for bad situations (e.g. muggings)

# Threat Analysis in Different Countries

**Examples are from Brazil**

- Advice for tourists on being outside in Brazil, especially after dark:
  - Hide your watch, mobile phone and other valuables.
  - Don’t use your smart phone for directions.
  - Don’t wear fancy clothes.
  - Always take the taxi after dark, even for short distances.
  - Always have a bit of cash with you, in case you get mugged.
- Threats for car drivers in Brazil:
  - Most cars have tinted windows: makes it hard to assess value of car and passengers.
  - Nobody stops at traffic lights, especially after dark: high risk of getting mugged.
- Can you think of other examples?

# Security Threat Model: STRIDE (1/3)

**Model-based analysis approach developed by Microsoft.**

Categories of **security threats** in STRIDE:

- **Spoofing of user identity**
  - Impersonating a different user.
  - Example: Access of credential storage to obtain valid credentials, and then using username/password to gain access as that user.

- **Tampering with data**
  - Malicious modification of data.
  - Example 1: unauthorised changes made to persistent data, e.g. data in a data base.
  - Example 2: alteration of data as it flows between two computers over an open network, such as the Internet. (“man in the middle attack”)

# Security Threat Model: STRIDE (2/3)

- **Repudiation** (“Nachweisbarkeit”)
  - Threats are caused by users denying to perform an action without other parties being able to prove otherwise
  - Example: User gains unauthorised access to database and modifies data. Afterwards he deletes all traces of modification in the logs. That database is lacking e.g. decentralised logging facilities.

- **Information disclosure**
  - Exposure of information to individuals who are not supposed to have access to it.
  - Examples: read a file which belongs to another user, read data in transit between two computers.

# Security Threat Model: STRIDE (3/3)

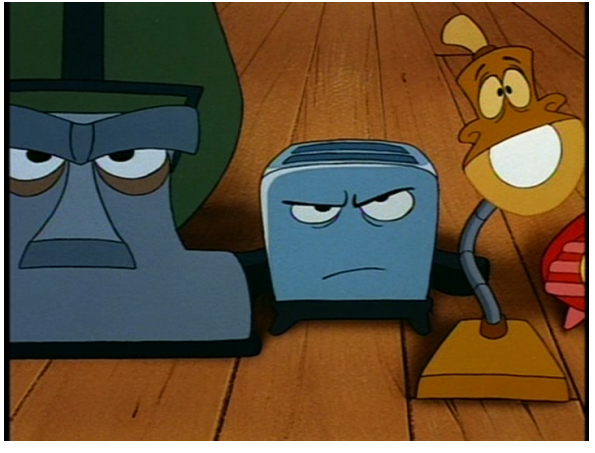
- **Denial of service**
  - Denying of a service to the valid users of that service
  - Protecting against this threat involves improving system availability and reliability.
  - Example: making a web server temporarily unavailable or unusable.

- **Elevation of privilege:**
  - Unprivileged user gains privileged access and can compromise or destroy entire system.
  - Example: gaining root privileges after logging in as a regular user on a Unix system.

# Lets do a Quick Threat Analysis for an Example: DDoS Attacks Triggered by IoT Botnet

- On 21st October 2016 several major websites like Amazon and Paypal where knocked off the web

- Reason: Distributed Denial of Service attack on DNS provider Dyn
  - Majority of traffic generated by Mirai botnet
  - 10s of millions of IPs involved
  - Most from Internet of Things (IoT) devices like cameras and routers using XiongMai hardware
  - IoT devices are hard to patch: old exploits and default passwords are easy to use



Details at http://arstechnica.com/information-technology/2016/10/inside-the-machine-uprising-how-cameras-dvrs-took-down-parts-of-the-internet/

# Threat analysis: DDoS attacks triggered by IoT Botnet

- Spoofing?
  - Yes, threat vector to compromise the devices used in the Mirai IoT botnet, e.g. with default passwords
- Tampering?
  - Yes, another threat vector used to build the Mirai IoT botnet
- Repudiation?
  - Yes, no trace of attacker (individual), no, all evidence of attacks is in the open
- Information disclosure?
  - No, not goal of attack
- Denial of service?
  - Yes, the goal of the attack was the Dyn dynamic DNS service
- Elevation of privilege?
  - No, not goal of attack, but might have been used to build Mirai IoT botnet

Access to more technical details allows more granular threat analysis.

# Privacy Threat Modeling Methodology: LINDDUN

- Inspired by Microsoft's STRIDE security threat model
- Model-based approach starting with data flow diagrams (DFDs)
- In addition, knowledge-based approach as provides a catalogue of most common attack paths associated with the different threat categories.
- LINDDUN follows the **Privacy by Design** paradigm:
  - can be used to include privacy as early as possible in development process
  - can also be applied to existing software systems to identify privacy threats
- All LINDDUN materials are available on their web site, in the "Material" section: https://distrinet.cs.kuleuven.be/software/linddun/download.php

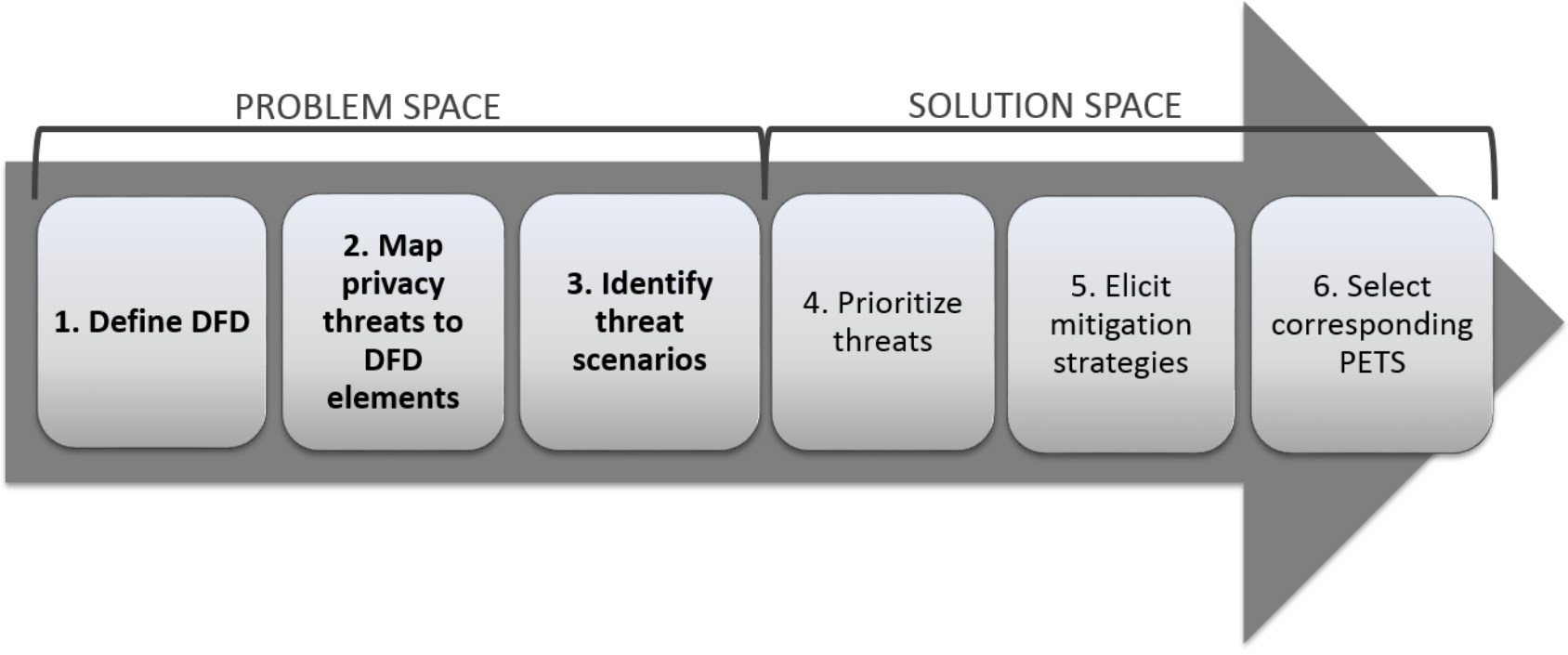
# Modifying the LINDDUN Methodology for this Lecture

- LINDDUN provides vocabulary to identify and analyze privacy threats
- LINDDUN methodology enumerates ALL potential threats in a system
- Great for designing and analyzing industrial projects, but beyond the scope of this lecture

→ We will reuse the following

- LINDDUN threat categories
- 1st step: Define Data Flow Diagram (DFD)
- 2nd step: Mapping the DFD to LINDDUN threat categories
- 3rd step: Eliciting privacy threats for each relevant DF element (without using the misuse case template)

# LINDDUN: Overview of Steps in Methodology



# Categorisation of Privacy Threats in LINDDUN

- **Hard privacy threats**
  - **L**inkability
  - **I**dentifiability
  - **N**on-repudiation
  - **D**etectability
  - **D**isclosure of information

- **Soft privacy threats**
  - Content **U**nawareness
  - Policy and consent **N**on-compliance

# LINDDUN Privacy Threats: Linkability

**Linkability**

- Being able to sufficiently distinguish whether 2 IOI (items of interest) are linked or not, even without knowing the actual identity of the subject of the linkable IOI.
- Not being able to hide the link between two or more actions/identities/pieces of information.

**Examples :**

- Anonymous letters written by the same person
- Web page visits by the same user
- Entries in two databases related to the same person
- People related by a friendship link, etc.

