TECHNISCHE UNIVERSITÄT DRESDEN

Faculty of Computer Science, Institute of Architecture of Systems, Chair of Data Security and Data Protection

Implementability of the Identity Management Part in Pfitzmann/Hansen's Terminology for a Complex Digital World

Manuela Berg, Katrin Borcea-Pfitzmann

Helsingborg, 02.08.2010

Goal

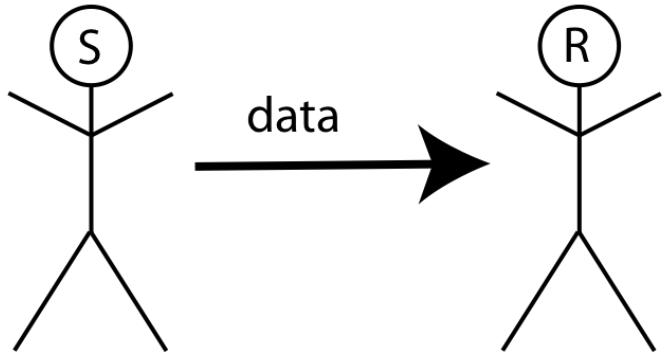
- computer-mediated interaction between individuals
- using a description of a complex digital world
- identifying objects for acting entities needed for applications
- definition of privacy

01 The Problem Set

The Complex Digital World

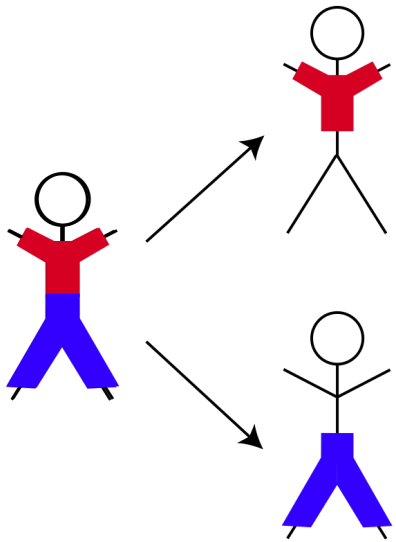
Traditional Sender-Receiver Model

- one sender
- one receiver
- flow of data
- fixed time



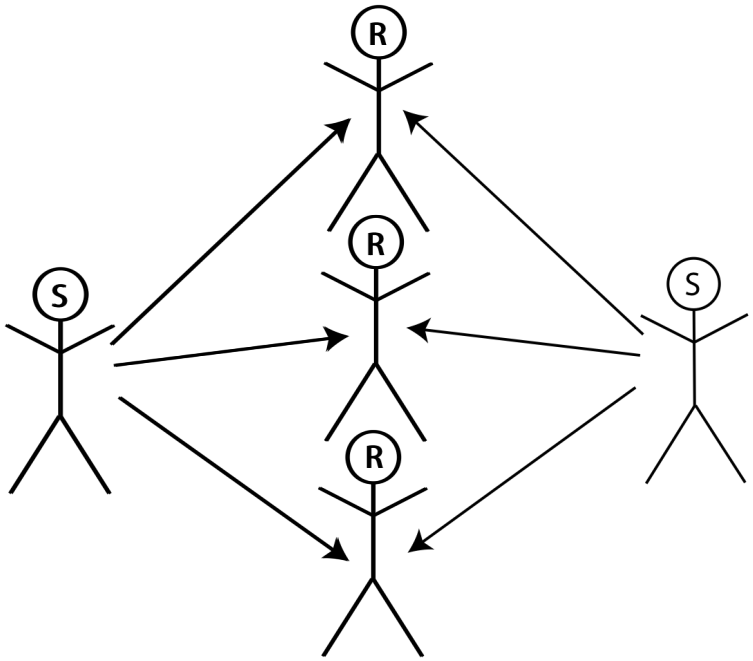
Why not only the Sender-Receiver Model?

- Who are the senders and the receivers?
  1. focus on individuals
  2. individuals and their representations



Why not only the Sender-Receiver Model?

- Who are the senders and the receivers?
- How many senders and receivers?



Why not only the Sender-Receiver Model?

- Who are the senders and the receivers?
- How many senders and receivers?
- Which duration of time?

Why not only the Sender-Receiver Model?

