# Multilateral Privacy and Requirements Engineering in Information Systems

Seda Gürses
COSIC, ESAT

K.U. Leuven
Belgium

# Outline

- Introduction to Approach
- Privacy Requirements Analysis Problem
- MPRA Method
- Overview of MPRA Templates

# INTRODUCTION

# electronic toll pricing

- functional goal:
  - calculate personalized fees for each citizen depending on following parameters:
    - the distance covered
    - kind of road used

# straightforward implementation

- vehicles carry on board unit
  - collects position of the vehicle over time
    - e.g., GPS receiver
- the service provider receives location data from OBU
  - to compute the bill for each customer
  - prepare detailed consumption reports for customer
    - visualize detailed report in car

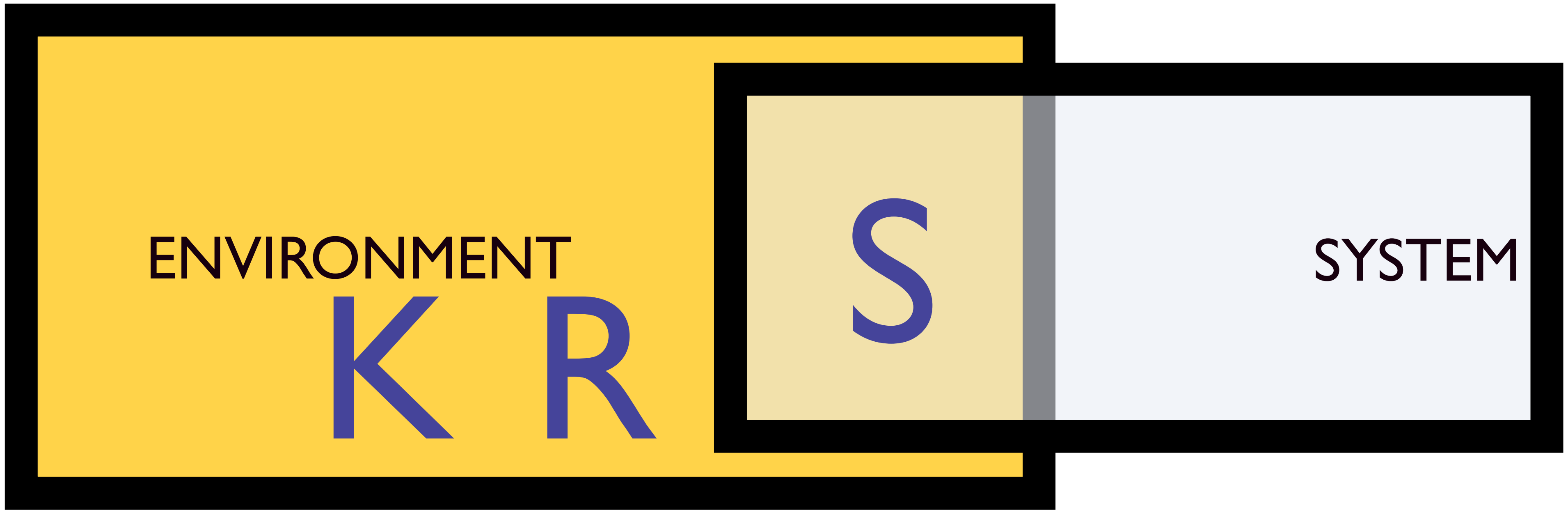
# any privacy concerns?

- for individuals?
  - e.g., a specialist doctor that visits patients with peculiar disease
  - e.g., an employer wants employees to share location reports
- for communities?
  - e.g., a rich and poor community whose neighborhood border
  - e.g., tax authority demands data for confirming tax returns
- for a car-sharing family?
  - e.g., parents and children

- all of these are (somehow) about privacy and the design of the system
- how do we deal with these issues when developing systems?
  - specifically: during requirements engineering

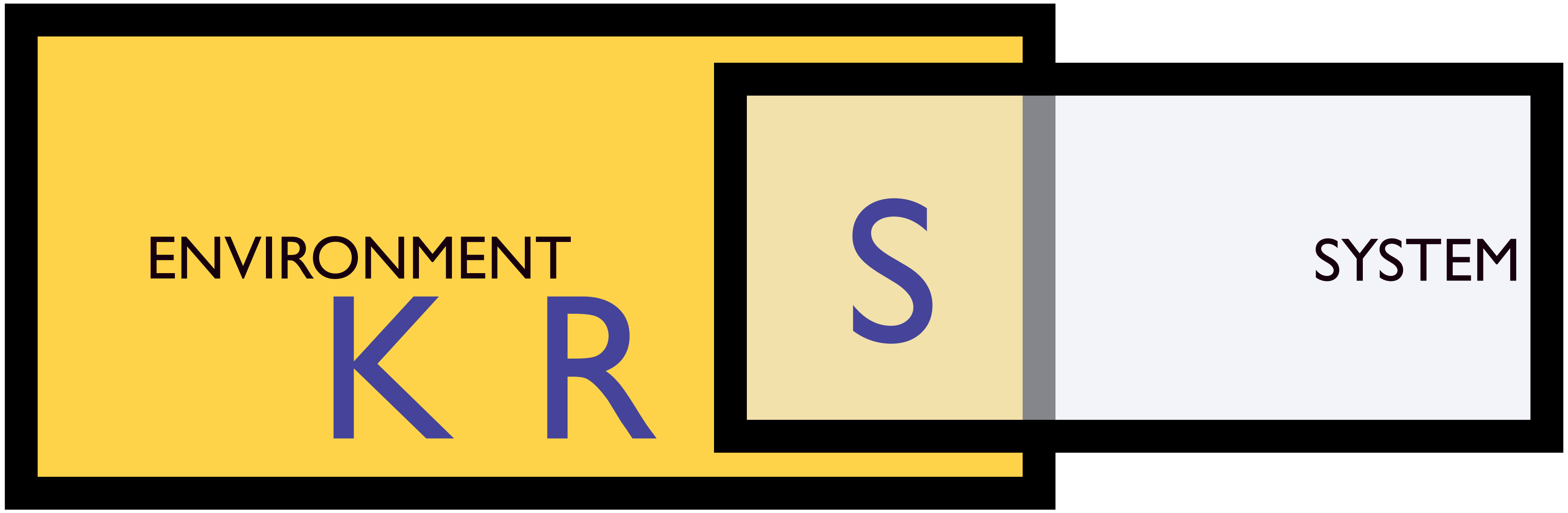
# PRIVACY REQUIREMENTS ANALYSIS PROBLEM

# Zave and Jackson Model of RE



- K: *domain assumptions* describe the behavior of the environment as it is
- R: *requirements* are statements about the desired conditions in an environment
- S: *specification* is a restricted form of requirement providing enough information for the engineer to implement the system

# Zave and Jackson Model of RE



$$K, S \vdash R$$

# requirements

- *functional requirements* state the desired behavior of the environment
- *non-functional requirements* either constrain the behavior of the environment or define certain desired qualities of the environment

# multilateral privacy requirements engineering

- reconcile:
  - privacy notions (legal & surveillance studies)
  - privacy solutions (computer science)
  - in a social context
  - multilaterally
  - during requirements engineering

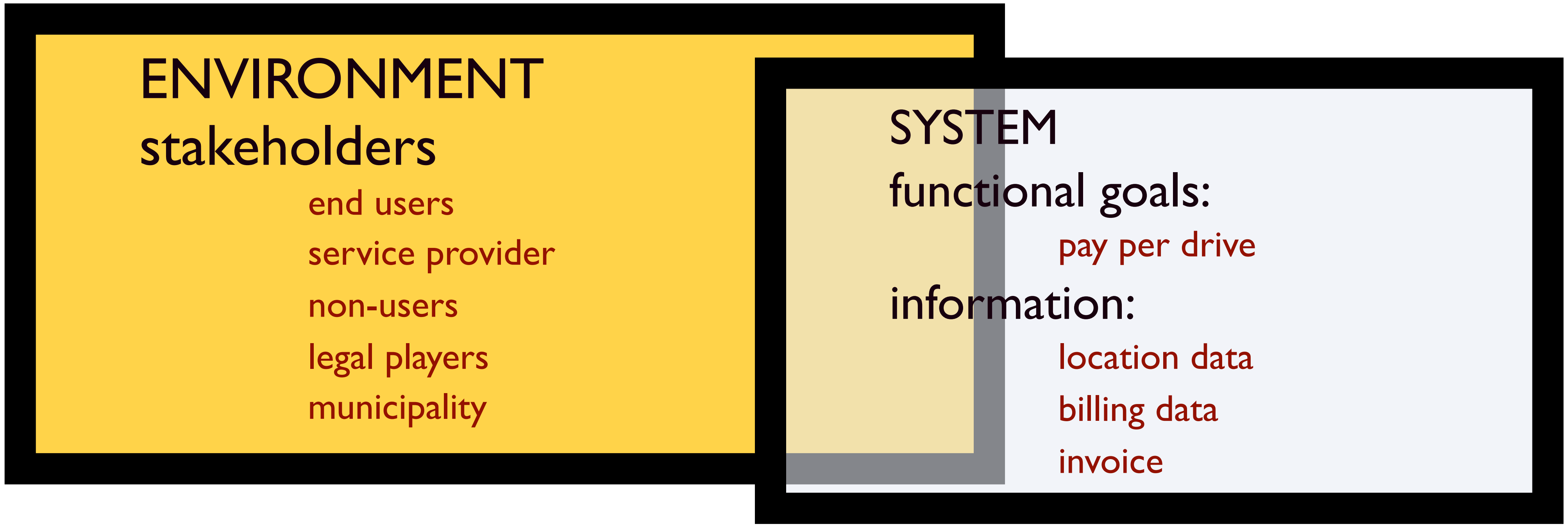
# multilatera analysis

ENVIRONMENT

stakeholders

- end users
- service provider
- non-users
- legal players
- municipality

# functional analysis



ENVIRONMENT

stakeholders

- end users
- service provider
- non-users
- legal players
- municipality

SYSTEM

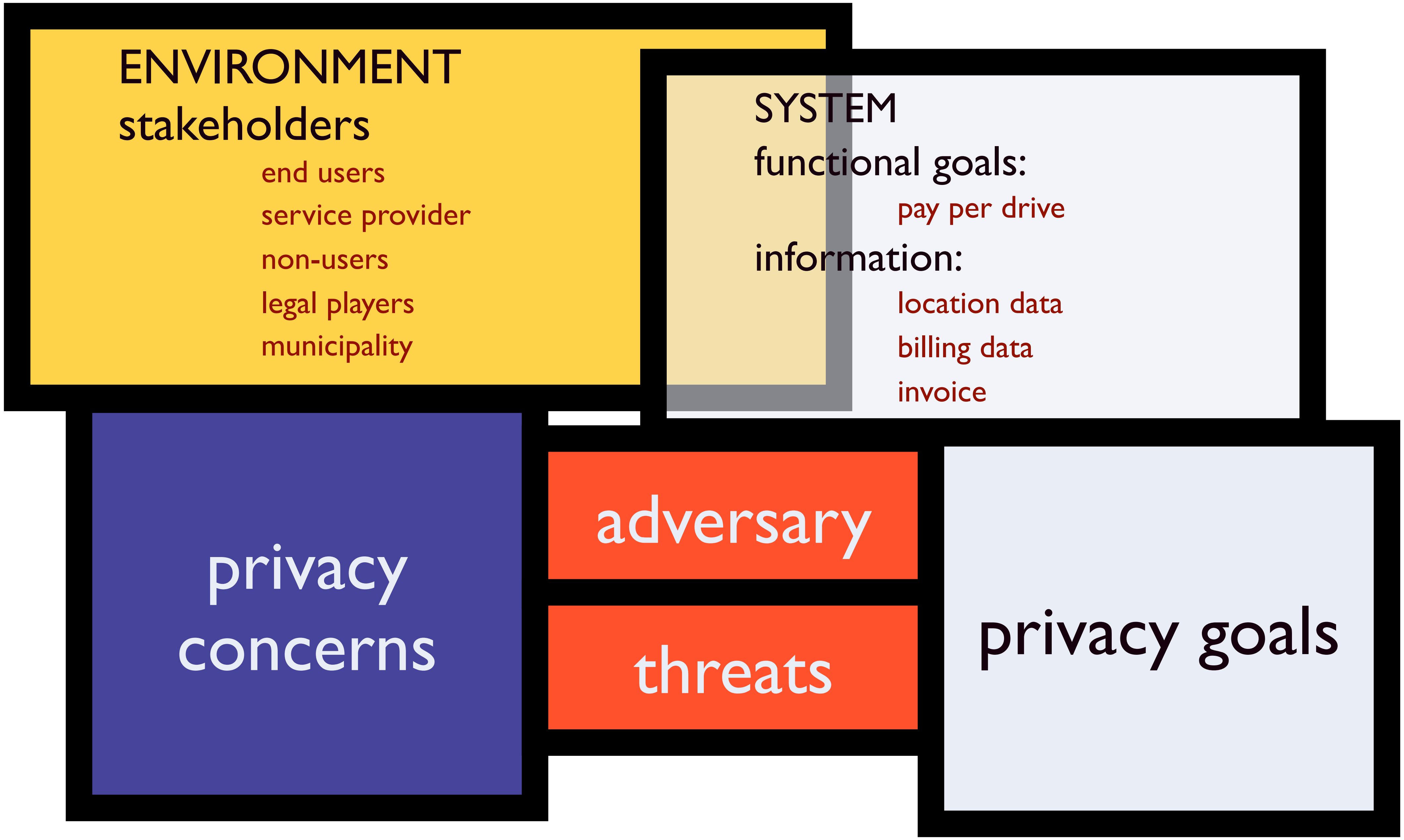
functional goals:

- pay per drive

information:

- location data
- billing data
- invoice

# privacy analysis



ENVIRONMENT

stakeholders

- end users
- service provider
- non-users
- legal players
- municipality

SYSTEM

functional goals:

- pay per drive

information:

- location data
- billing data
- invoice

privacy concerns

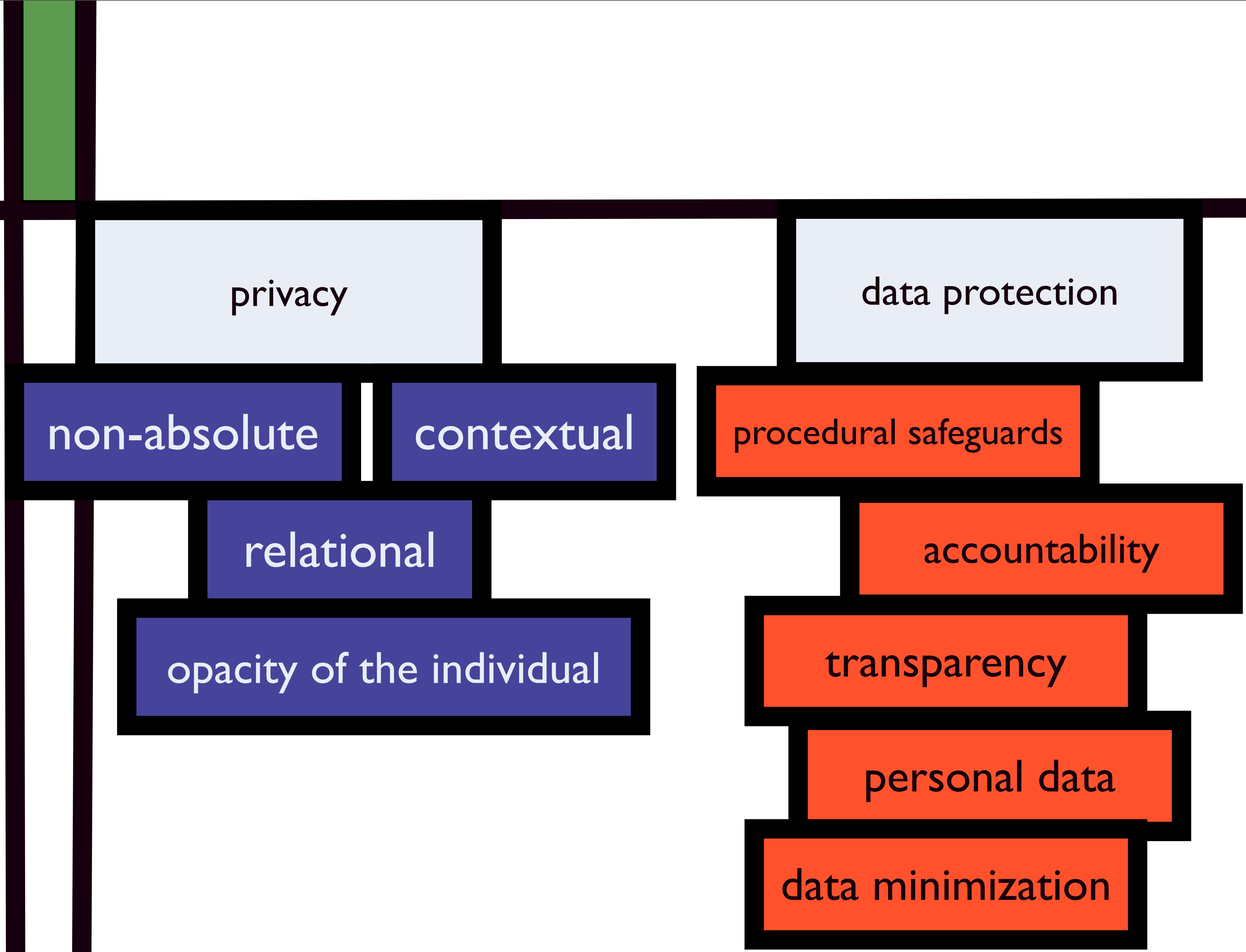
adversary

threats

privacy goals

# privacy?

- what is privacy?
- a non-functional requirement
    - in security engineering:
        - breach of confidentiality
    - anything else?



privacy

non-absolute

contextual

relational

opacity of the individual

data protection

procedural safeguards

accountability

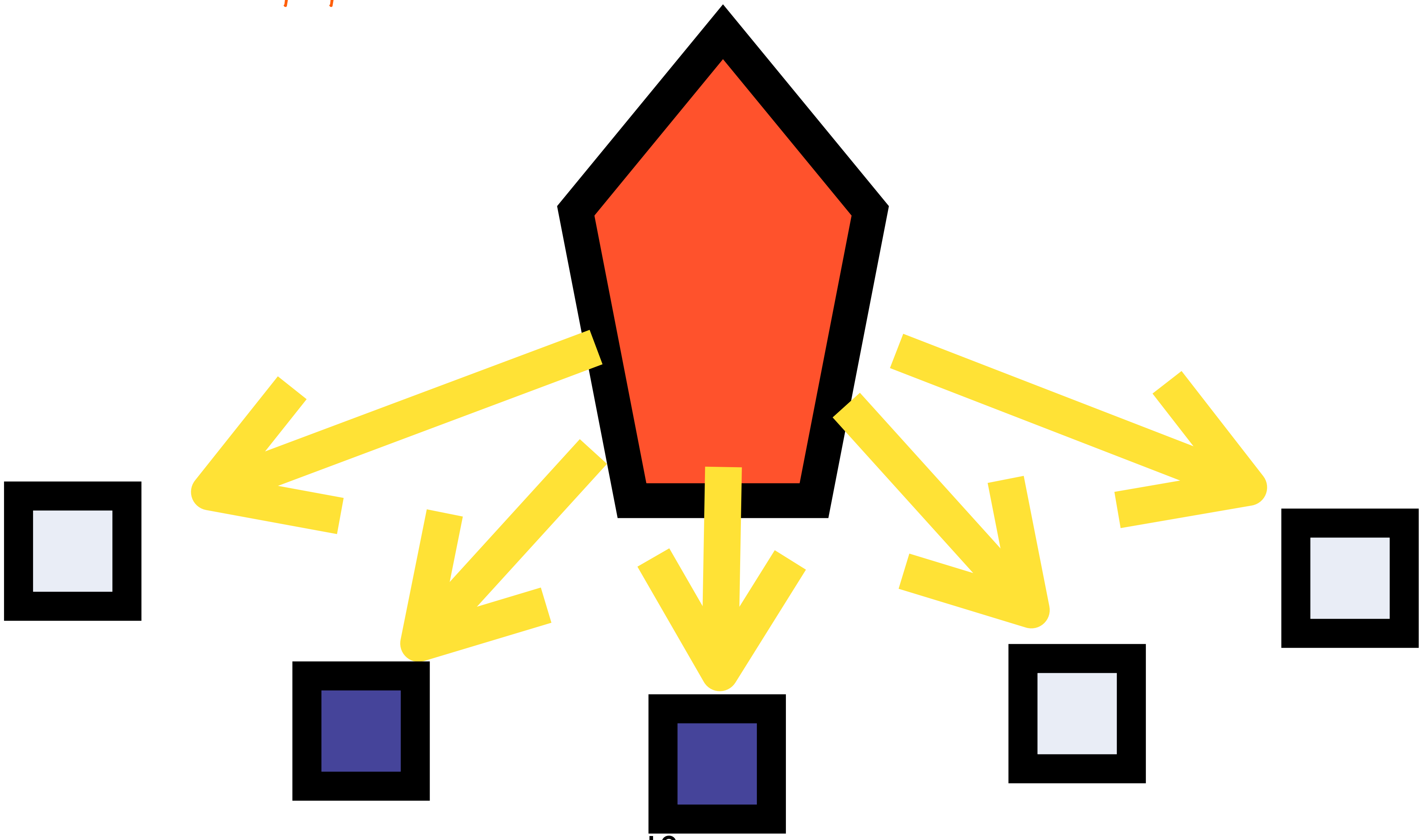
transparency

personal data

data minimization

# surveillance studies

Surveillance



# privacy requirements definition

lack of universality

lack of satisfiability

subjectivity

contrivability

agonism

legal compliance

negotiability

environmental factors

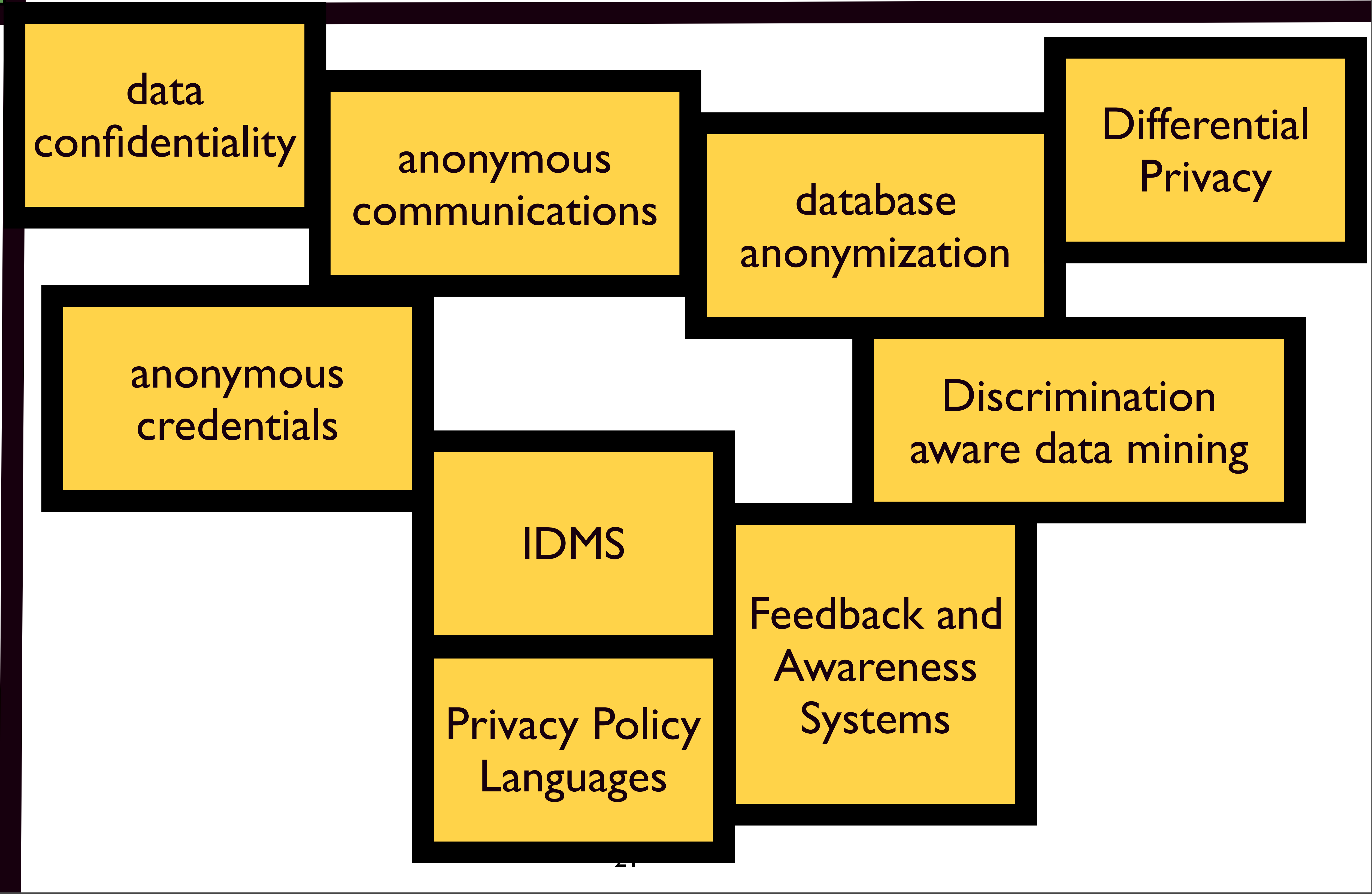
counter - factuality

temporality

# multilateral privacy requirements engineering

- reconcile:
    - privacy notions (legal & surveillance studies)
    - privacy solutions (computer science)
    - in a social context
    - multilaterally
    - during requirements engineering

# solutions from privacy research



data confidentiality

anonymous communications

database anonymization

Differential Privacy

anonymous credentials

Discrimination aware data mining

IDMS

Feedback and Awareness Systems

Privacy Policy Languages

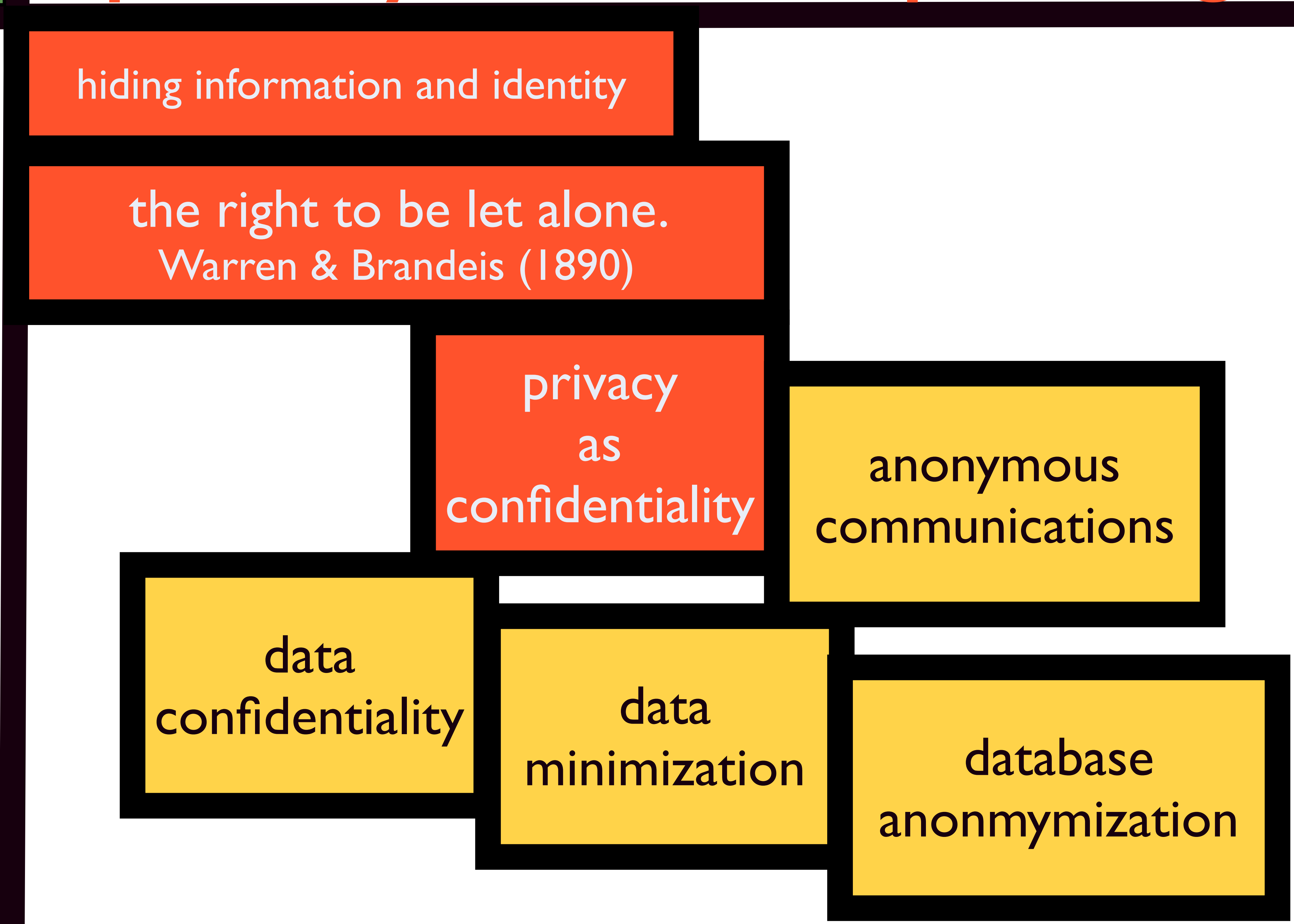
# privacy research paradigms

hiding information and identity

the right to be let alone.
Warren & Brandeis (1890)

privacy
as
confidentiality

# privacy research paradigms



hiding information and identity

the right to be let alone.
Warren & Brandeis (1890)