# LINDDUN privacy threats: Linkability

**Consequences:**

- *Identifiability* when too much linkable information is combined
- *Inference* when “group data” is linkable
  - can lead to societal harm, like discrimination
    (e.g. if an insurance company knows that people who live in a certain area get sick more often, they might increase their insurance cost for that target group)

# LINDDUN Privacy Threats: Identifiability

**Identifiability**

- Being able to sufficiently identify the subject within a set of subjects (i.e. the anonymity set)
- Not being able to hide the link between the identity and the IOI (an action or piece of information)

**Examples :**

– Identifying the reader of a web page
– Identifying the sender of an email
– Identifying the person to whom an entry in a database relates

**Consequences :**

– Can lead to severe privacy violations (when subject assumes he is anonymous)

# LINDDUN Privacy Threats: Identifiability

**Related Concepts**

## Anonymity

- Description in terms of identifiability: the attacker cannot sufficiently identify the subject within a set of subjects, the anonymity set
- Description in terms of linkability: anonymity of a subject with respect to an attribute may be defined as unlinkability of this subject and this attribute

## Pseudonymity

- Usage of multiple pseudonyms for different purposes
- Each pseudonym gets reused multiple times
- Difference or sameness of psuedonyms can not be identified
- No linkability between pseudonym and real identity

# LINDDUN Privacy Threats: Non-Repudiation

**Non-Repudiation**

- Not being able to deny a claim
- Having irrefutable evidence concerning the occurrence or non-occurrence of an event or action

**Examples :**

– Anonymous online voting systems

– Systems which allow whistleblowers to anonymously report something

# LINDDUN Privacy Threats: Non-Repudiation

## Important considerations:

- Achieving non-repudiation in a system enables plausible deniability.
- This threat is usually a security goal.
- However for must use cases non-repudiation and accountability exclude each other.

## Consequences:

- Accountability: when a person is not able to repudiate an action or piece of information, he can be held accountable. (e.g. a whistleblower can be prosecuted)

# LINDDUN Privacy Threats: Detectability

**Detectability**

- An attacker can sufficiently distinguish whether an item of interest (IOI) exists or not
- Detectability concerns IOIs of which the content is not known to the attacker

**Examples :**

– Knowing whether an entry in a database corresponds to a real person

– Being able to distinguish whether someone or no one is in a given location

– Knowing whether a message was sent

# LINDDUN Privacy Threats: Detectability

## Consequence:

- Inference: By detecting whether an IOI exists, one can deduce certain information, even without actually having access to that information
- Example for inference: Knowing that a celebrity has a health record in a rehab facility, you can deduce the celebrity has an addiction, even without having access to the actual health record

# LINDDUN Privacy Threats: Disclosure of information

**Disclosure of Information**

- Exposing information to someone not authorized to see it
- Mitigating any disclosure of information results in confidentiality of a system

**Examples :**

– Transferring un-encrypted email

– Not applying access control to a classified document

– Not protecting a database containing sensitive information

# LINDDUN Privacy Threats: Disclosure of Information

**Important considerations:**

- Confidentiality is an important pre-requisite for preserving of privacy
- However, STRIDE should be used for a full analysis of security threats

# LINDDUN Privacy Threats: Unawareness

**Unawareness**

- Not understanding the consequences of sharing personal information in the past, present, or future

- The awareness property focuses on the user's consciousness regarding his own data. The user needs to be aware of the consequences of sharing information

**Examples :**

– Unawareness of who can read a users posts to social networks such as Facebook
– Unawareness of personal data shared with 3rd party services e.g. via loyalty cards or credit cards

**Consequences :**

– Linkability / identifiability: the more information is available, the easier it can be linked (and identified)

# LINDDUN Privacy Threats: Non-Compliance

**Non-Compliance**

- Not following the (data protection) legislation, the advertised policies or the existing user consents
- The compliance property requires the whole system as data controller to inform the data subject about the system's privacy policy, and allow the data subject to specify consents in compliance with legislation, before users accessing the system

**Example (medical domain) :**

– In some countries, healthcare professionals are only allowed to access medical information if the data subject has given informed consent (or in case of emergency)

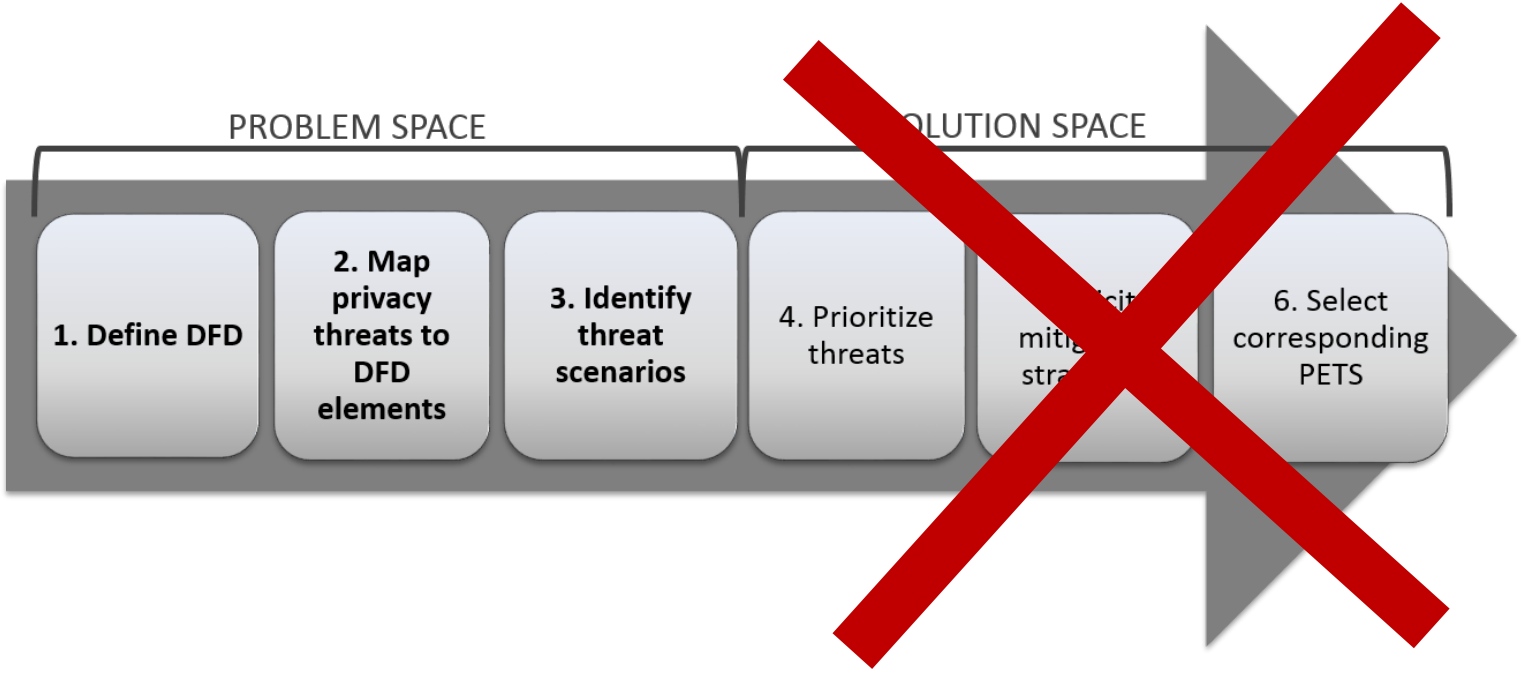
**Consequences :**

– Fines (when violating legislation, or not adhering to the communicated corporate policies
– Loss of image, credibility, etc.

# Categorization of Privacy Threats in LINDDUN

- **Hard privacy threats**
  - **L**inkability
  - **I**dentifiability
  - **N**on-repudiation
  - **D**etectability
  - **D**isclosure of informtion
- **Soft privacy threats**
  - Content **U**nawareness
  - Policy and consent **N**on-compliance

# LINDDUN: Overview of Steps in Methodology



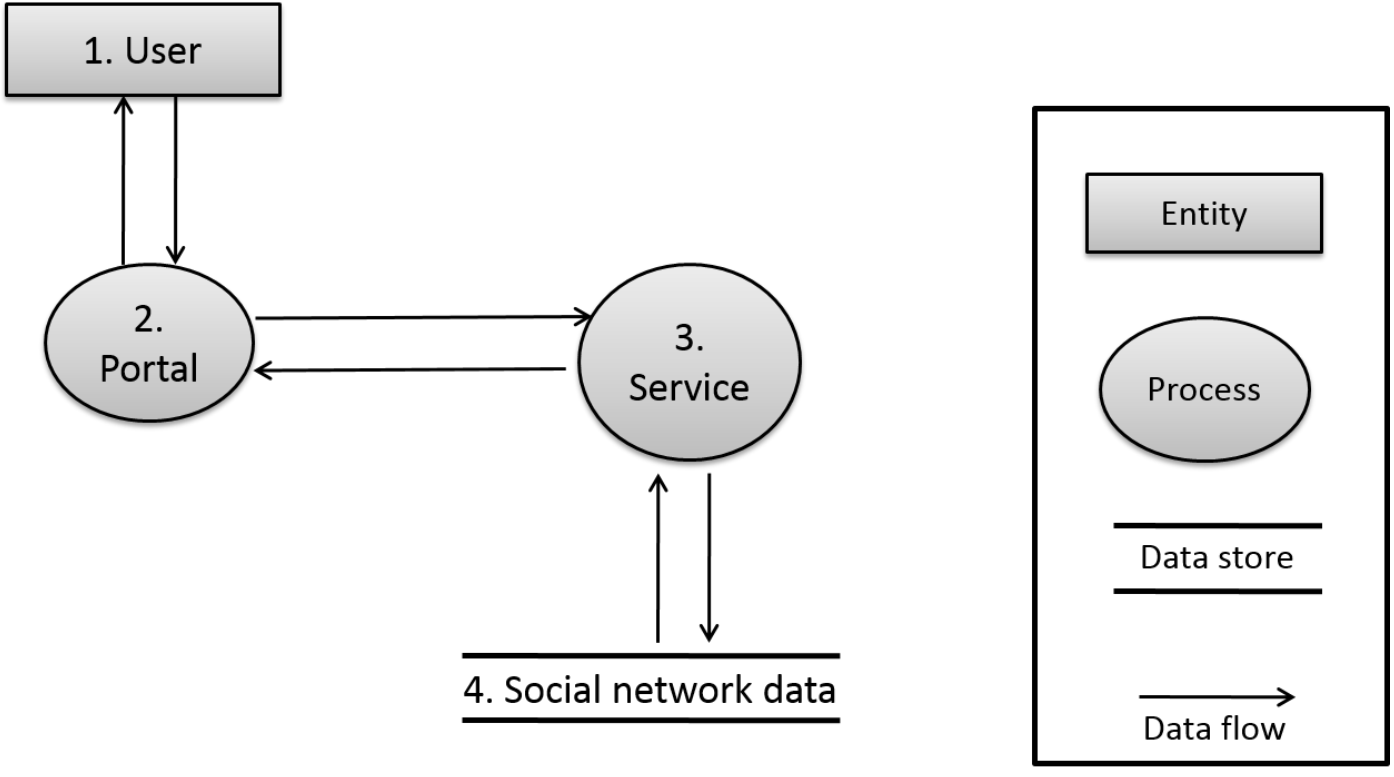
# LINDDUN: 1st step: Define Data Flow Diagram (DFD)