- Who are the senders and the receivers?
- How many senders and receivers?
- Which duration of time?
- Which kind of relationship between senders and receivers?

  not necessarily flow of data ⇒ roles not fixed
  different quality and quantity

Why not only the Sender-Receiver Model?

- Who are the senders and the receivers?
- How many senders and receivers?
- Which duration of time?
- Which kind of relationship between senders and receivers?
  - not necessarily flow of data ⇒ roles not fixed
  - different quality and quantity
- What about different situations?

Comparison

Sender-Receiver Model

- Sender and receiver
- Fixed time
- Data flow as relationship
- One-to-one relationships
- No interest in situations

Complex Digital World

- Not necessarily fixed senders and receivers
- Dynamic time possible
- Different qualities and quantities of relationships
- Many-to-many relationships
- Situations might make the difference

01 The Problem Set

[Pfitzmann/Hansen]

The Terminology

- [Pfitzmann/Hansen 2000]:
  - Anonymity, unobservability, and pseudonymity - a proposal for terminology
  - 1st publication
- [Pfitzmann/Hansen 2010]:
  - A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management
  - continuously evolving

Definition of subject

A *subject* is a possibly acting entity such as, e.g., a human being (i.e., a natural person), a legal person, or a computer.

Definitions of

- Anonymity
- Identity

→ based on subject (and individual person)

02 Problems Arising from the Terminology

Anonymity

Definition of anonymity [Pfitzmann/Hansen]

Anonymity of a subject from an attacker's perspective means that the attacker cannot sufficiently identify the subject within a set of subjects, the *anonymity set.*

1. **Anonymity of an individual in a set of individuals**
   - as in the definition
2. **Anonymity of a digital representation in a set of digital representations**
   - contained in the definition
   - not distinguishable from 1.
3. **Anonymity in the sense of unlinkability between an individual and his digital representations**

   anonymization in the German law for data protection §3 (6) [BDSG] : act of making personal data anonymous as the transformation of personal data in a way to make it difficult or impossible to link personal data to the individual.

02 Problems Arising from the Terminology

Identity

[Pfitzmann/Hansen 2010]: An *identity* is any subset of attribute values of an individual person which sufficiently identifies this individual person within any set of persons.

Necessary design decision

What is contained in the identity?

Are perceptions contained in the identity?

- -perception of an individual about others
- -perception of others about the individual

When are identities equal (or sufficiently equal)?

Who establishes an identity?

Identity as socio-centric concept

- Means that each identity is omnipresent
- Unique individual characterization

Identity as ego-centric concept

- More appropriate for interaction between individuals
- Perceptions included as attributes

02 Problems Arising from the Terminology

Privacy

Definition of Privacy [Westin 67]:

Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

- claim
- individuals, groups, or institutions
- information
- others
- situations

03 Separating the Digital World from the Physical World

Data and Information [Dict]:

Data is a group of symbols or continuous functions which become information due to known or supposed agreements. Data is supposed to be processed and are the result of processing. Information is the knowledge about states and events in the real world.

Entities, Oge() and Ego()

- Digital entities as pure data (in the digital world)
- Physical entities as collection of information (in the physical world)
- Oge(): information → data
- Ego(): data → information
- Perceptions as part of the entities

04 Definition of Privacy

Definition of Privacy

Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

Definition of Privacy

Privacy is the **claim** of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

- claim → result of negotiating and enforcing

Definition of Privacy

Privacy is the **claim** of **individuals, groups, or institutions** to determine for themselves when, how, and to what extent information about them is communicated to others.

- claim → result of negotiating and enforcing
- individuals, groups, or institutions → physical entity

Definition of Privacy

Privacy is the **claim** of **individuals, groups, or institutions** to determine for themselves when, how, and to what extent **information** about them is communicated to others.

- claim → result of negotiating and enforcing
- individuals, groups, or institutions → physical entity
- information → data

Definition of Privacy

Privacy is the **claim** of **individuals, groups, or institutions** to determine for themselves when, how, and to what extent **information** about them is communicated to **others**.