privacy
as
confidentiality

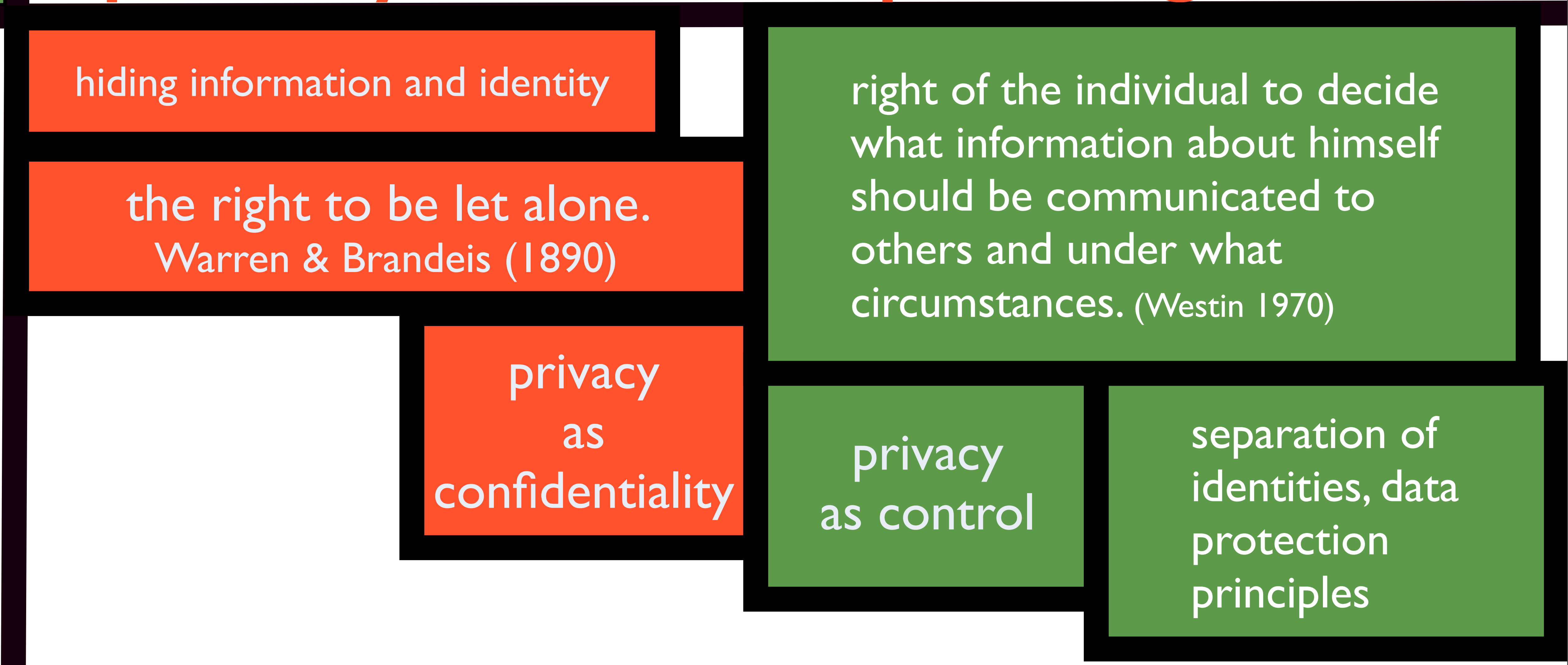
anonymous
communications

data
confidentiality

data
minimization

database
anonmymization

# privacy research paradigms



hiding information and identity

the right to be let alone.
Warren & Brandeis (1890)

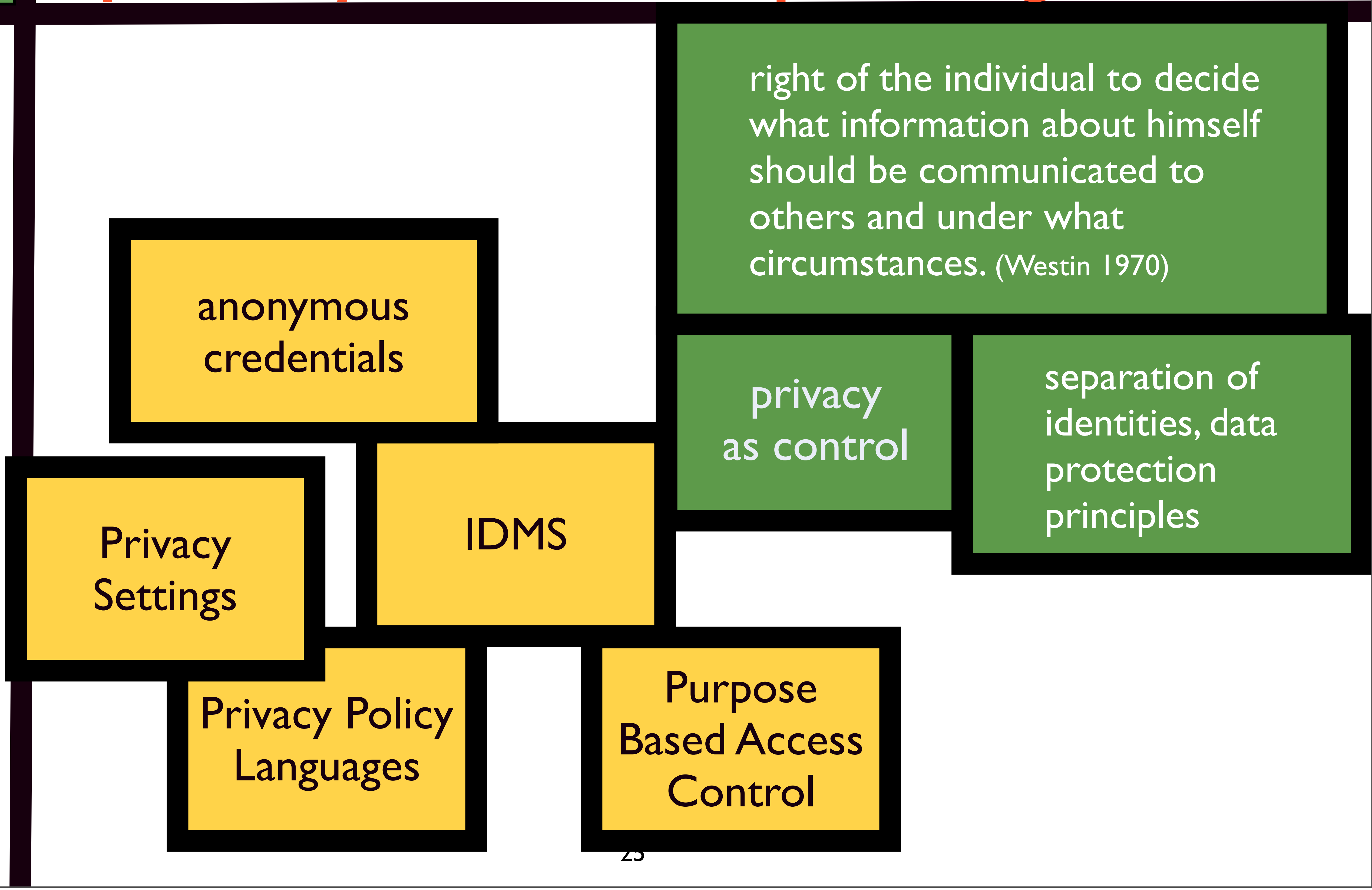
privacy as confidentiality

right of the individual to decide what information about himself should be communicated to others and under what circumstances. (Westin 1970)

privacy as control

separation of identities, data protection principles

# privacy research paradigms



right of the individual to decide what information about himself should be communicated to others and under what circumstances. (Westin 1970)

privacy as control

separation of identities, data protection principles

anonymous credentials

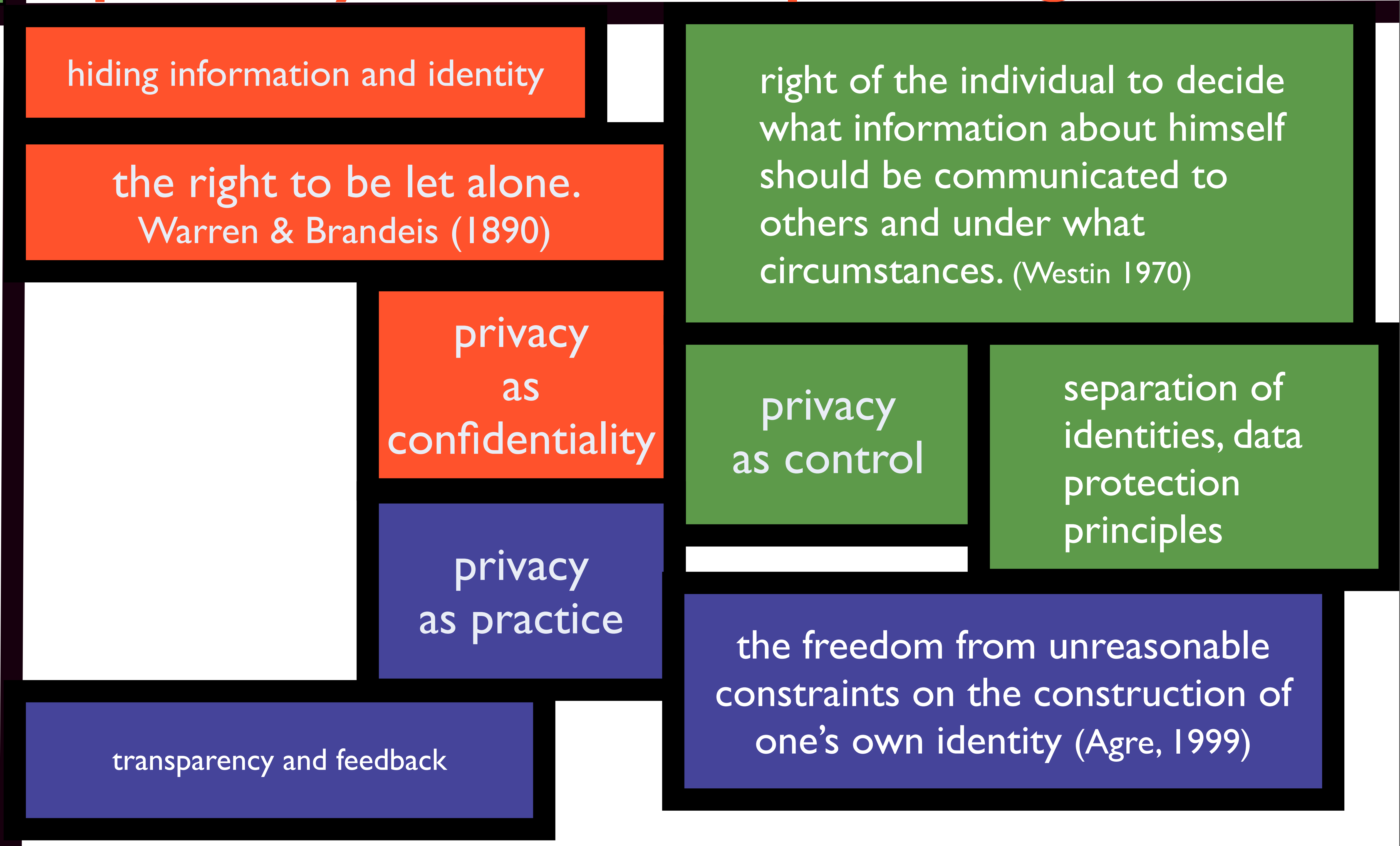
Privacy Settings

IDMS

Privacy Policy Languages

Purpose Based Access Control

# privacy research paradigms



hiding information and identity

the right to be let alone.
Warren & Brandeis (1890)

privacy
as
confidentiality

right of the individual to decide what information about himself should be communicated to others and under what circumstances. (Westin 1970)

privacy
as control

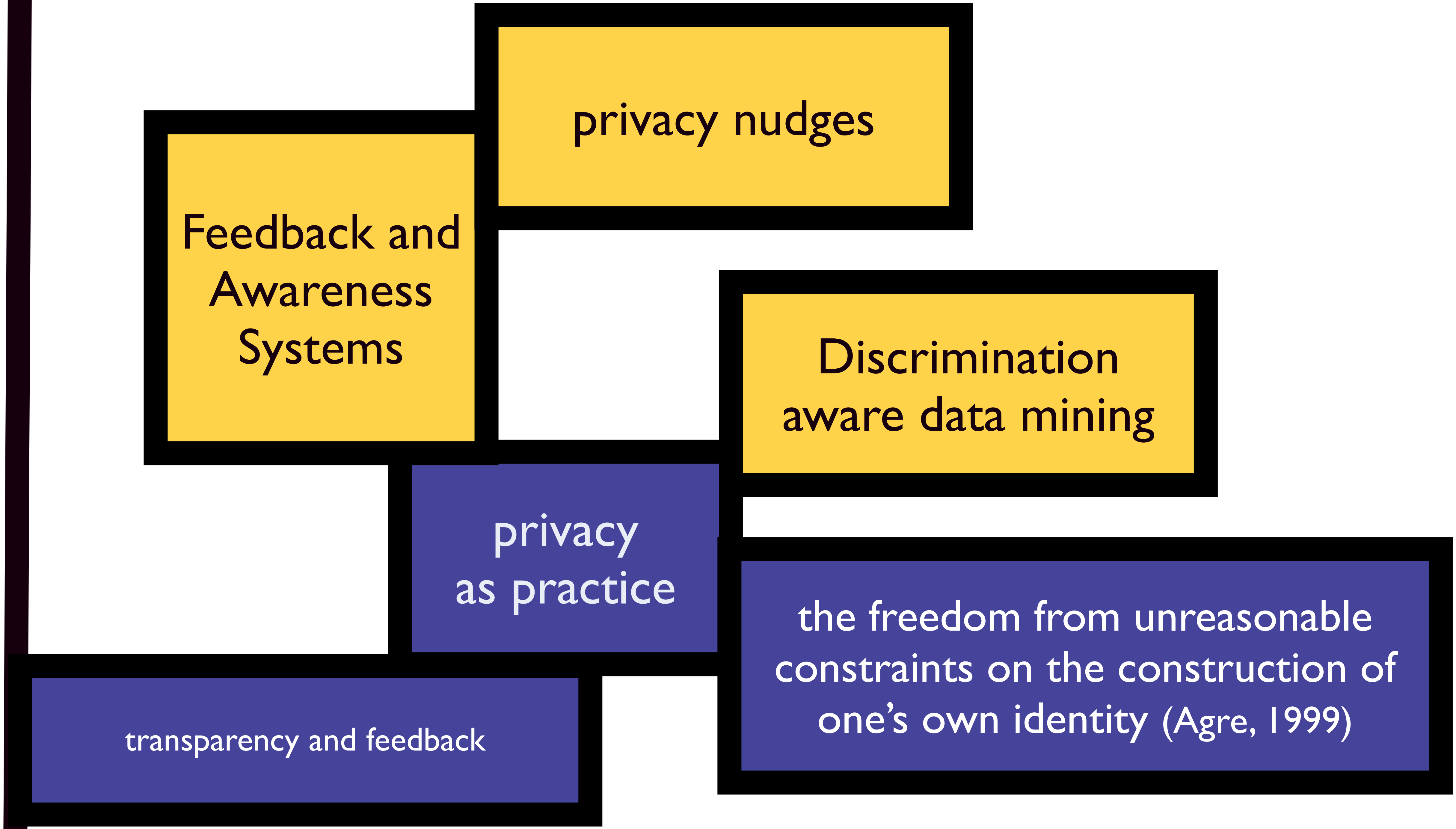
separation of identities, data protection principles

privacy
as practice

transparency and feedback

the freedom from unreasonable constraints on the construction of one’s own identity (Agre, 1999)