A DFD is a structured, graphical representation of the system, using only 4 types of building blocks:

- **Process (P):** any kind of software operating on the data
- **Data store (DS):** a passive container of data
- **External entity (E):** a source or destination of data, such as a user of the system or external 3rd party services
- **Data flow (DF):** a named flow of data
- Optional: add dashed lines to indicate **trust boundaries**, where parties with different privileges / levels of trust interact

- The DFD model is based on the available system description.
- More granular system descriptions (e.g. UML diagrams) will allow to model more granular privacy threats

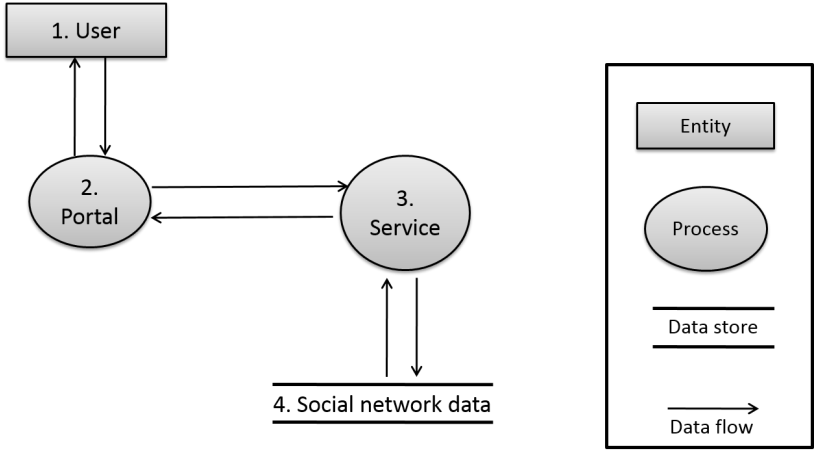
# LINDDUN 1st step: DFD for Running Example: Generic Social Network



# Process for Generating the DFD

**If you don't have an architecture diagram available:**

1. Create one main process.
2. Add actors of the system as external entities (users and 3rd party services)
3. Add data stores.
4. Now decompose the main process as necessary.
   1. Often there is one separate process to handle each external entity and each data store.
5. Now add data flows to connect elements which share data.
6. Put labels on the data flows if possible.
7. If multiple types of data are transmitted, think about adding multiple data flows, as this can result in multiple separate threats.
8. Put names or numbers on the elements.



# LINDDUN: 2nd step: Mapping the DFD to LINDDUN threat categories

| | L | I | N | D | D | U | N |
|---|---|---|---|---|---|---|---|
| **Entity** | X | X | | | | X | |
| **Data store** | X | X | X | X | X | | X |
| **Data flow** | X | X | X | X | X | | X |
| **Process** | X | X | X | X | X | | X |

- For each element in the DFD, identify the threats which are applicable the element
- The table shows the threats associated with each DFD element.
- In a nutshell:
  - External entities can only be threatened by linkability, identifiability and unawareness.
  - All other elements can be threatened by all 7 threats except for unawareness.
  - Non-compliance threatens the whole system, not just one element.
- Document your assumptions, if you want to exclude a threat to a specific element.

# LINDDUN: 2nd step: Mapping the DFD to LINDDUN Threat Categories for the Running Example

- Numbered threats in the table will be analysed
- Threats marked with X in grey area are considered not relevant to the system, due to the following assumptions:
  - Processes on their own usually carry no threats
  - All internal communication is trustworthy
  - Only interactions between data store and system and user and system need to be analysed
  - Non-repudation and detectability are not important for the system

| | Threat target | L | I | N | D | D | U | N |
|---|---|---|---|---|---|---|---|---|
| Data Store | Social network DB | 1 | 4 | × | × | 7 | | 10 |
| Data Flow | User data stream (user – portal) | 2 | 5 | × | × | 8 | | 10* |
| | Service data stream (portal – service) | × | × | × | × | × | | 10* |
| | DB data stream (service – DB) | × | × | × | × | × | | 10* |
| Process | Portal | × | × | × | × | × | | 10* |
| | Social network service | × | × | × | × | × | | 10* |
| Entity | User | 3 | 6 | | | | 9 | |

# LINDDUN: 3rd step: Eliciting Privacy Threats

- **Idea:** Look at each remaining potential privacy threat, and think about how it could be attacked.

- This step has three sub-steps:
  - A.) Refine (abstract) threats via the threat tree pattern into concrete threats.
  - B.) Document if any concrete threats are not relevant to the system.
  - C.) Document threats as misuse cases (also called “threat scenario)

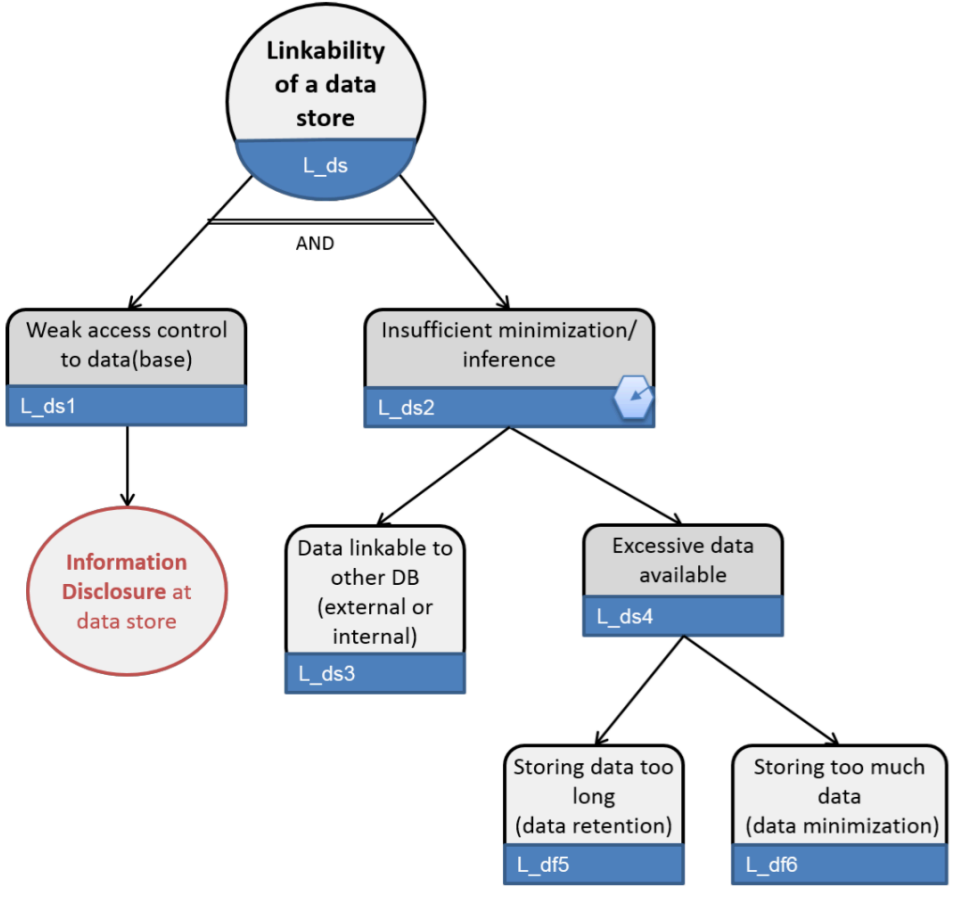
- All threat tree patterns are in the file “LINDDUN_catalog_v2.pdf”
  - Many of the trees are very similar, they document the most common concrete threats.
- Misuse cases follow a template, which is shown later in the slide set

# LINDDUN: 3rd step: Eliciting Privacy Threats for the Running Example

- A.) Refine (abstract) threats via the threat tree pattern into concrete threats.

**Threat 1:**
Linkability of social network database (data store)

Lets look at the threat tree pattern.



# LINDDUN: 3rd step: Eliciting privacy Threats for the Running Example

- Document threats as misuse cases.