- claim → result of negotiating and enforcing
- individuals, groups, or institutions → physical entity
- information → data
- others → whom

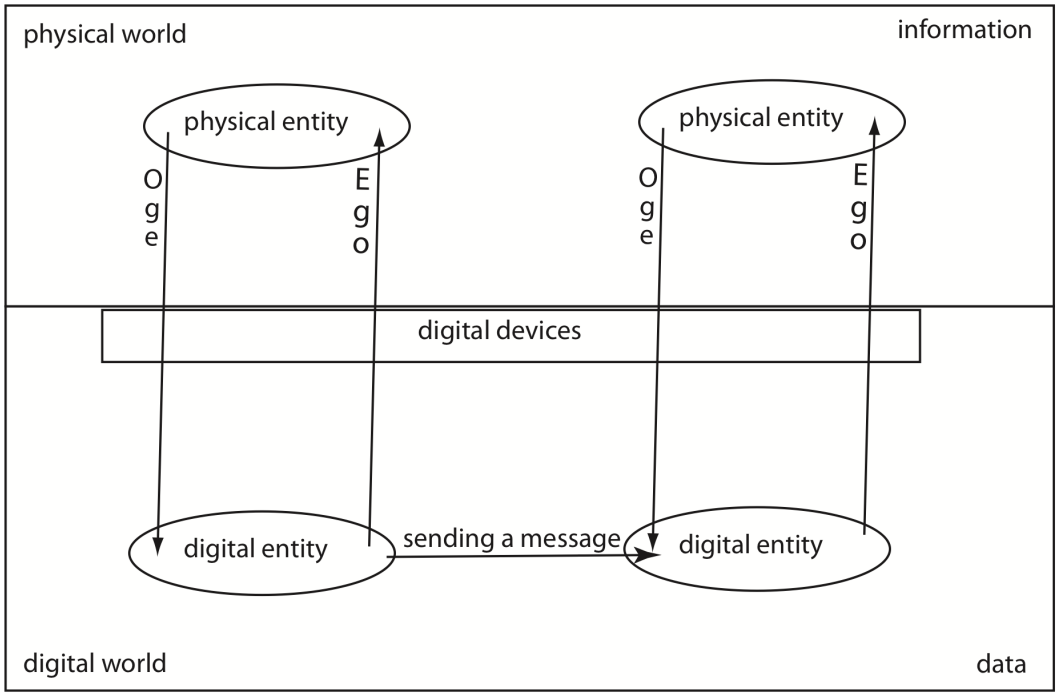
Definition of Privacy

Privacy is the **claim** of **individuals, groups, or institutions** to determine for themselves when, how, and to what extent **information** about them is communicated to **others**.

- claim → result of negotiating and enforcing
- individuals, groups, or institutions → physical entity
- information → data
- others → whom
- situations → in which context

04 Summary and Further Research

Entities, Oge() and Ego()



Definition of Privacy

Privacy of a physical entity is the result of negotiating and enforcing when, how, to what extent, and in which context which of its data is disclosed to whom.

➔ Identity management as one consequence of the definition of privacy

Further Research

- Partial identities
- Organizations and groups
- Dynamics based on time
- Anonymity based on separation of physical and digital world
- Privacy definition: direct/indirect enclosing, encryption and data

TECHNISCHE UNIVERSITÄT DRESDEN

Faculty of Computer Science, Institute of Architecture of Systems, Chair of Data Security and Data Protection

Implementability of the Identity Management Part in Pfitzmann/Hansen's Terminology for a Complex Digital World

Thank you for your attention!

References

[Pfitzmann/Hansen 2000]: Pfitzmann, M. Köhntopp (Hansen): Anonymity, unobservability, and pseudonymity - a proposal for terminology. In H. Federrath (editor): Workshop on Design Issues in Anonymity and Unobservability. Volume 2009 of Lecture Notes in Computer Science., Springer (2000), pages 1-9

[Pfitzmann/Hansen 2010]: A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. http://dud.inf.tu-dresden.de/Anon/Terminology.shtml [Version v0.33 of April 8, 2010].

[BDSG]: Bundesdatenschutzgesetz: Erster Abschnitt. (1990) (version 14.08.2009)

[Dict]: Schneider, U., Werner, D.: Taschenbuch der Informatik. 4. edn., Fachbuchverlag, Leipzig (2001)

[Westin 67]: Westin, A.F.: Privacy and Freedom. Atheneum, New York (1967)