# privacy research paradigms



privacy nudges

Feedback and Awareness Systems

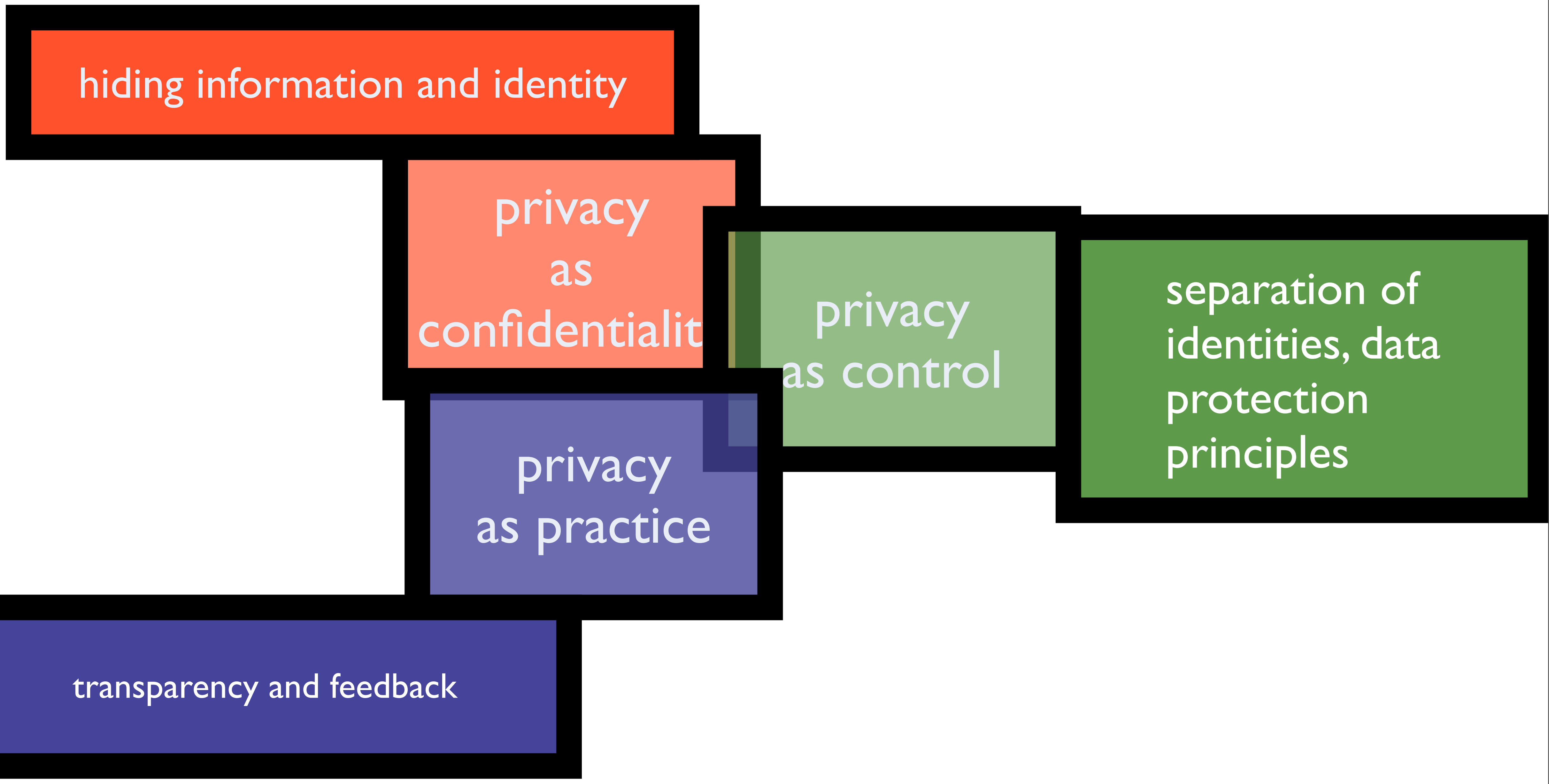
Discrimination aware data mining

privacy as practice

the freedom from unreasonable constraints on the construction of one’s own identity (Agre, 1999)

transparency and feedback

# privacy research paradigms



hiding information and identity

privacy as confidentialit

privacy as control

separation of identities, data protection principles

privacy as practice

transparency and feedback

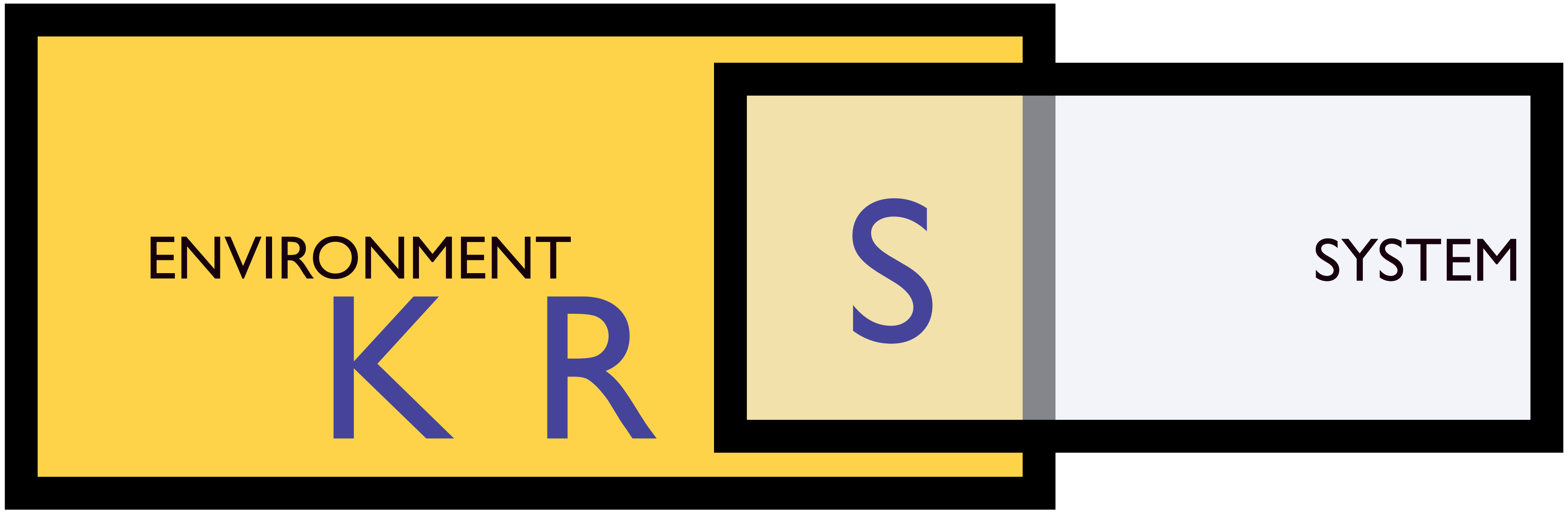
# multilateral privacy requirements engineering

- reconcile:
    - privacy notions (legal & surveillance studies)
    - privacy solutions (computer science)
    - in a social context
    - multilaterally
    - during requirements engineering

# privacy and the Zave & Jackson Model

- Zave and Jackson model is limited:
    - does not account for requirements that are not absolutely satisfiable
    - does not facilitate subjective articulations of domain assumptions, requirements or specifications
    - does not express stakeholder attitudes and emotions (only beliefs, desires and intentions)

# Zave and Jackson Model of RE

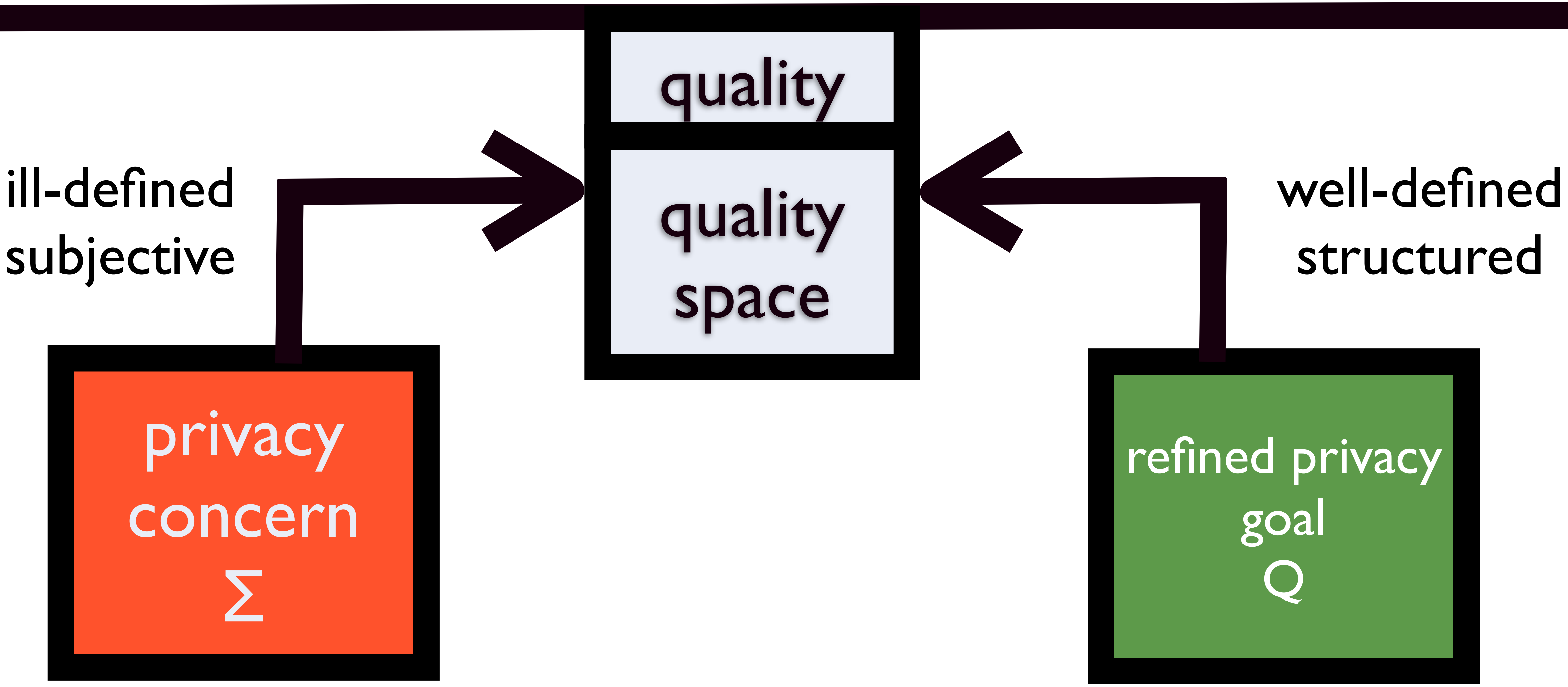


- K: *domain assumptions* describe the behavior of the environment as it is
- R: *requirements* are statements about the desired conditions in an environment
- S: *specification* is a restricted form of requirement providing enough information for the engineer to implement the system

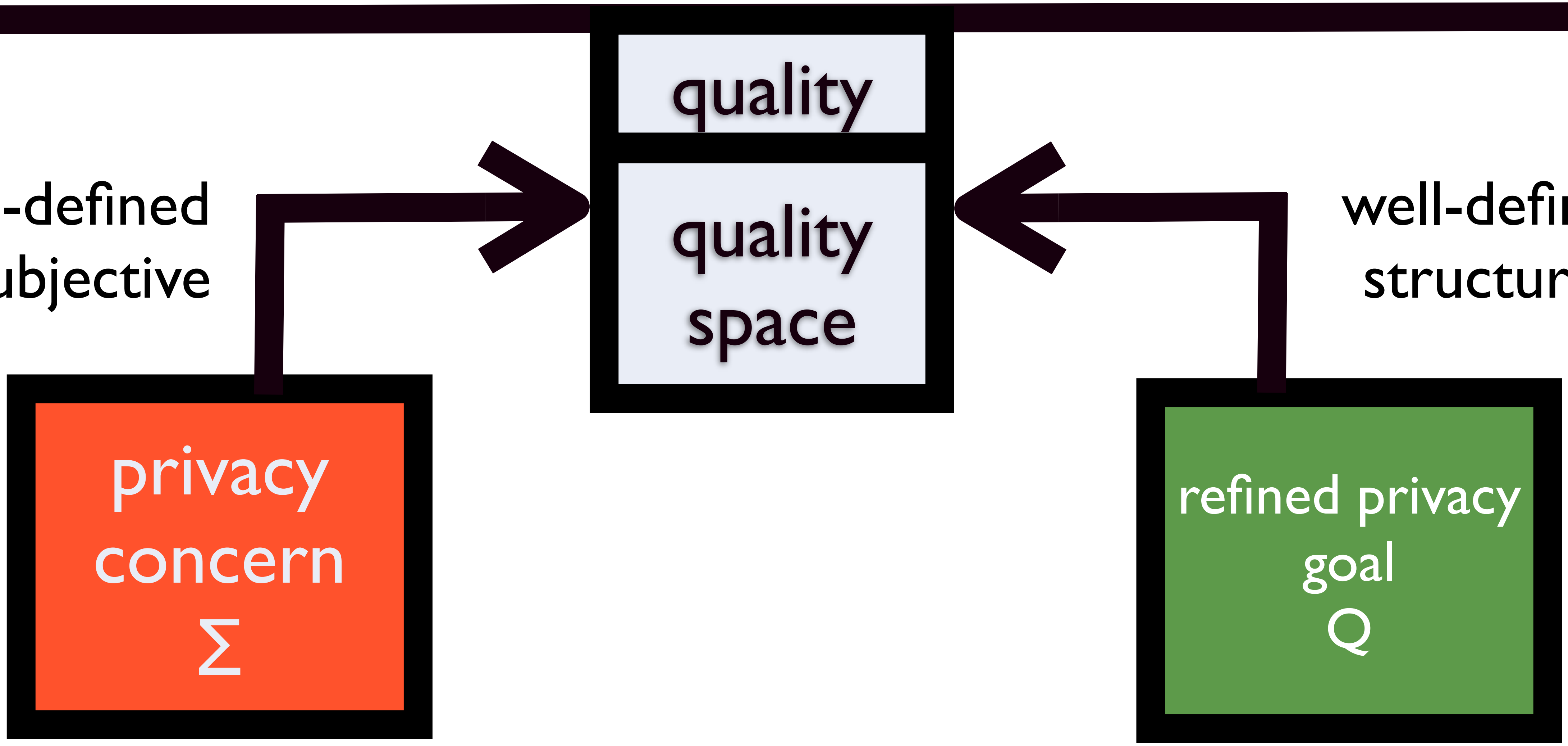
# requirements

- *functional requirements* state the desired behavior of the environment
- *non-functional requirements* either constrain the behavior of the environment or define certain desired qualities of the environment