**Threat 1:**
Linkability of social network database (data store)

**MUC 1 – Linkability of social network database (data store)**

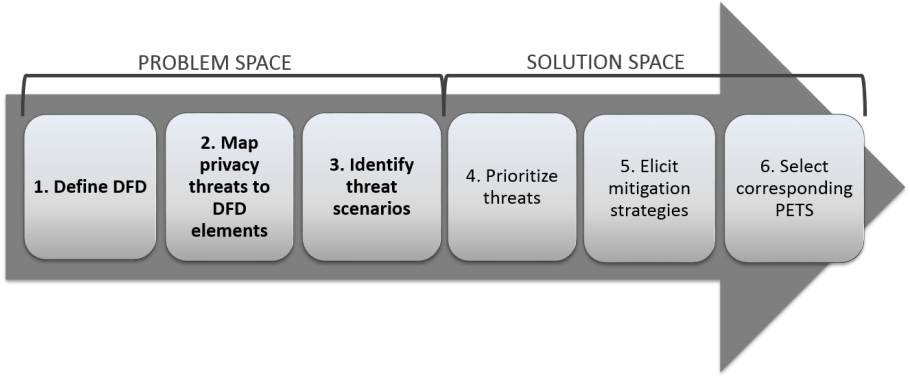
**Summary:** Data entries can be linked to the same person (without necessarily revealing the persons identity)
**Assets, stakeholders and threats:** Personal Identifiable Information (PII) of the user.
– Data entries can be linked to each other which might reveal the persons identity
– The misactor can build a profile of a user's on- line activities (interests, actives time, comments, updates, etc.)
**Primary misactor:** skilled insider / skilled outsider
**Basic Flow:**
1. The misactor gains access to the database
2. The misactor can link the data entries together and pos- sibly re-identify the data subject from the data content
**Alternative Flow:**
1. The misactor gains access to the database
2. Each data entry is linked to a pseudonym
3. The misactor can link the different pseudonyms together (linkability of entity)
4. Based on the pseudonyms, the misactor can link the different data entries
**Preconditions:**
• no or insufficient protection of the data store
• no or insufficient data anonymization techniques applied

# LINDDUN: 3rd step: Template for misuse cases

- **Summary**
- **Assets, stakeholders and threats:** which assets are important for whom, and what could the damage be if the misuse succeeds.
- **Primary misactor:** charactise the attacker. Accidental or intentionally. Insider / person with a skill / or somebody else.
- **Basic flow:** describe actions of the misuse.
- **Alternative flow:** describe other ways in which the misuse could happen.
- **Preconditions:** describe weaknesses of system which allow the misuse to happen.

# LINDDUN: Overview of Steps in Methodology

- The first three steps address the **problem space** of a system
- The last three steps address the **solution space.**
  – Those steps are much less concrete.
- In order to analyse the solution space, an understanding of the available PETs is required.
- **That is the goal of this lecture!**



# LINDDUN: 4th step: Prioritizing Threats

- In many cases, not all threats can be addressed.
- Prioritise threats using criteria applicable for the system:
  - time constraints
  - budget constraints
  - risk assessment
- General formula for risk assessment proposed by LINDDUN:

**Risk = likelihood X impact**

# LINDDUN: 5th step: from threats to mitigation strategies

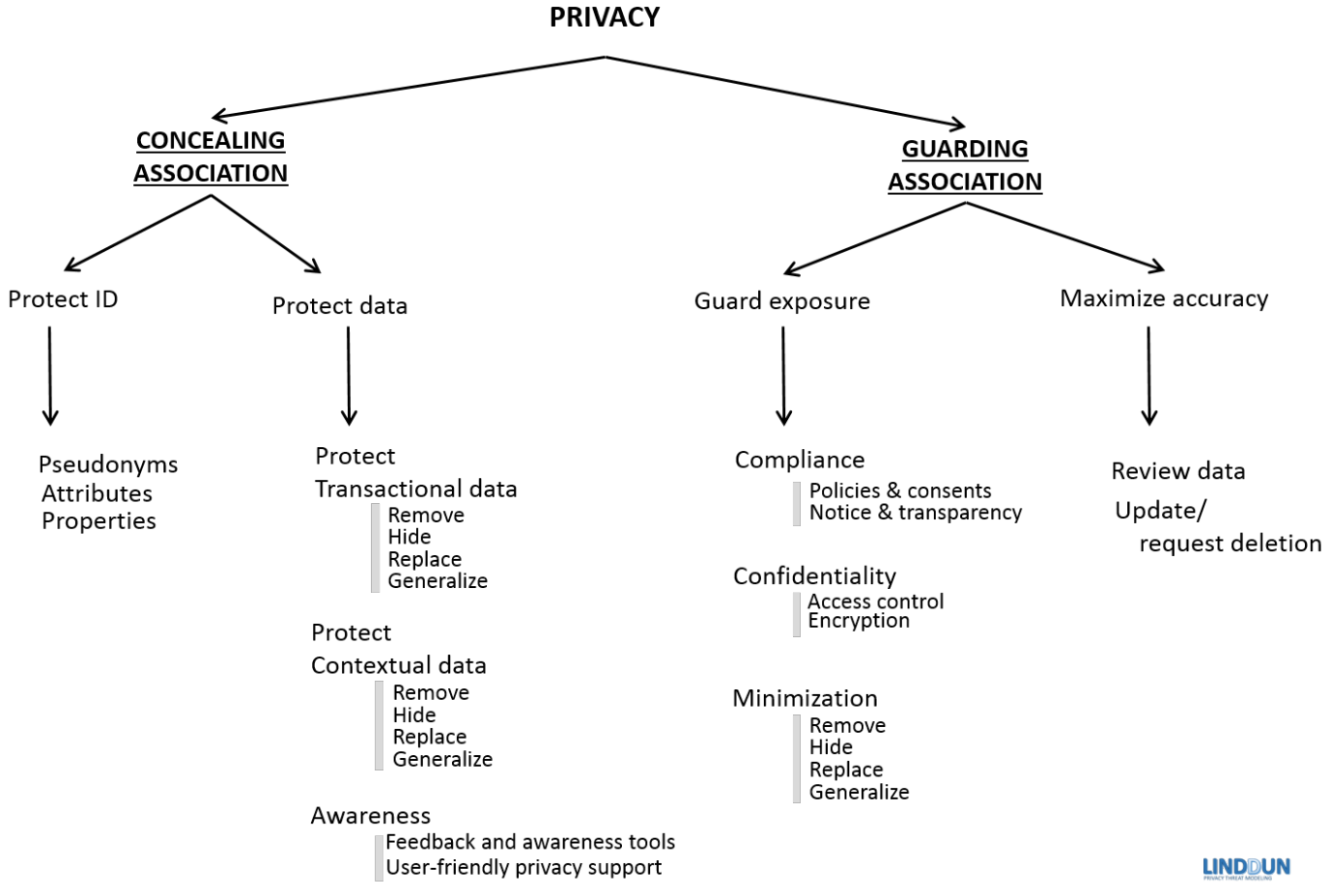
## Step A) Mapping the identified concrete threats to mitigation strategies

| Mitigation Strategy | LINDDUN Threat Tree |
|---|---|
| **Protect ID** | L_e, I_e |
| **Protect data** | |
| Transactional data | L_DF1, I_DF1 |
| Contextual data | L_DF2, I_DF2, D_DF, NR_DF |
| Awareness | U_1 |
| **Guard exposure** | |
| Compliance | NC |
| confidentiality | ID_DS, NR_DS, *_P |
| Minimization | L_DS, I_DS, D_DS |
| **Maximize accuracy** | |
| Review data | U_2 |
| Update/request deletion | NR_DS3 |

LINDDUN

# LINDDUN: 5th step: from Threats to Mitigation Strategies

## Step B) Select mitigation approach from the taxonomy of mitigation strategies



# LINDDUN: 6th step: from Strategies to Privacy Enhancing Technologies (PET)

## Now select a concrete PET matching the selected strategy

| Mitigation Strategy | | | | | Privacy Enhancing Techniques (PETs) |
|---|---|---|---|---|---|
| Concealing association | Protect ID | Pseudonyms | | | Privacy enhancing identity management system [HBC+04], User-controlled identity management system [CPHH02] |
| | | Attributes | | | Privacy preserving biometrics [STP09], Private authentication [AF04, ABB+04] |
| | | Properties | | | Anonymous credentials (single show [BC93], multishow [CL04]) |
| | Protect data | Transactional data | Remove | | (see awareness to minimize information sharing) |
| | | | Hide | Data-flow specific | Multi-party computation (Secure function evaluation) [Yao82, NN01], Anonymous buyerseller watermarking protocol [DBPP09] |
| | | | | General | see guard exposure - Confidentiality - encryption |
| | | | Replace | | / |
| | | | Generalize | | see guard exposure - minimization - generalize |
| | | Contextual data | Remove | | Mix-networks (1981) [Cha81], , ISDN-mixes [PPW91], Onion Routing (1996) [GRS96],Tor (2004) [DMS04]) |
| | | | Hide | General | Crowds (1998) [RR98], Low-latency communication (Freedom Network (1999-2001) [BGS01], Java Anon Proxy (JAP) (2000) [BFK00] |
| | | | | Undetectability | Steganography [AP98] , Covert communication [MNCM03], Spread spectrum [KM01] |
| | | | | Non-repudiation | Deniable authentication [Nao02], Off-the-record messaging [BGB04] |
| | | | Replace | | Mixmaster Type 2 (1994) [Mixa],Mixminion Type 3 (2003) [Mixb]) Single proxy (90s) (Penet pseudonymous remailer (1993-1996), Anonymizer, SafeWeb), anonymous Remailer (Cipherpunk Type 0, Type 1 [Bac], |
| | | | Generalize | Undetectability | dummy traffic, DC-networks (1985) [Cha85, Cha88] |
| | | Awareness | Feedback and awareness tools | | Feedback tools for user privacy awareness [LHDL04, PK09, LBW08] |
| | | | User-friendly privacy support | | Data removal tools (spyware removal, browser cleaning tools, activity traces eraser,harddisk data eraser) |
| Guarding association | Guard exposure | Compliance | Policies and Consents | | Policy communication (P3P [W3C]), Policy enforcement (XACML [oo], EPAL [IBM]) |
| | | | Notice and Transparency | | / |
| | | Confidentiality | Encryption | | Symmetric key & public key encryption [MOV97], Deniable encryption [Nao02],Homomorphic encryption [FG07] , Verifiable encryption [CD98] |
| | | | Access control | | Context-based access control [GMPT01], Privacy-aware access control [CF08, ACK+09] |
| | | Minimization | Remove | | / |
| | | | Hide | Receiver privacy | Private information retrieval [CGKS98], Oblivious transfer [Rab81, Cac98]) |
| | | | | Database privacy | Privacy preserving data mining [VBF+04, Pin02], Searchable encryption [ABC+05],Private search [OS05] |
| | | | | General | see guard exposure - confidentiality - encryption |
| | | | Replace | | / |
| | | | Generalize | | K-anonymity model [Swe02b, Swe02a], l-Diversity [MGKV06] |
| | Maximize accuracy | Review data | | | / |
| | | Update/ request deletion | | | / |

LINDDUN

# LINDDUN: 6th step: from Strategies to Privacy Enhancing Technologies (PET)

## Now select a concrete PET matching the selected strategy

| Mitigation Strategy | | | | | Privacy Enhancing Techniques (PETs) |
|---|---|---|---|---|---|
| Concealing association | Protect ID | Pseudonyms | | | Privacy enhancing identity management system [HBC+04], User-controlled identity m |
| | | Attributes | | | Privacy preserving biometrics [STP09], Private authentication [AF04, ABB+04] |
| | | Properties | | | Anonymous credentials (single show [BC93], multishow [CL04]) |
| | Protect data | Transactional data | Remove | | (see awareness to minimize information sharing) |
| | | | Hide | Data-flow specific | Multi-party computation (Secure function evaluation) [Yao82, NN01], Anonymous buy |
| | | | | General | see guard exposure - Confidentiality - encryption |
| | | | Replace | | / |
| | | | Generalize | | see guard exposure - minimization - generalize |
| | | Contextual data | Remove | | Mix-networks (1981) [Cha81], , ISDN-mixes [PPW91], Onion Routing (1996) [GRS96],T |
| | | | Hide | General | Crowds (1998) [RR98], Low-latency communication (Freedom Network (1999-2001) [ |
| | | | | Undetectability Non-repudiation | Steganography [AP98] , Covert communication [MNCM03], Spread spectrum [KM01] Deniable authentication [Nao02], Off-the-record messaging [BGB04] |
| | | | Replace | | Mixmaster Type 2 (1994) [Mixa],Mixminion Type 3 (2003) [Mixb]) Single proxy (90s) ( Anonymizer, SafeWeb), anonymous Remailer (Cipherpunk Type 0, Type 1 [Bac], |
| | | | Generalize | Undetectability | dummy traffic, DC-networks (1985) [Cha85, Cha88] |
| | | Awareness | Feedback and awareness tools | | Feedback tools for user privacy awareness [LHDL04, PK09, LBW08] |
| | | | User-friendly privacy support | | Data removal tools (spyware removal, browser cleaning tools, activity traces eraser,ha |

# LINDDUN: 6th step: from Strategies to Privacy Enhancing Technologies (PET)

## Now select a concrete PET matching the selected strategy

| | | | | | |
|---|---|---|---|---|---|
| | | Contextual data | Hide | Undetectability<br>Non-repudiation | Steganography [AP98] , Covert communication [MNCM03], Spread spectrum [KM01]<br>Deniable authentication [Nao02], Off-the-record messaging [BGB04] |
| | | | Replace | | Mixmaster Type 2 (1994) [Mixa],Mixminion Type 3 (2003) [Mixb]) Single proxy (90s) (P<br>Anonymizer, SafeWeb), anonymous Remailer (Cipherpunk Type 0, Type 1 [Bac], |
| | | | Generalize | Undetectability | dummy traffic, DC-networks (1985) [Cha85, Cha88] |
| | | Awareness | Feedback and awareness tools | | Feedback tools for user privacy awareness [LHDL04, PK09, LBW08] |
| | | | User-friendly privacy support | | Data removal tools (spyware removal, browser cleaning tools, activity traces eraser,ha |
| Guarding association | | Compliance | Policies and Consents | | Policy communication (P3P [W3C]), Policy enforcement (XACML [oo], EPAL [IBM]) |
| | | | Notice and Transparency | | / |
| | | Confidentiality | Encryption | | Symmetric key & public key encryption [MOV97], Deniable encryption [Nao02],Homon<br>[CD98] |
| | | | Access control | | Context-based access control [GMPT01], Privacy-aware access control [CF08, ACK+09] |
| | **Guard exposure** | Minimization | Remove | | / |
| | | | Hide | Receiver privacy | Private information retrieval [CGKS98], Oblivious transfer [Rab81, Cac98]) |
| | | | | Database privacy | Privacy preserving data mining [VBF+04, Pin02], Searchable encryption [ABC+05],Priva |
| | | | | General | see guard exposure - confidentiality - encryption |
| | | | Replace | | / |
| | | | Generalize | | K-anonymity model [Swe02b, Swe02a], l-Diversity [MGKV06] |
| | **Maximize accuracy** | Review data | | | / |
| | | Update/ request deletion | | | / |

# Review of LINDDUN methodology

# Categorization of Privacy Threats in LINDDUN

**Hard Privacy Threats**

| | |
|---|---|
| **Linkability(L):** | Determine if IOI's belong together |
| **Identifiability(I):** | Determine real world identity among anonymity set |
| **Non-repudiation(N)** | Proof that event or action happened |
| **Detectability(D)** | Determine if an IOI exists or nor, independent of knowing content |
| **Disclosure of information(D)** | Exposing information to someone not authorized to see it. |

# Categorization of Privacy Threats in LINDDUN

**Soft Privacy Threats**

| | |
|---|---|
| **Unawareness(U)** | Not understanding the consequences of sharing personal information in the past, present or future. |
| **Policy and consent non-compliance(N)** | Not following the (data protection) legislation, the advertised policies or the existing user consents. |

# Clarification on Non-Repudiation

## Cryptography context

- A service that provides proof of the integrity and origin of data
- Or an authentication that can be asserted to be genuine with high assurance.

## Security threat modelling

- Non-repudiation is a **desirable** system property, which **reduces** security threats
- Implementing non-repudiation in a system results in full **accountability** of all users
- This provides proof of attacker actions after the attack

# Clarification on Non-Repudiation

## Privacy threat modelling

- Non-repudiation is an **undesirable** system property, which **adds** privacy threats
- Eliminating all non-repudiation threats results in **plausible deniability**
- This enables users to deny using a system or being in a data set or having performed an action.

# Modifying the LINDDUN Methodology for this Lecture

- LINDDUN provides vocabulary to identify and analyze privacy threats
- LINDDUN methodology enumerates ALL potential threats in a system
- Great for designing and analyzing industrial projects, but beyond the scope of this lecture

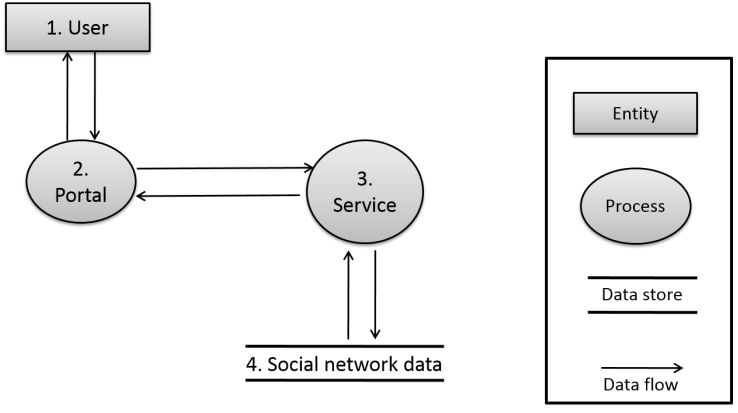
→ We will reuse the following

- LINDDUN threat categories
- 1st step: Define Data Flow Diagram (DFD)
- 2nd step: Mapping the DFD to LINDDUN threat categories
- 3rd step: Eliciting privacy threats for each relevant DF element (without using the misuse case template)

# LINDDUN: 1st step: Define Data Flow Diagram (DFD)

## LINDDUN Problem Space analysis

- **Process (P):** any kind of software operating on the data
- **Data store (DS):** a passive container of data
- **External entity (E):** a source or destination of data, such as a user of the system or external 3rd party services
- **Data flow (DF):** a named flow of data
- Optional: add dashed lines to indicate **trust boundaries**, where parties with different privileges / levels of trust interact