# privacy requirements ontology



# privacy requirements ontology



quality

quality space

ill-defined
subjective

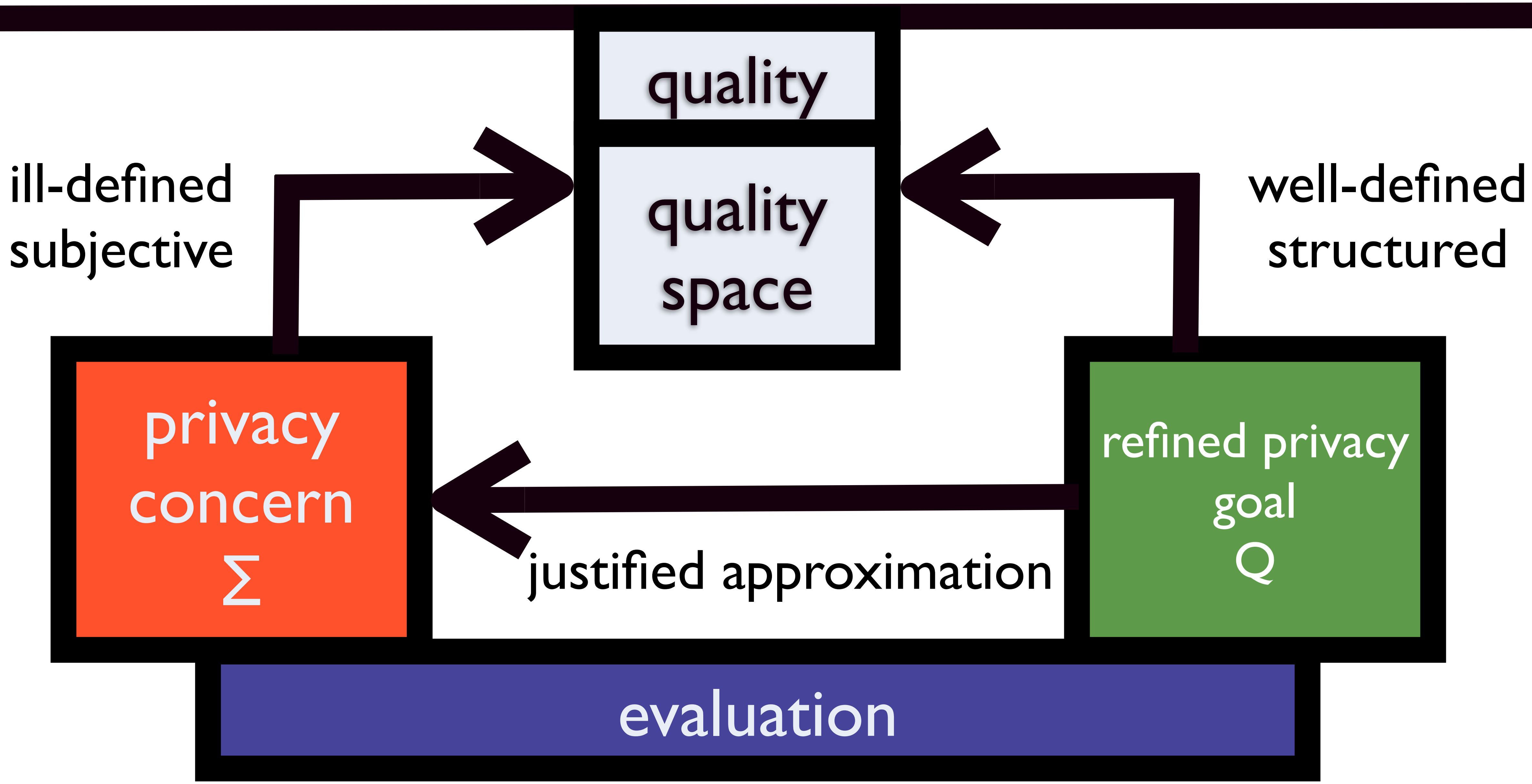
privacy concern
Σ

well-defined
structured

refined privacy goal
Q

color: red

munsell color notation:
10 red
hue 7
chroma 8


quality
quality space
ill-defined
subjective
well-defined
structured
privacy concern
Σ
refined privacy goal
Q
justified approximation
evaluation