# LINDDUN: 2nd step: Mapping the DFD to LINDDUN Threat Categories

## LINDDUN Problem Space Analysis

- For each element in the DFD, identify the threats which are applicable the element
- Put a number on threats in the table which should be analyzed
- Document your assumptions, if you want to exclude a threat to a specific element

| | Threat target | L | I | N | D | D | U | N |
|---|---|---|---|---|---|---|---|---|
| Data Store | Social network DB | 1 | 4 | × | × | 7 | | 10 |
| Data Flow | User data stream (user – portal) | 2 | 5 | × | × | 8 | | 10* |
| | Service data stream (portal – service) | × | × | × | × | × | | 10* |
| | DB data stream (service – DB) | × | × | × | × | × | | 10* |
| Process | Portal | × | × | × | × | × | | 10* |
| | Social network service | × | × | × | × | × | | 10* |
| Entity | User | 3 | 6 | | | | 9 | |

# LINDDUN: 3rd step: Eliciting Privacy Threats

**LINDDUN Problem Space Analysis**

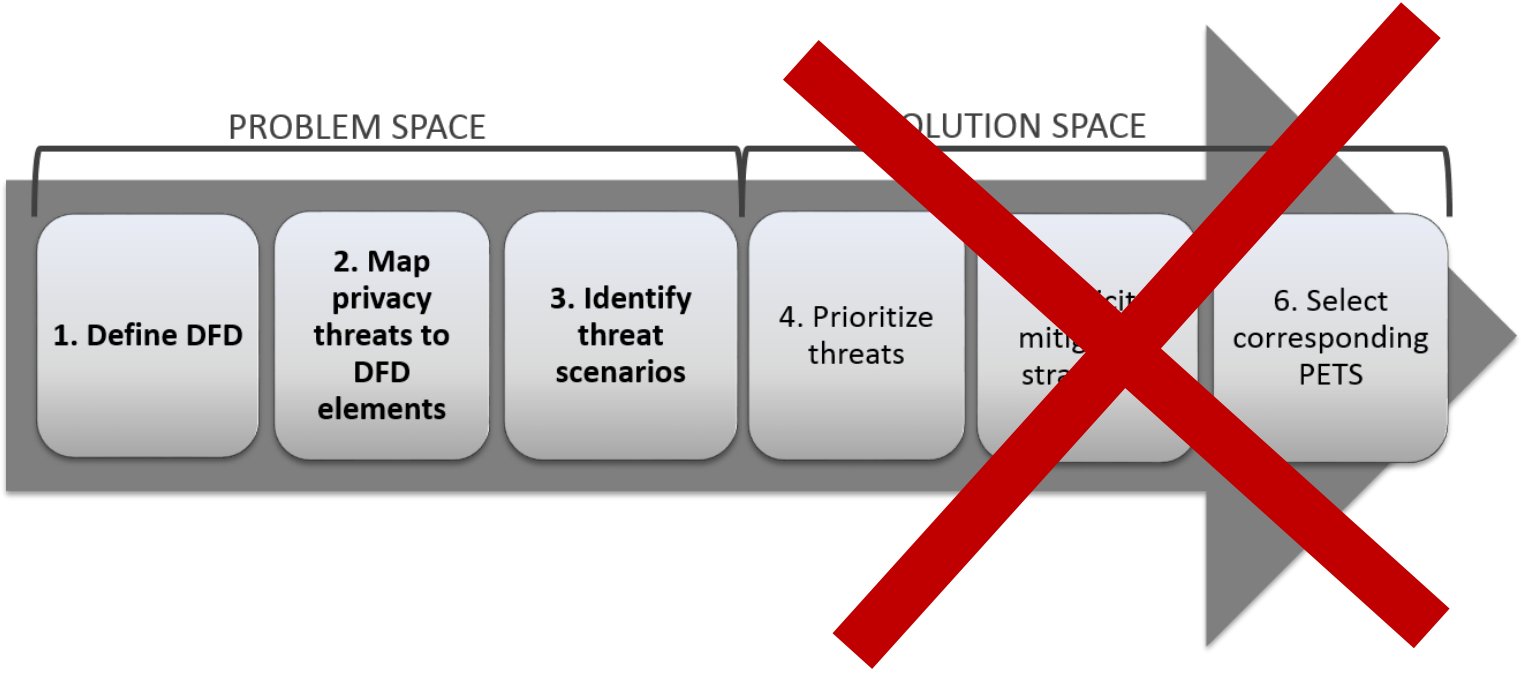
- **Idea:** Look at each remaining potential privacy threat, and think about how it could be attacked

- The LINDDUN Authors suggest that this step has three sub-steps:
  - A.) Refine (abstract) threats via the threat tree pattern into concrete threats
  - B.) Document if any concrete threats are not relevant to the system.
  - C.) Document threats as misuse cases (also called “threat scenario”)

- For the scope of this lecture, we consider these 3 sub-steps optional

- But if you can’t think of a threat, it makes sense to consult the threat tree documentation

# LINDDUN: Overview of Steps in Methodology



# Applying LINDDUN to a Real World Example

# Background: News Reports on Merchants of Personal Browsing Histories

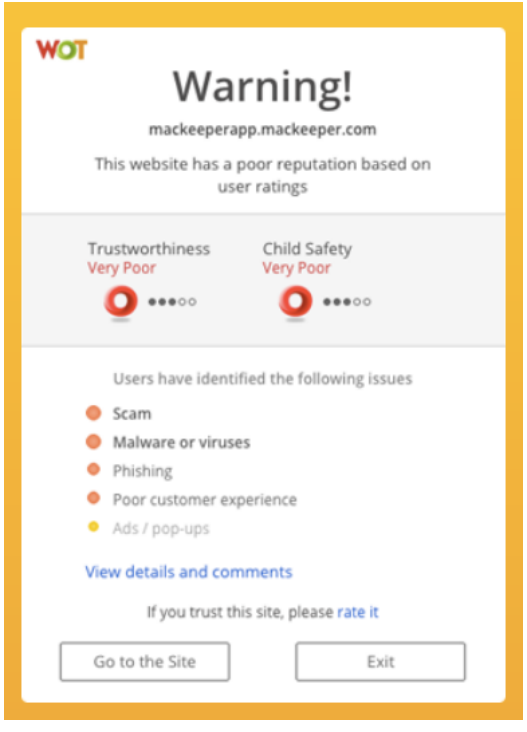
- On 1.11.2016, German media[1] reported on **personal browsing histories** for sale
- Reporters were able to **de-anonymise data** about:
  - Politicians
  - Judges
  - Police personal
  - Reporters
- **Impact for society:** individuals become susceptible to blackmail

Where did this data come from?

# The Web Of Trust (WOT) Browser Plugin

## Web of Trust (WOT) Browser Plugin (900.000 active users)

- **Function of plugin:**
  - Warn users of un-trustworthy web sites
  - Collect ratings from users
- **Technical details:**
  - WOT is a browser plugin, it runs e.g. in Firefox
  - For every web page visited, it sends the following to the WOT main server: personal ID, current page, previously visited page
  - Source code for WOT plugin is on Github
- **Legal details:**
  - EULA claims that only non-personal information is collected.
  - EULA claims that if no product registration is performed, then no data is collected.

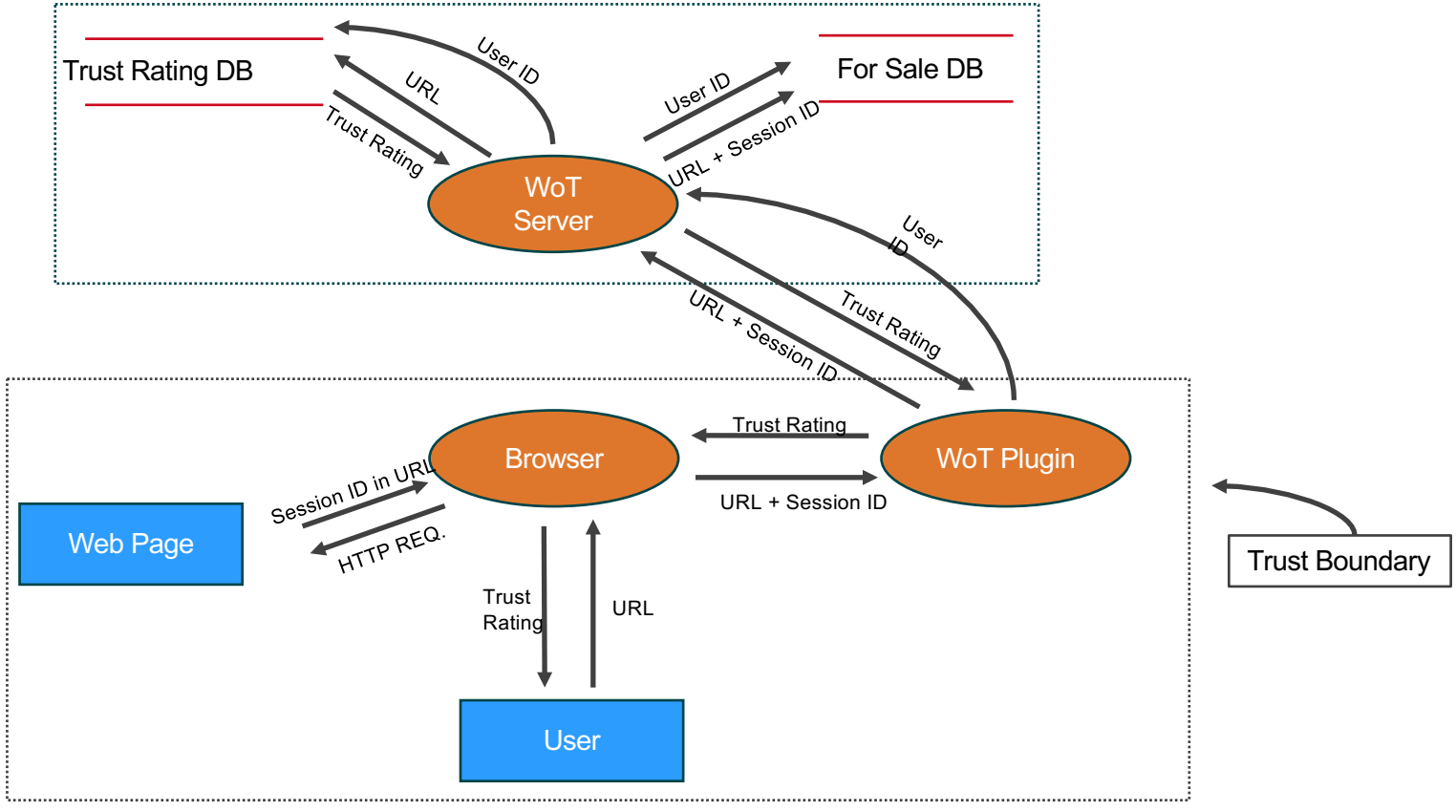



Technical details in German at: https://www.kuketz-blog.de/wot-addon-wie-ein-browser-addon-seine-nutzer-ausspaeht/