# MULTILATERAL PRIVACY REQUIREMENTS ANALYSIS

# privacy requirements ontology

stakeholder arbitration

# privacy requirements ontology

stakeholder arbitration

surveillance information

# privacy requirements ontology

stakeholder arbitration

surveillance information

functionality

# privacy requirements ontology

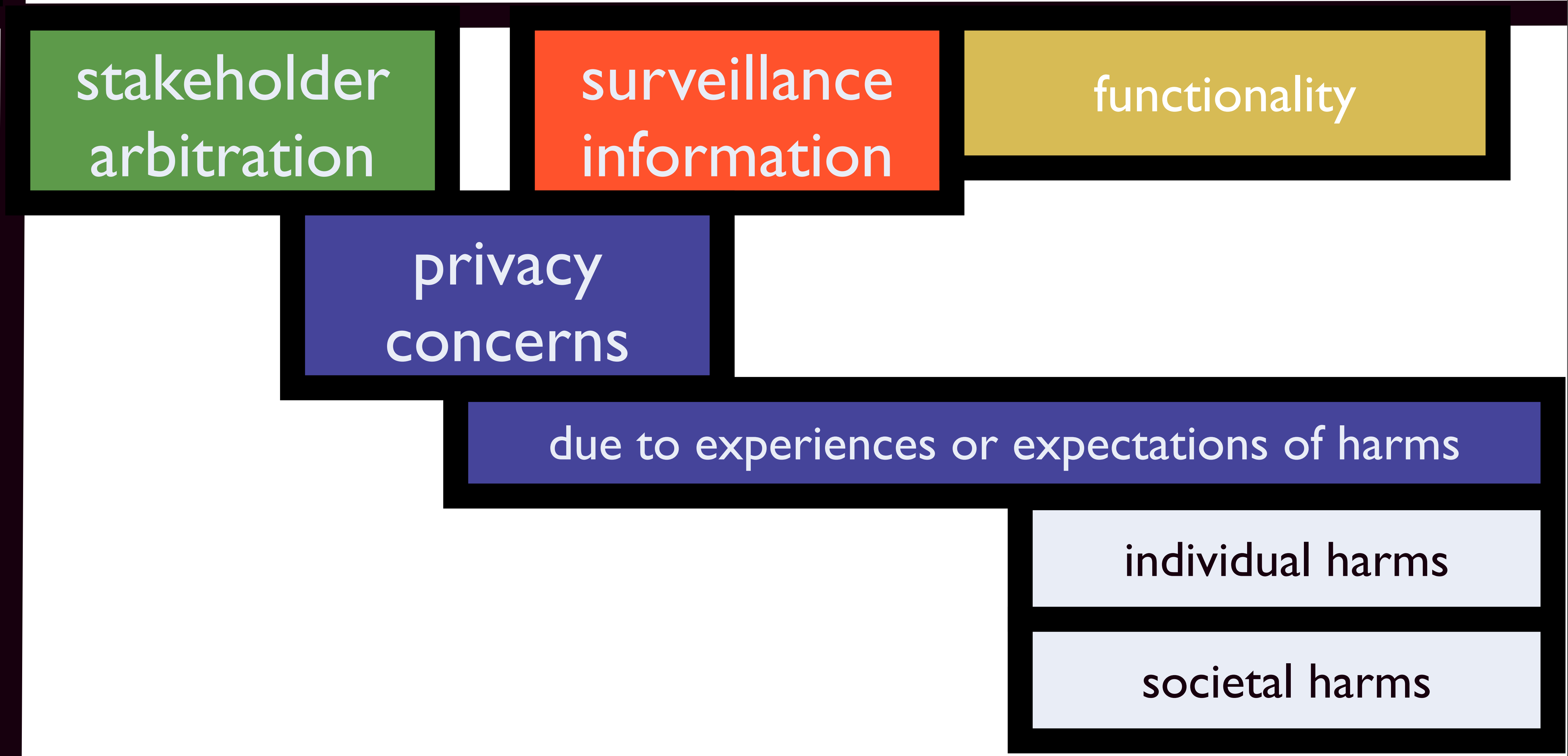
stakeholder arbitration

surveillance information

functionality

privacy concerns

# privacy requirements ontology



stakeholder arbitration

surveillance information

functionality

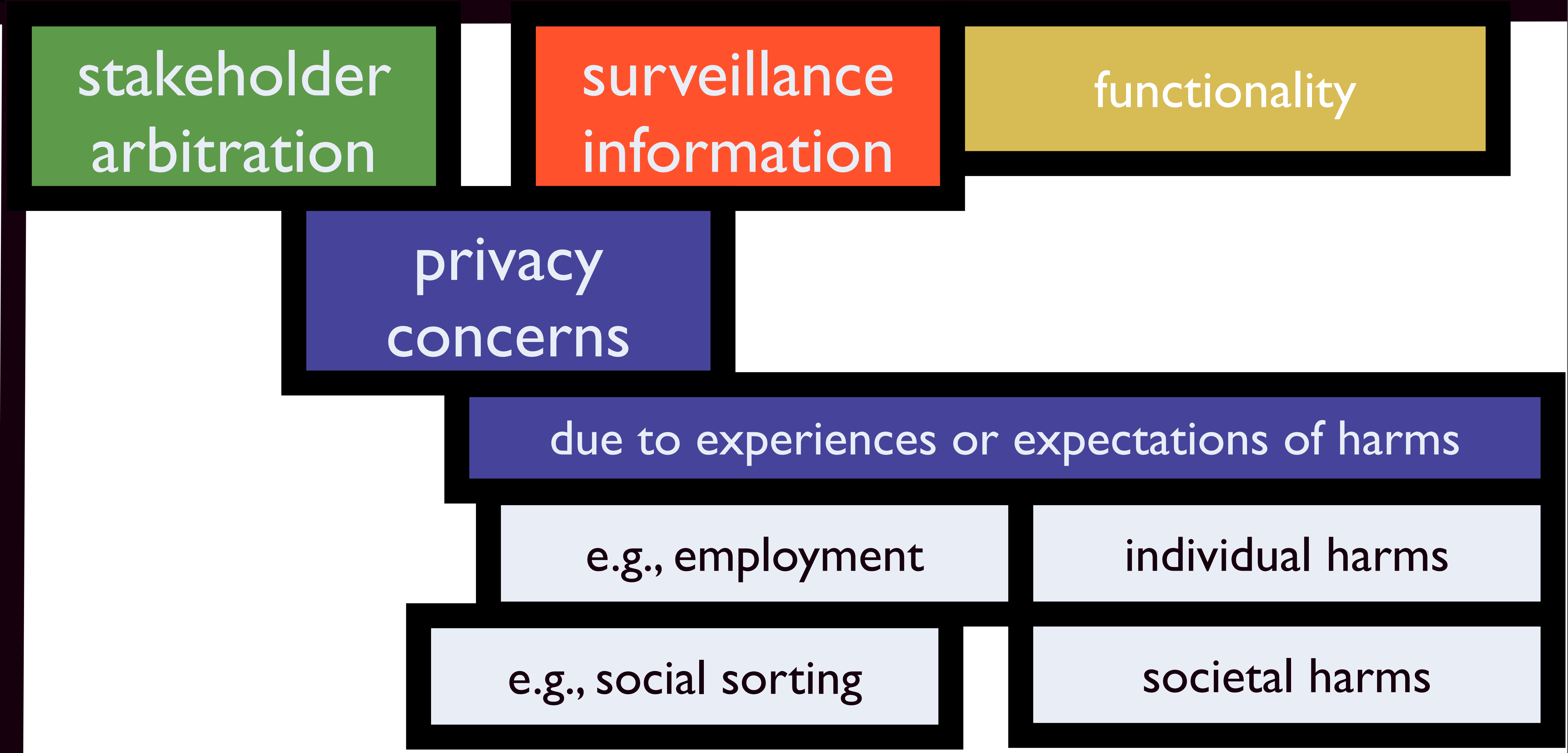
privacy concerns

due to experiences or expectations of harms

individual harms

societal harms

# privacy requirements ontology



stakeholder arbitration

surveillance information

functionality

privacy concerns

due to experiences or expectations of harms

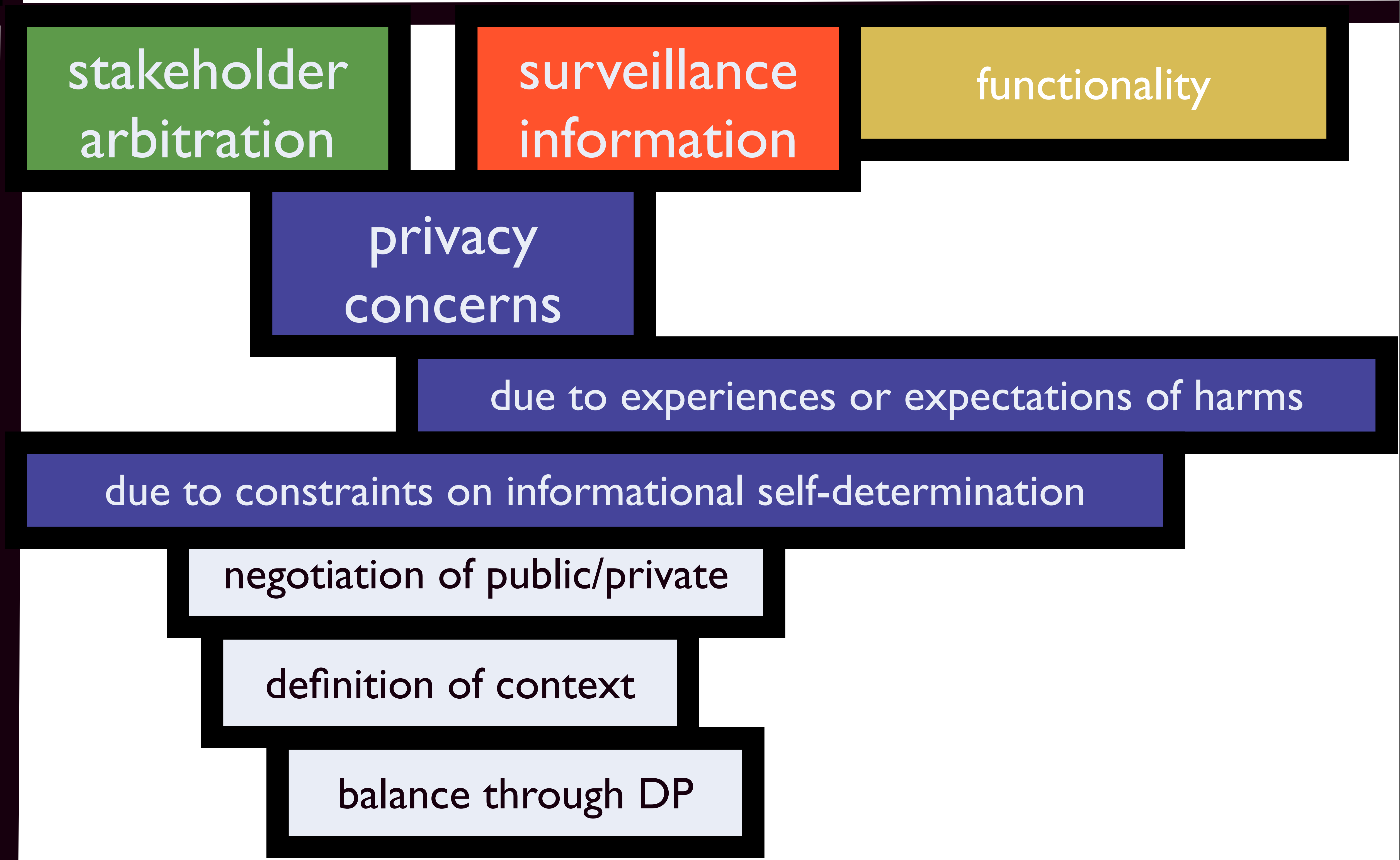
e.g., employment

individual harms

e.g., social sorting

societal harms

# privacy requirements ontology



stakeholder arbitration

surveillance information

functionality

privacy concerns

due to experiences or expectations of harms

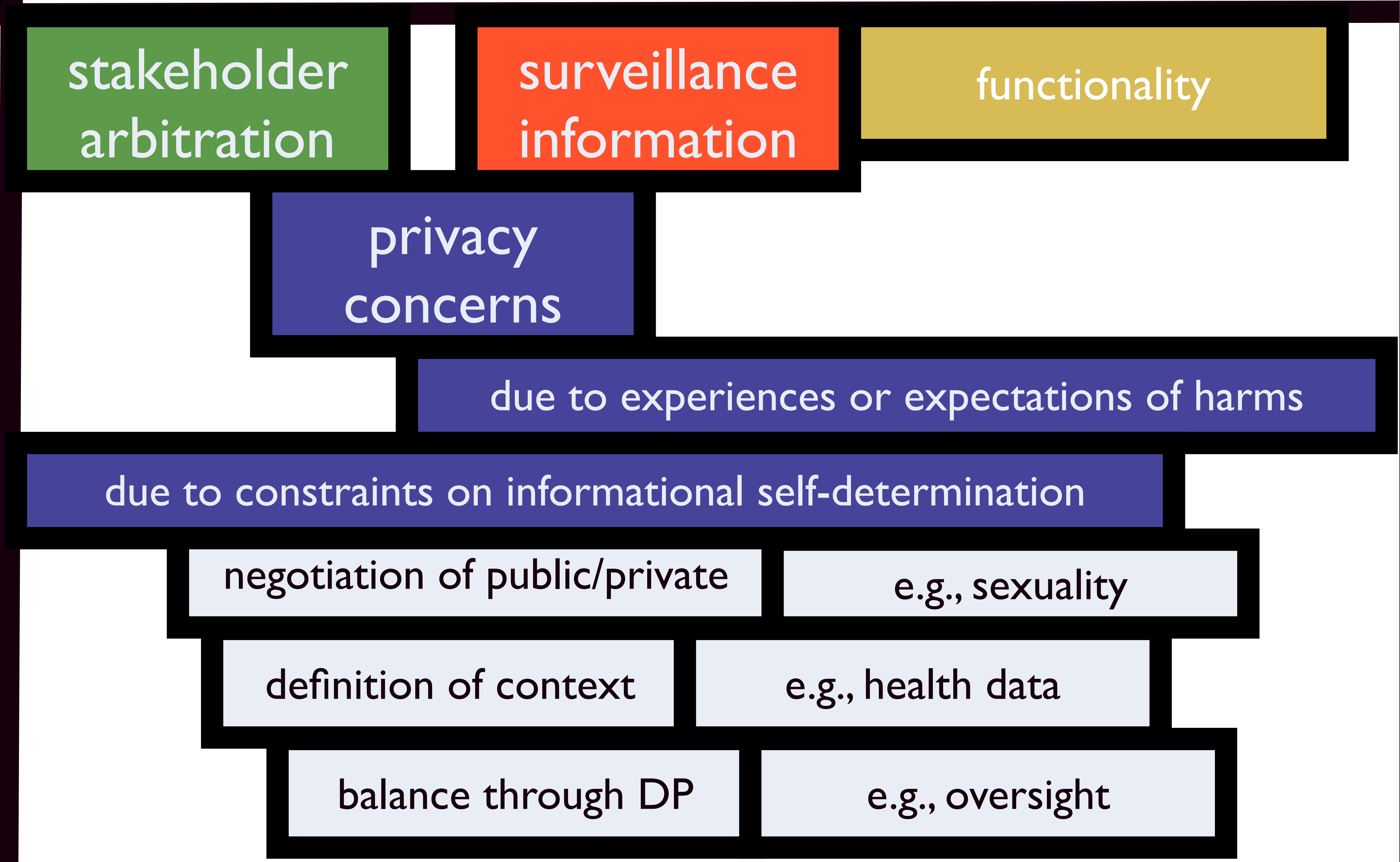
due to constraints on informational self-determination