# Privacy Breach from the Web Of Trust (WOT) Browser Plugin

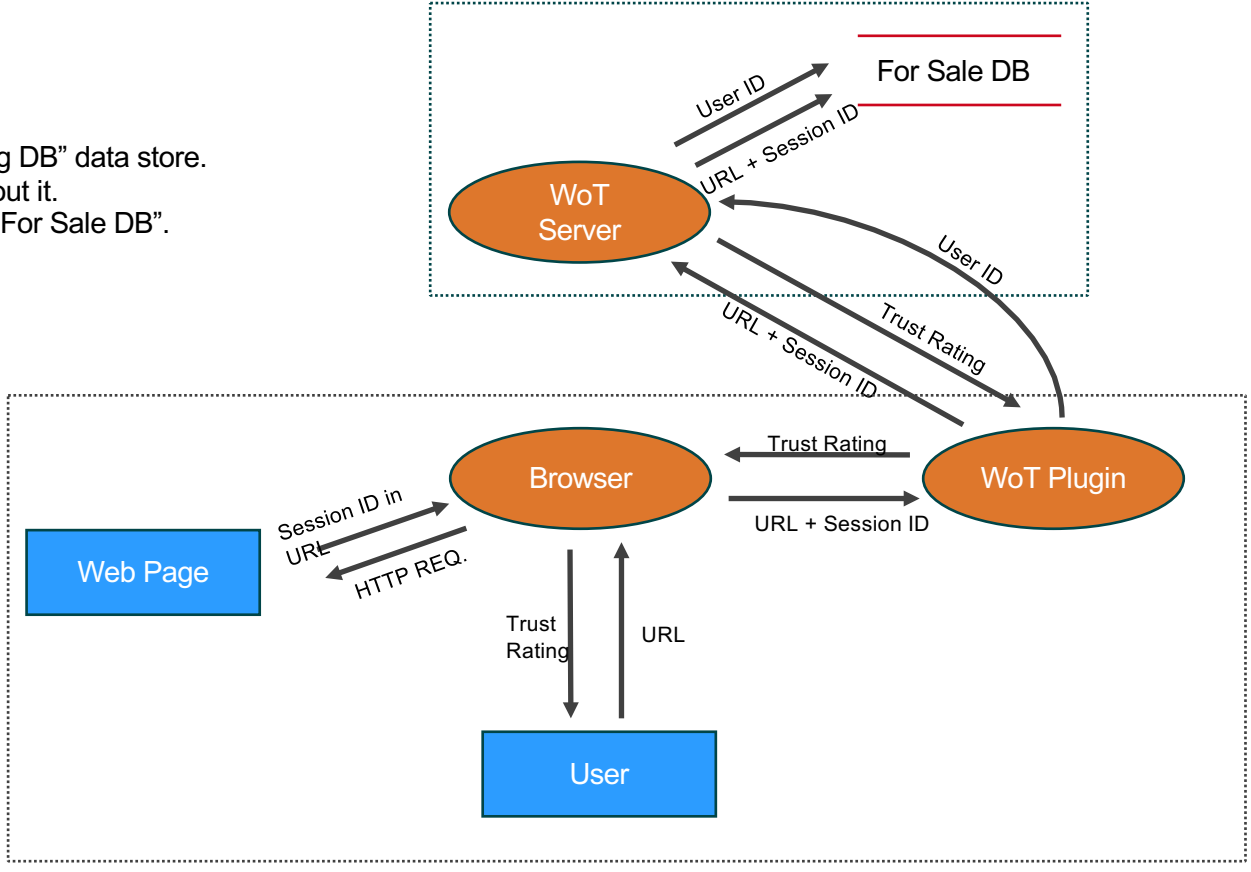
- **Privacy breach:**
  - WOT collected complete surfing history of every plugin user
  - WOT sold these data sets commercially
  - WOT “anonymised” the data assigning every user a pseudonymous ID
- WOT sold data which contains URLs with **personally identifiable information (PII)**
  - User names
  - Unique UserID for web site e.g. Twitter, Skype
  - Frequently visited web pages such as employer
- Data also contained **sensitive information:**
  - E-commerce products
  - Text submitted to translation web site
  - Sexual preferences on porn sites

# LINDDUN 1st step: Define DFD Based in Available Details



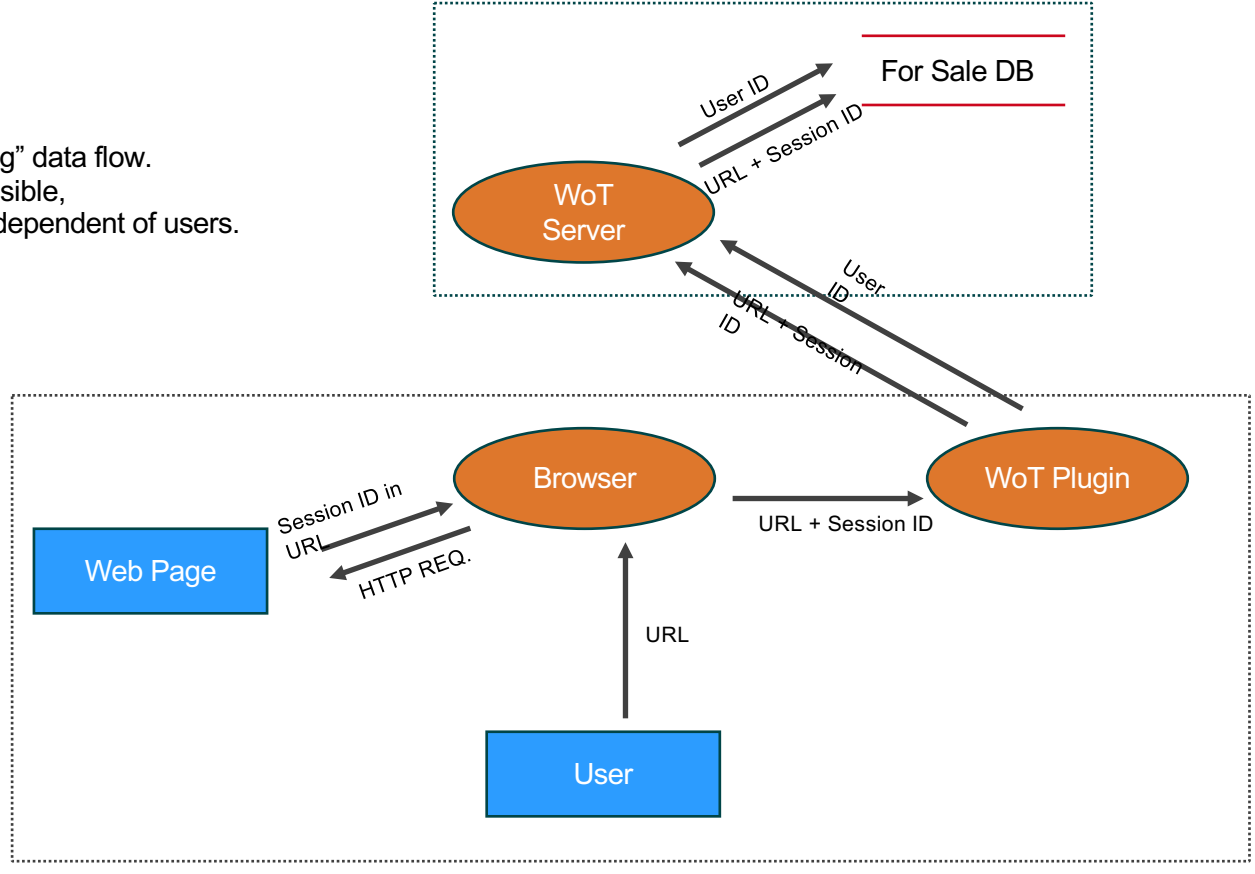
# LINDDUN 1st step: Define Minimal DFD

Assumption 1:
Remove “Trust Rating DB” data store.
No known details about it.
Less important than “For Sale DB”.