negotiation of public/private

definition of context

balance through DP

# privacy requirements ontology



stakeholder arbitration

surveillance information

functionality

privacy concerns

due to experiences or expectations of harms

due to constraints on informational self-determination

negotiation of public/private

e.g., sexuality

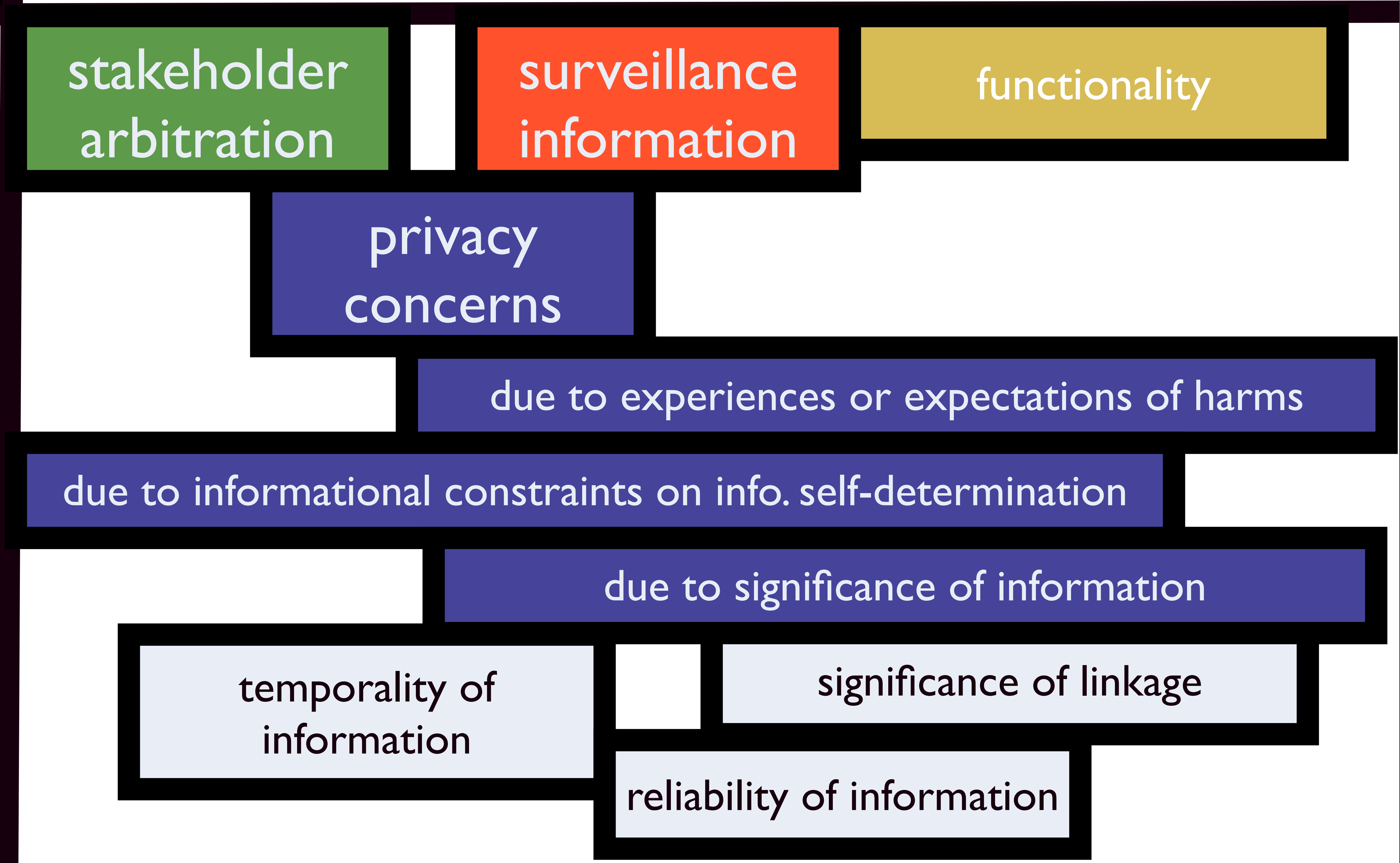
definition of context

e.g., health data

balance through DP

e.g., oversight

# privacy requirements ontology



stakeholder arbitration

surveillance information

functionality

privacy concerns

due to experiences or expectations of harms

due to informational constraints on info. self-determination

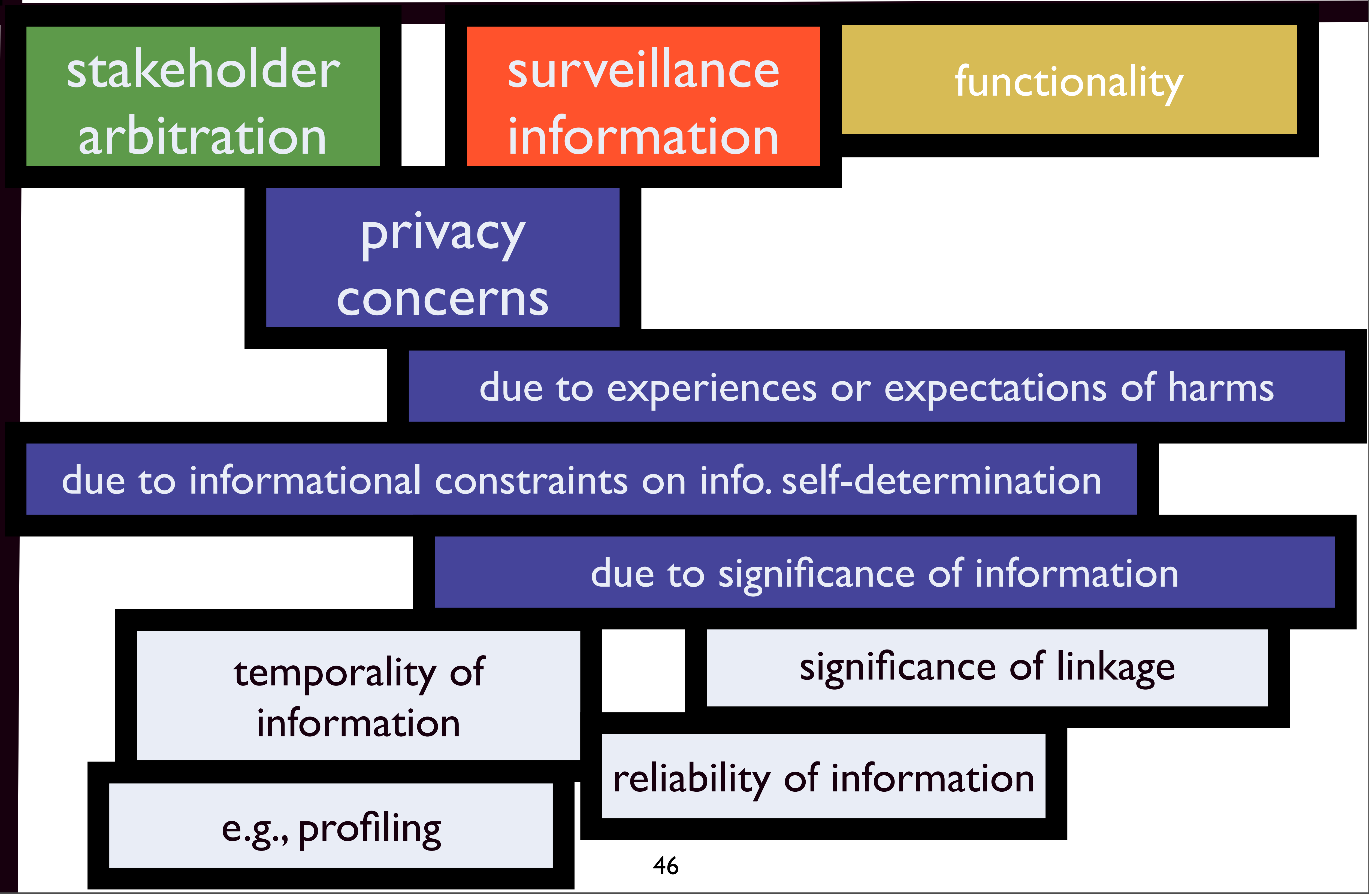
due to significance of information

temporality of information

significance of linkage

reliability of information

# privacy requirements ontology



stakeholder arbitration

surveillance information

functionality

privacy concerns

due to experiences or expectations of harms

due to informational constraints on info. self-determination

due to significance of information

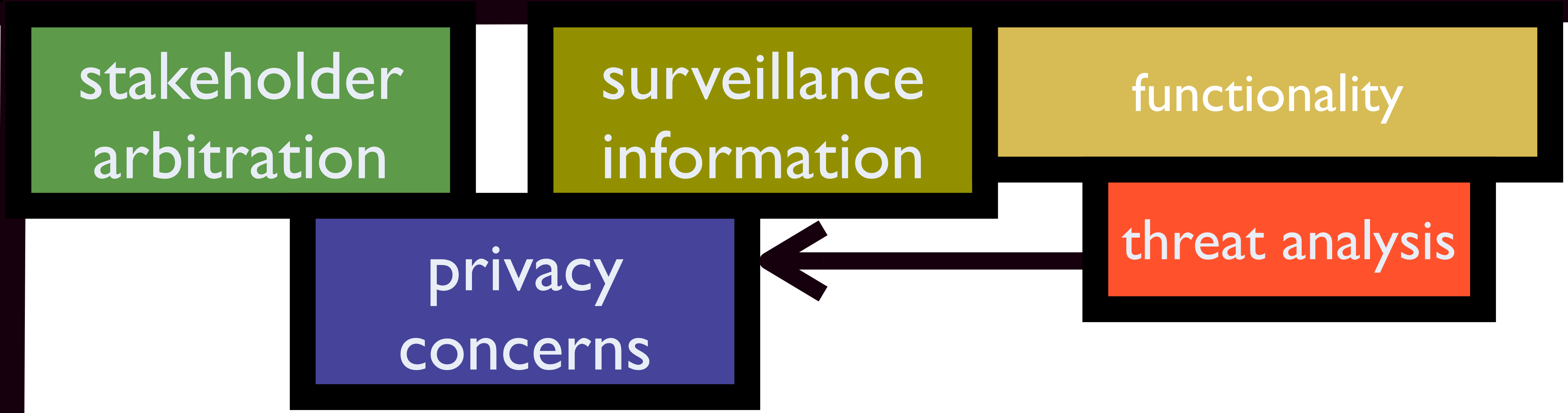
temporality of information

significance of linkage

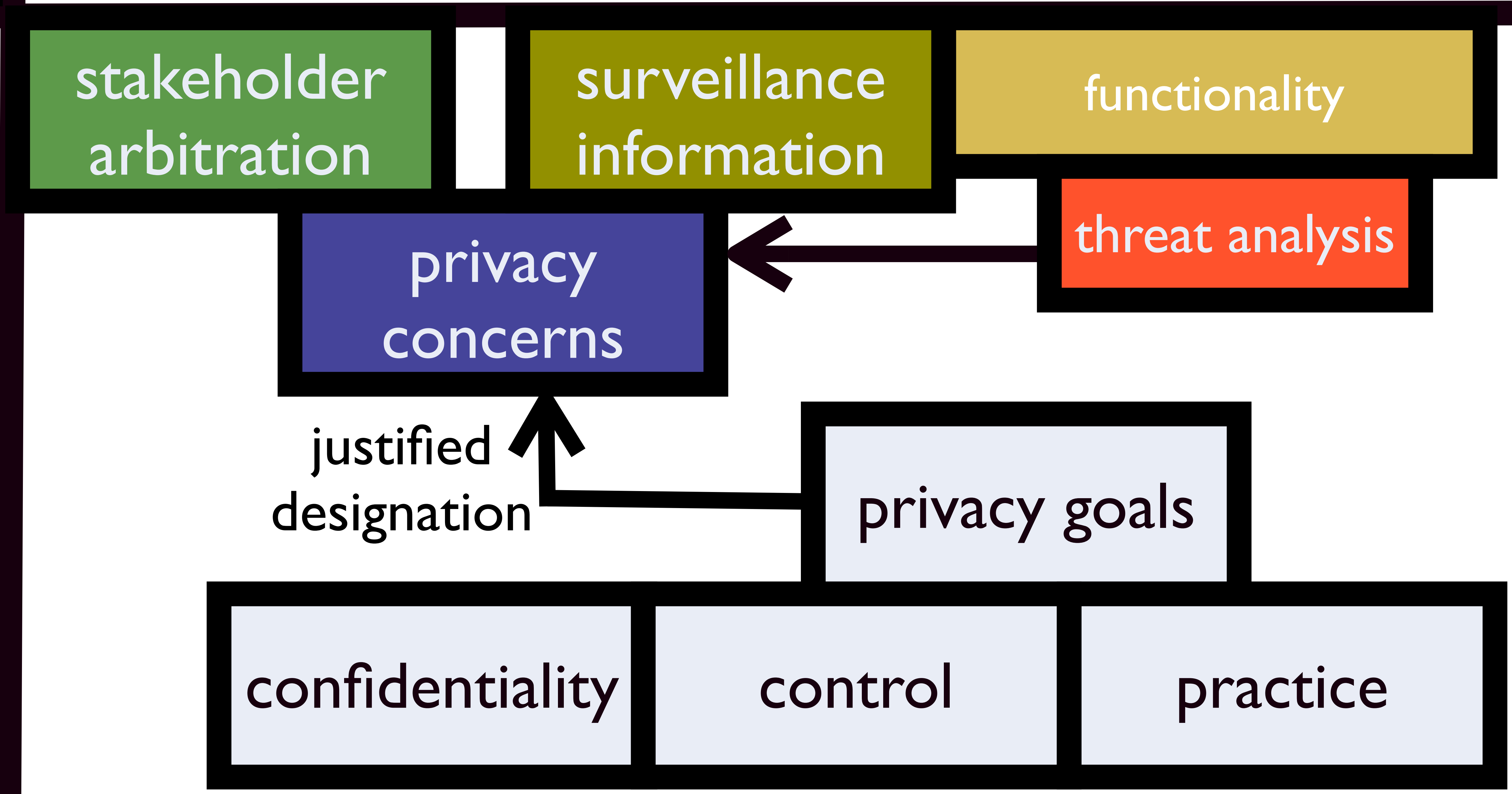
reliability of information

e.g., profiling

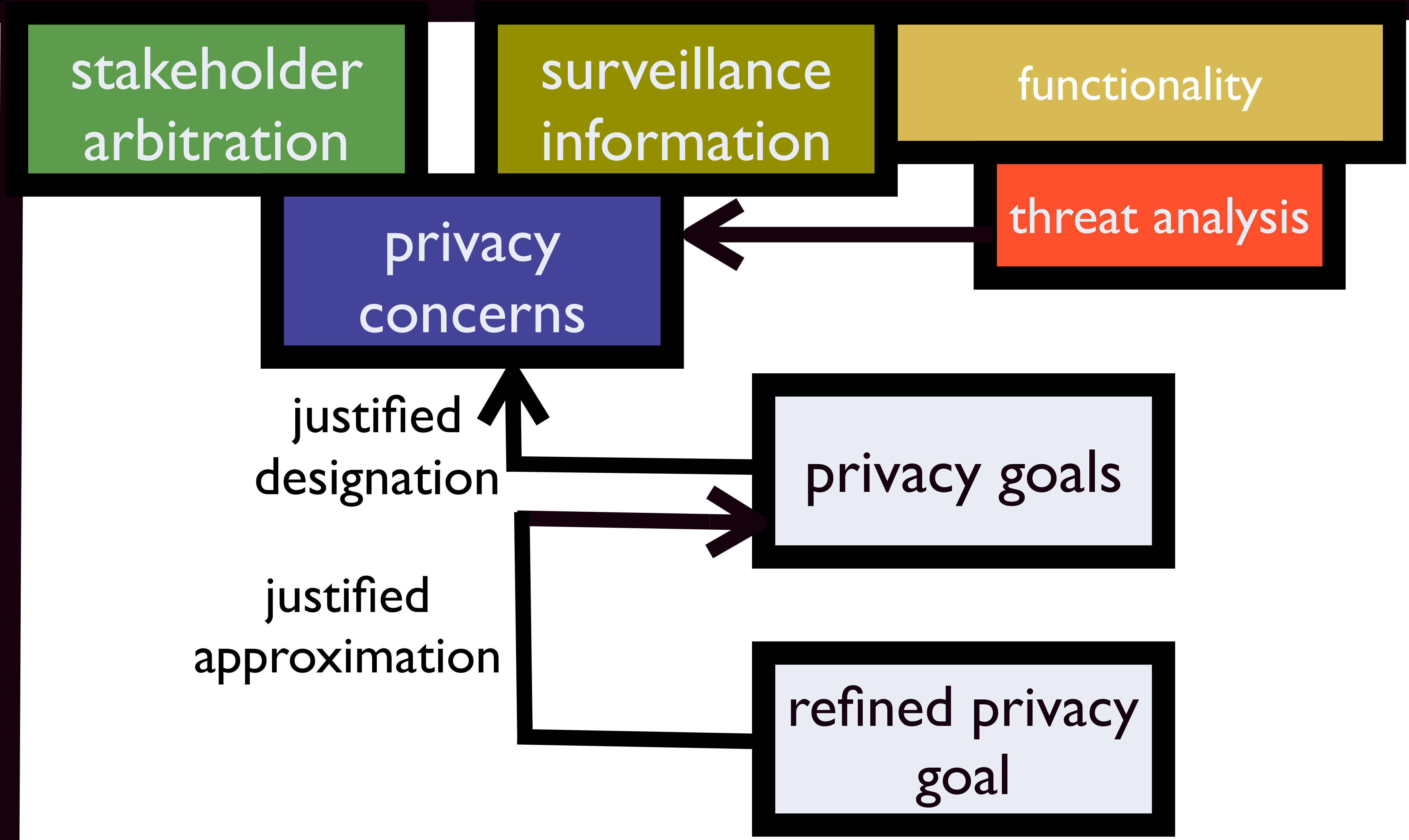
# privacy requirements ontology



# privacy requirements ontology



# privacy requirements ontology



stakeholder arbitration

surveillance information

functionality

threat analysis

privacy concerns

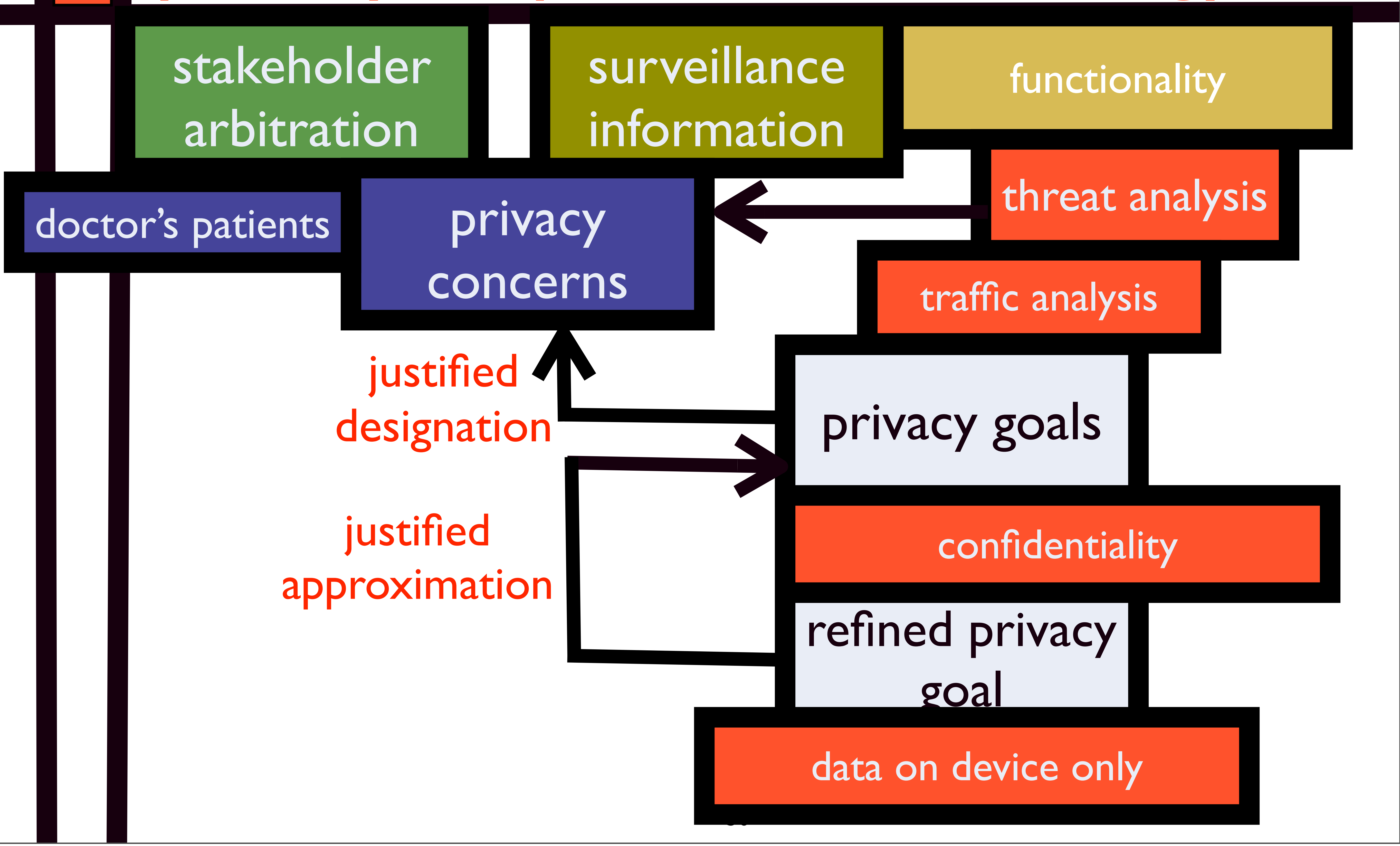
justified designation

privacy goals

justified approximation

refined privacy goal

# privacy requirements ontology



stakeholder arbitration

surveillance information

functionality

doctor's patients

privacy concerns

threat analysis

traffic analysis

justified designation

privacy goals

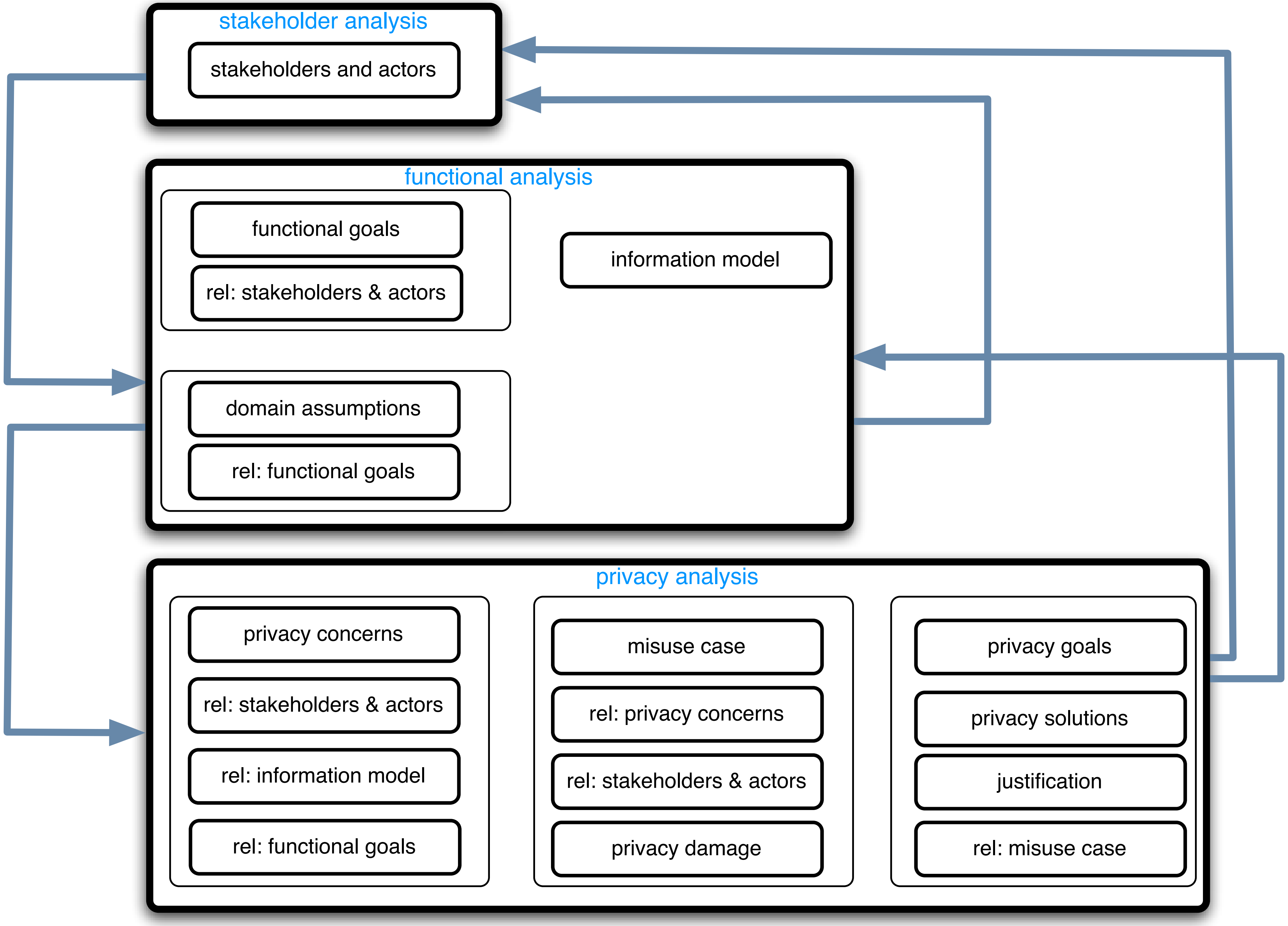
justified approximation

confidentiality

refined privacy goal

data on device only

# template overview



# Thank you!

- sguerses@esat.kuleuven.be

# privacy engineering (Guarda and Zannone 2008)

- a systematic effort to embed privacy relevant legal primitives into technical and governance design
  - specify (organizational) privacy promises
  - guarantee their enforcement
  - comply with data protection legislation