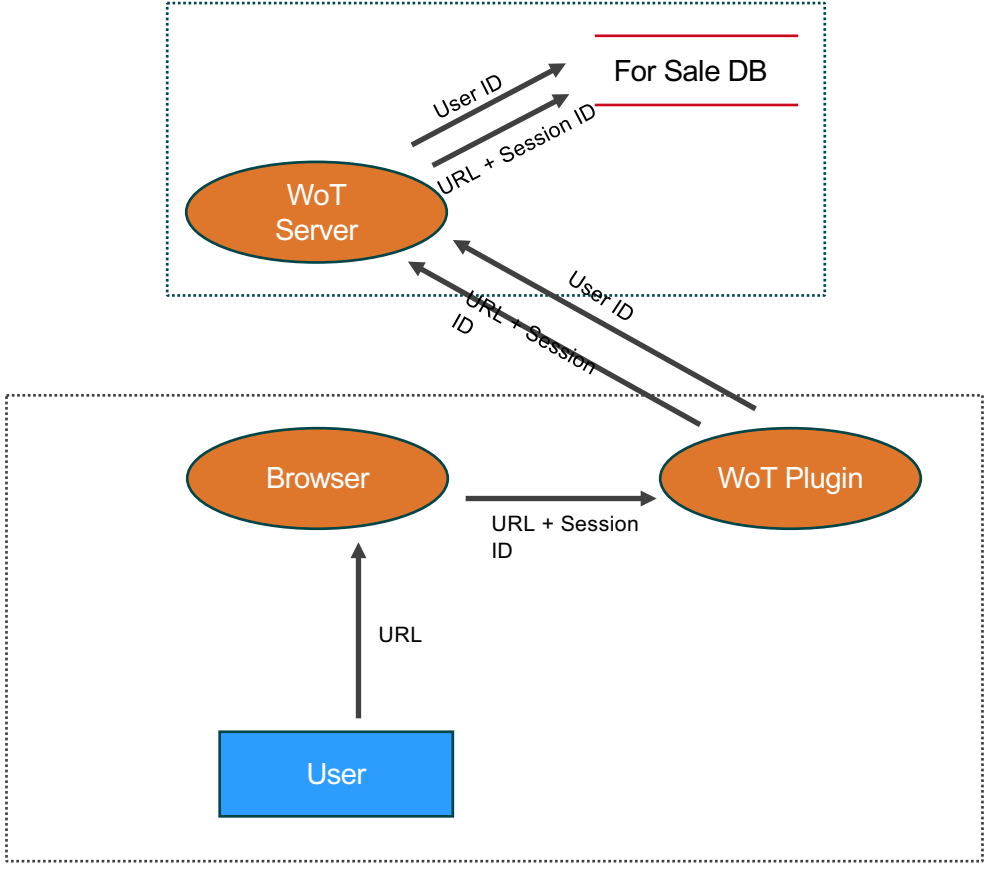
# LINDDUN 1st step: Define Minimal DFD

Assumption 2:
Remove “Trust Rating” data flow.
No privacy leaks possible,
as site ratings are independent of users.



# LINDDUN 1st step: Define Minimal DFD

Assumption 3:
Remove “Web site” external entity.
For DFD it is enough that WoT Plugin gets URL+SessionID from browser.



# LINDDUN 2nd step: Mapping the Minimal DFD to LINDDUN Threat Categories

| DFD Element | L Linkability | I Identifiability | N Non-repudiation | D Detectability | D Disclosure | U Unawareness | N Non-compliance |
|---|---|---|---|---|---|---|---|
| Data Store "For Sale DB" | | | | | | | |
| Data Flow WOT Plugin to WOT Server | | | | | | | |
| User of WOT Plugin | | | | | | | |
| Whole WOT System | | | | | | | |

These are the DFD elements which are still relevant for a privacy threat analysis.

# LINDDUN 2nd step: Mapping the Minimal DFD to LINDDUN Threat Categories

| | L | I | N | D | D | U | N |
|---|---|---|---|---|---|---|---|
| **Entity** | X | X | | | | X | |
| **Data store** | X | X | X | X | X | | X |
| **Data flow** | X | X | X | X | X | | X |
| **Process** | X | X | X | X | X | | X |

Use this table to determine which threats apply to which types of DFD elements.

# LINDDUN 2nd step: Mapping the Minimal DFD to LINDDUN Threat Categories

| DFD Element | L Linkability | I Identifiability | N Non-repudiation | D Detectability | D Disclosure | U Unawareness | N Non-compliance |
|---|---|---|---|---|---|---|---|
| Data Store "For Sale DB" | X | X | X | X | X | | |
| Data Flow WOT Plugin to WOT Server | X | X | X | X | X | | |
| User of WOT Plugin | X | X | | | | X | |
| Whole WOT System | | | | | | | X |

Every X marks a potential privacy threat, which we need to consider for analysis.

# Examples of Attacks on the Data Set

- **Re-Identification of judge:**
  - Browsing history contained URL of e-commerce site for buying robes (e.g. http://www.natterer-roben.de/)
  - Some form of real world identity
  - URLs of porn sites with information about specific sexual preferences
- **Re-identification of reporters:**
  - Creation of web server with secret sub-domain
  - Installation of clean virtual machine (VM)
  - Only Firefox with WOT Plugin installed in the VM
  - Wait until secret sub-domain appears in data set
- **Re-identification of police man:**
  - police man used Google Translate to translate a complete letter to English
  - letter text included his real name

# 3rd step: Eliciting Privacy Threats for each Relevant DF Element

**Data store "For Sale DB"**

- **Linkability: yes**
  - from the news articles, we can assume that URLs from the same user are grouped together in the "For Sale DB"
  - URLs which are saved in the same group, can be linked to the same user
  - Multiple groups of URLs could be linked if the contain the same URLs with the same session IDs
  - Example: profile from Laptop and working PC can be linked

- **Identifiability: yes**
  - whenever a group of URLs contains a real name or personal page
  - real world identity for user can be identified
  - in other cases, the most frequently visited pages could contain identity

- **Non-repudiation: yes**
  - The data set can be used to prove that a user has WOT installed
  - The PIIs can be used to prove that a person viewed certain URLs
  - This makes the users susceptible to blackmail

# 3rd step: Eliciting privacy threats for each relevant DF element

**Data store “For Sale DB”**

- **Detectability: yes**
  - its possible to show that a user visited a page without knowing what the page contains
  - Example: we could see a e-banking URL, without knowing the account balance.

- **Disclosure of information: yes**
  - as the data is for sale, attackers who are not meant to have access to it, can gain access.
  - The URLs can contain information which are PIIs or sensitive details
  - Example: email text passed to Google translate via URL

- **Summary:**
  - insufficient removal and / or anonymisation of PIIs in data store “For Sale DB”
  - data minimisation is not done
  - the WOT service could also be provided based on collecting only domain names

# 3rd step: Eliciting privacy threats for each relevant DF element

**Data flow from WOT Plugin to WOT Server**

- **Linkability: yes**
  - The WOT user ID is sent to the server unmasked
  - An attacker who can intercept traffic can link individual communications with the server via the userID
  - An attacker could intercept Wifi traffic or could perform a man in the middle attack from inside Internet Service Provider
- **Identifiability: no**
  - All the PII is in the URLs are masked when sent to server
- **Non-repudiation: yes (but depends on attack)**
  - The message which the WOT plugin sends to the server has specific format
  - Allows proving that a user has WOT plugin installed
  - However specific URLs can not be intercepted without access to ”for sale” database.

# 3rd step: Eliciting Privacy Threats For each Relevant DF Element

**Data flow from WOT Plugin to WOT Server**

- **Detectability: no (but depends on the attack)**
  - its not possible to show which pages a user visited
  - but it is possible to show that a user has WOT plugin installed
- **Disclosure of information: no**
  - all PII and IOIs are masked when they are sent to the server
  - no disclosure of data is possible from the data flow alone
- **Summary:**
  - the WOT userID should at least be masked like the URLs
  - or just not generate a userID at all
  - data minimization principle is not followed

# 3rd step: Eliciting Privacy Threats for each Relevant DF Element

**User of WOT plugin**

- **Linkability: depends on WOT account creation**
  - If the user has not created an account at WOT site, then he is not linkable via WOT credentials
  - If the user has a WOT account, he is linkable across different devices
- **Identifiability: depends on WOT account creation**
  - If the user has a WOT account, his real world identity can be identified
- **Unawareness: yes**
  - EULA clearly states that no PIIs are collected
  - User is unaware of what is happening without inspecting the traffic of the plug-in
- **Summary:**
  - WOT plugin is clearly not respecting the users privacy

# 3rd step: Eliciting Privacy Threats for each Relevant DF Element

**Whole system: WOT plugin and server, as well as staff of WOT**

- **Non-compliance: yes**
  - WOT sells data with PIIs but claims that it does not collect PIIs
  - This is a clear breach of the EULA on the side of WOT

# Summary of Privacy Threat Analysis of WOT Plugin

- WOT plugin is clearly in breach of its EULA
- Generating userID is unnecessary for functionality of plugin
- Sending full URL with session ID is unnecessary for functionality of plugin
- WOT plugin does not follow principle of data minimisation
- WOT data for sale is not sufficiently anonymised

- This analysis is based on the news reports and the technical analysis by Mr. Kuketz, without inspecting the WOT source code.

# Sources from the media (all in German)

- NDR Reportage “Nackt im Netz: Millionen Nutzer ausgespäht” (Text und Video)
  - https://www.ndr.de/nachrichten/netzwelt/Nackt-im-Netz-Millionen-Nutzer-ausgespaeht,nacktimnetz100.html
- Heise.de high level overview (Text)
  - https://www.heise.de/newsticker/meldung/Millionen-Surf-Profile-Daten-stammen-angeblich-auch-von-Browser-Addon-WOT-3453820.html
- Netzpolitik.org about the societal impact:
  - https://netzpolitik.org/2016/datenhungrige-browserplugins-machen-politiker-erpressbar-und-bedrohen-journalismus/
- Technical analysis of communication between WOT Plugin and WOT Server:
  - https://www.kuketz-blog.de/wot-addon-wie-ein-browser-addon-seine-nutzer-ausspaeht/
- WOT Plugin code for Firefox version:
  - https://github.com/mywot/firefox-xul