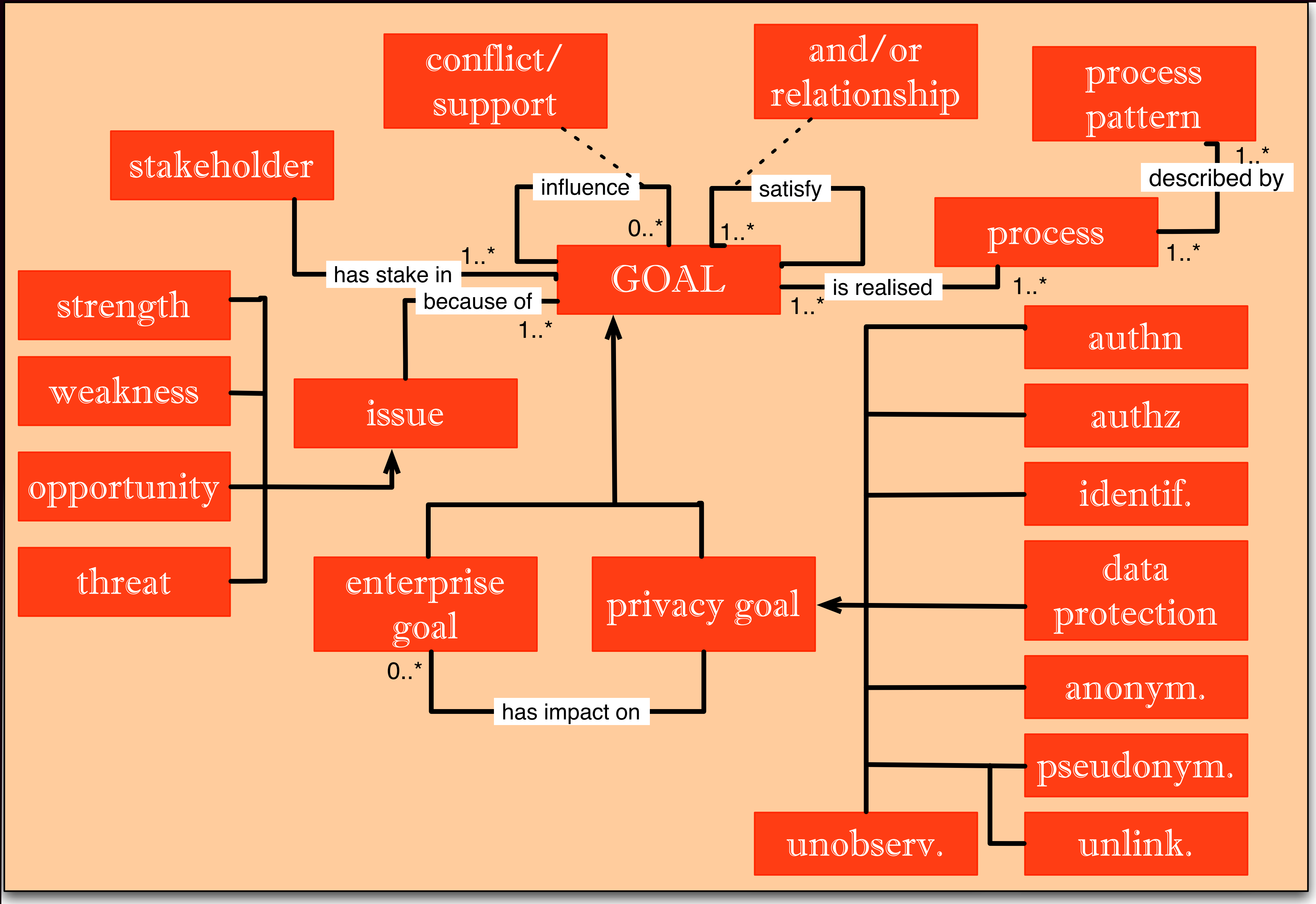
# privacy engineering methodology (Guarda and Zannone 2008)

- capture the structure of organizations and their environments
- capture the purposes for which personal data are collected
    - link permissions to them
- identify the kind of data involved in processing
- capture the obligations and link to permission

# multilateral privacy requirements engineering

- reconcile:
  - privacy notions (legal & surveillance studies)
  - privacy solutions (policy languages and ACL)
  - in a social context (organizational perspective)
  - multilaterally (organization and law)
  - during requirements engineering

# PriS Method
# (Kalloniatis et al. 2008)

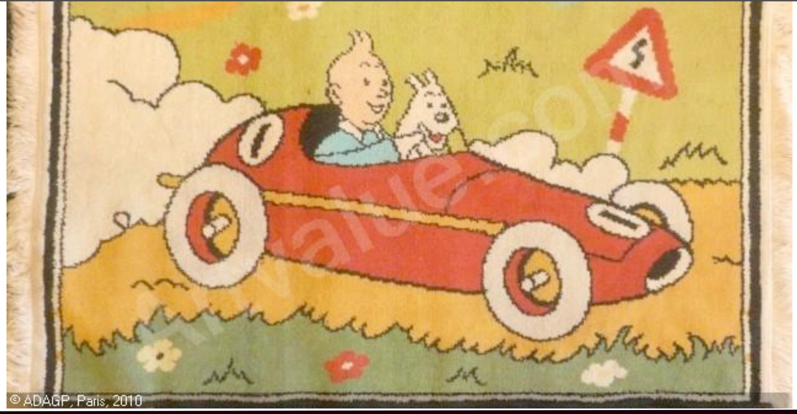


# multilateral privacy requirements engineering

- reconcile:
  - privacy notions (legal & surveillance studies)
  - privacy solutions (security properties)
  - in a social context (engineer, enterprise and law)
  - multilaterally
  - during requirements engineering

# Presentations

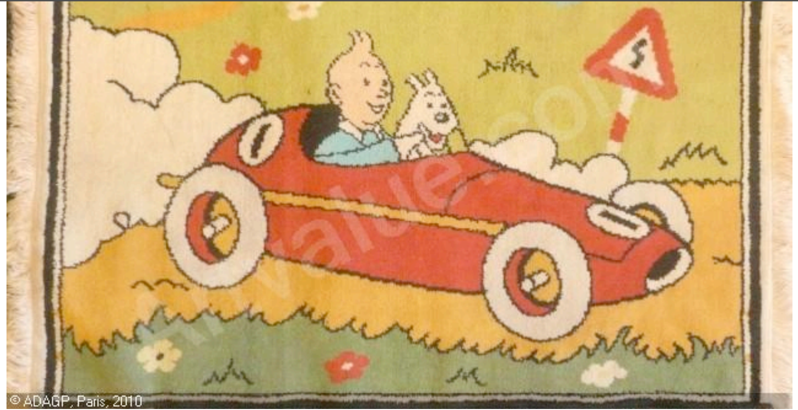
# TINTIN



© ADAGP, Paris, 2010

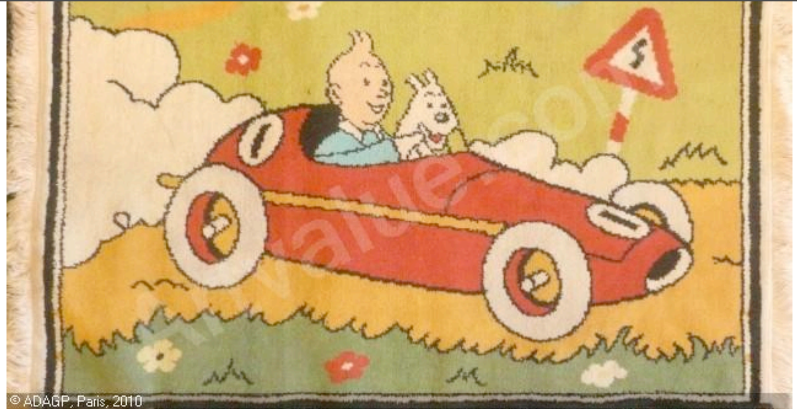
- Company: Privacy Aware Automative Navigation Service
  - target: 70 million privacy aware users world wide
  - target profit: 1.000 million in 5 years
- Functionality:
  - Basic:
    - locate user on road
    - use maps to provide user with routing instructions
    - expected profit 600 million

# TINTIN


© ADAGP, Paris, 2010

- Advanced Functionality:
  - dead reckoning: determine current position based on a previous position
    - sensors on tires and steering wheel
  - additional service: attention analysis
    - end users: profit 50 million
    - insurance company reports: profit 100 million

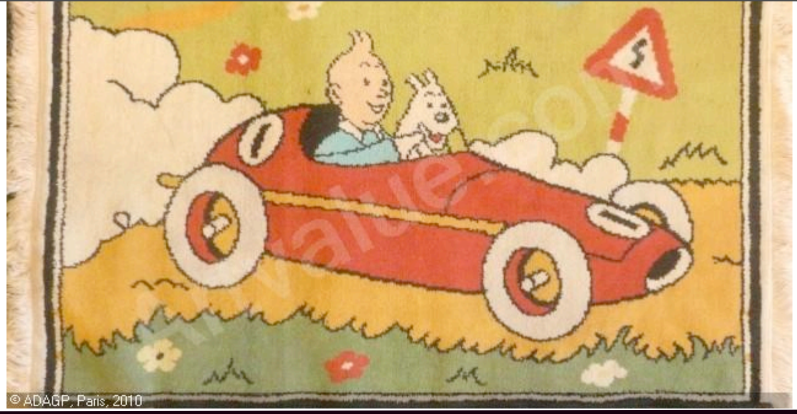
# TINTIN



© ADAGP, Paris, 2010

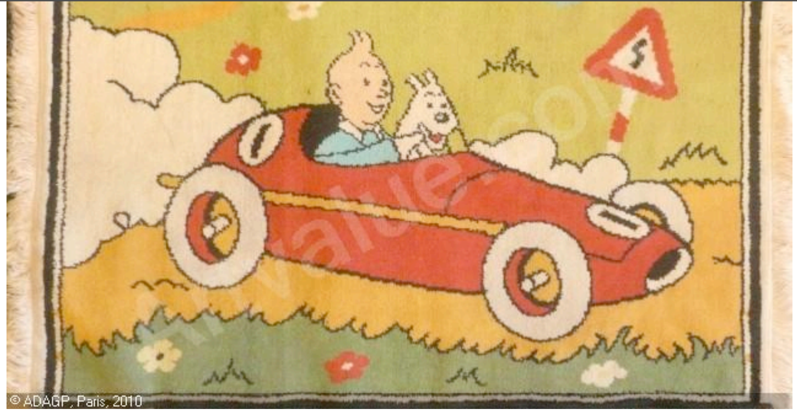
- Advanced Functionality:
  - live traffic and route updates:
    - re-routing based on traffic congestion
      - end users: profit 200 million
    - additional service: recommender system
      - where people on your route went today!
        - end users: profit 10 million
        - advertisers: profit 400 million
        - law enforcement and city planning: profit 20 million

# TINTIN



- Further sales:
  - proprietary maps:
    - end users: profit 300 million
    - advertisement: 300 million
  - user data:
    - advertisers: profit 400 million

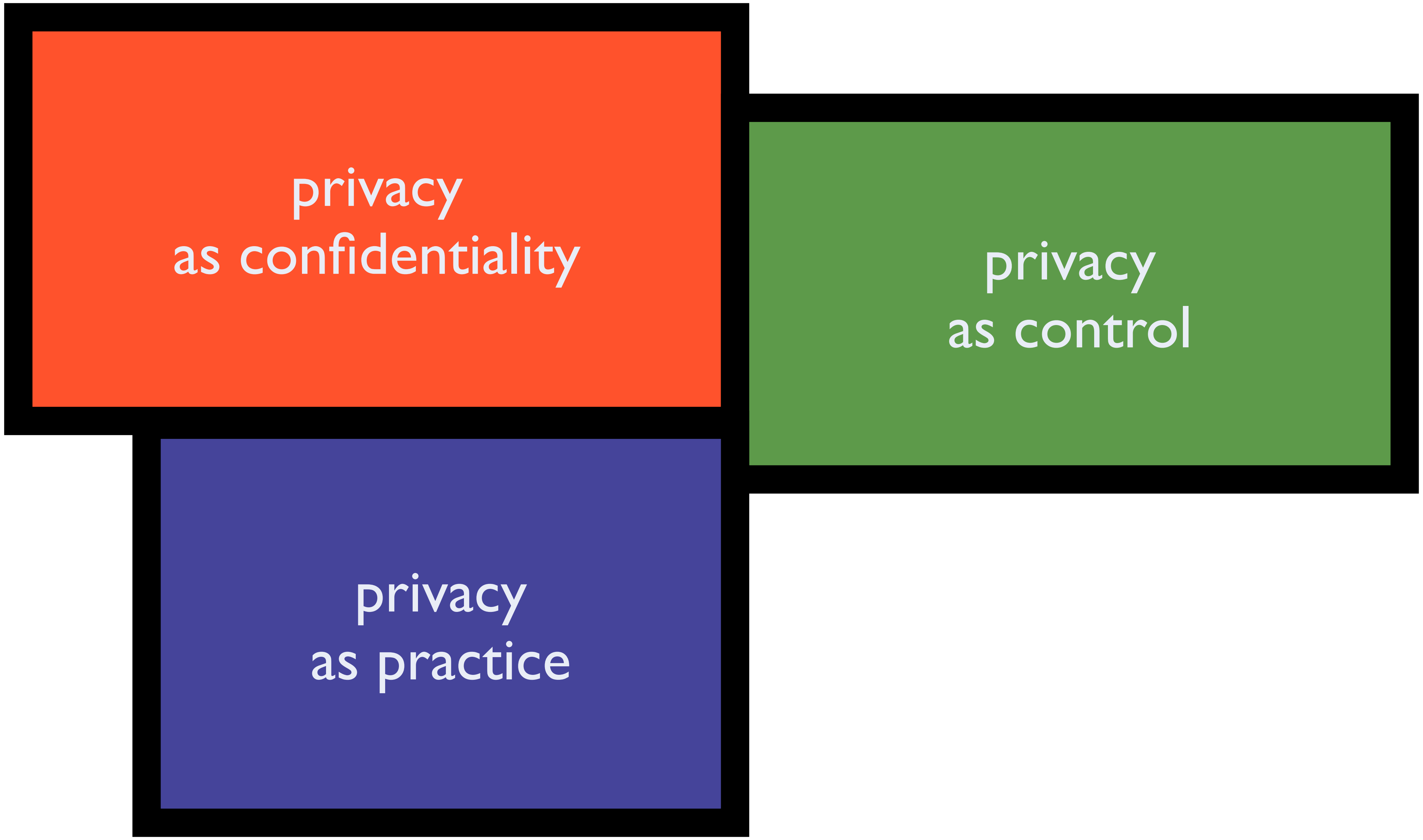
# TINTIN



© ADAGP, Paris, 2010

- Privacy Breach:
  - 30 % of end users leave
  - advertisers do not want to be associated
  - losses:
    - advertisement and additional sales: 500 million
    - 30 % of user income
    - liability costs: 200 million

# 3 groups



privacy as confidentiality

privacy as control

privacy as practice

- slides and exercise sheet:
    - http://bit.ly/kYUqyu

# the groups

- at least one legal person
  - privacy and data protection requirements
- at least one crypto/security person
  - use of privacy technologies
- nice: at least one data mining person
  - additional func + feedback and awareness