An Introduction to Privacy

Prof. Federica Paci

Lecture Outline

- What is privacy
- Privacy properties

Learning Outcomes

- At the end of this lecture you should be able to:
  - Provide a definition of privacy
  - Provide examples of privacy threats
  - Link privacy enhancing technologies to privacy threats

The Dead of Privacy

Offline World → Online World

Information is hard/costly to collect, store, search, access:

- Conversations face to face
- Letters in the post
- Papers in a physical archive
- Paying with cash
- Following your movements
- Know who your friends are
- Looking for info in paper books

Information is easy/cheap to collect, store, search, access:

- Instant messaging
- Emails
- Files in the cloud
- Paying with credit cards
- Location tracking
- Social Network Graphs
- Searching on google

Surveillance Capitalism (S. Zuboff)

Government Surveillance

GCHQ intercepted foreign politicians' communications at G20 summits

Exclusive: phones were monitored and fake internet cafes set up to gather information from allies in London in 2009

▲ Documents uncovered by the NSA whistleblower, Edward Snowden, reveal surveillance of G20 delegates' emails and BlackBerrys. Photograph: Guardian

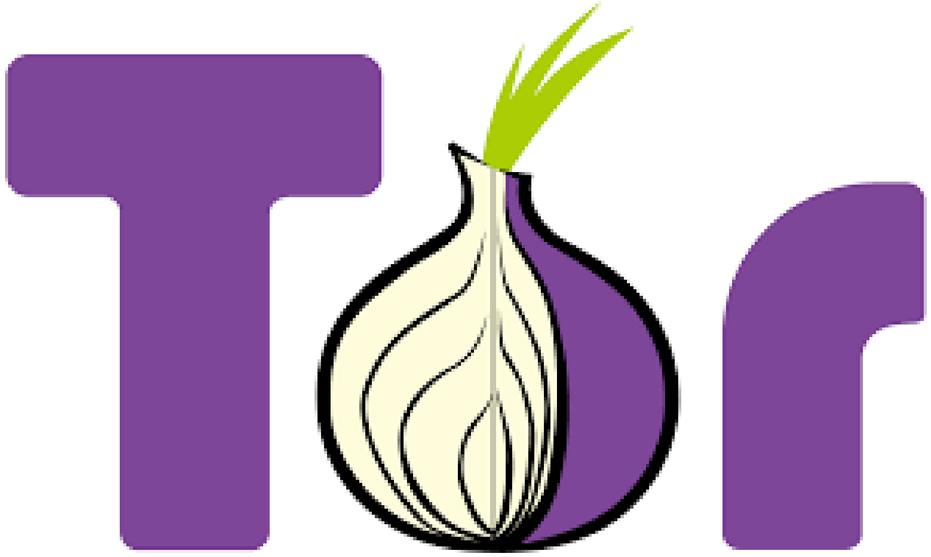
A Data Breach Every Other Day

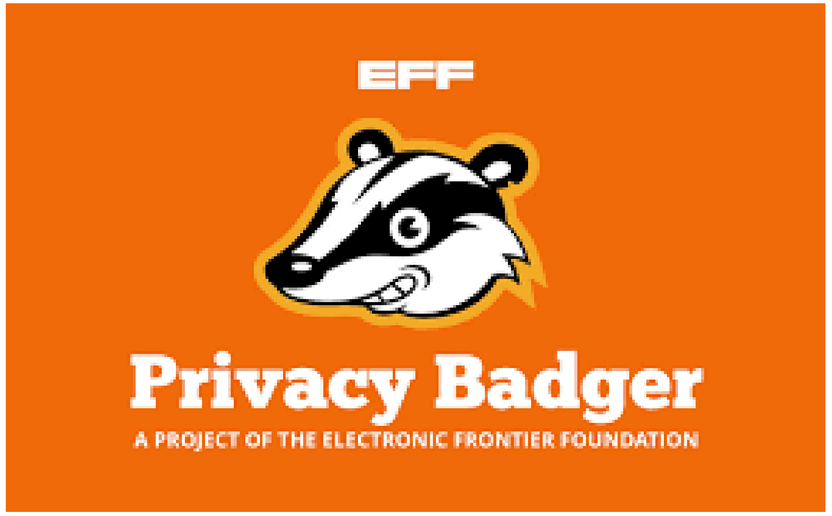
Facebook Data Breach 2021 Exposes Personal Info of 1.5 Billion Users: 2 Tools to Check If Your Data Have Been Leaked

TRENDING NEWS

iPhone Malware Security Warning: New Fake Shutdown Trick Lets Hackers Spy on You!

Re-Gaining Privacy





Privacy Definitions

What is Privacy?

Privacy is a concept in disarray. Nobody can articulate what it means. As one commentator has observed, privacy suffers from "an embarrassment of meanings."

Privacy Definitions

"the right to be let alone"
Warren and Brandeis (1890)

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

"the freedom from unreasonable constraints on the constructions of one's identity" *Agre & Rotenberg (2001)*

Privacy Definitions

"Privacy as Contextual Integrity"
Nissenbaum (2004)

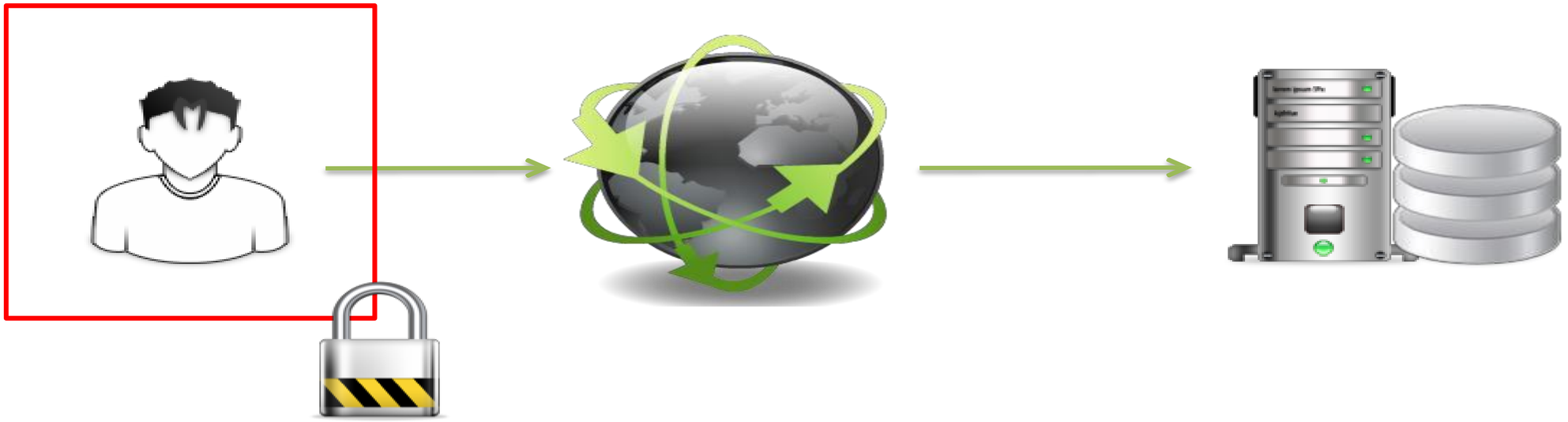
"Taxonomy of privacy harms" Solove *(2006)*

"Transparency, purpose, proportionality, accountability, "
GDPR *(2018)*

Privacy Properties

Hard Privacy

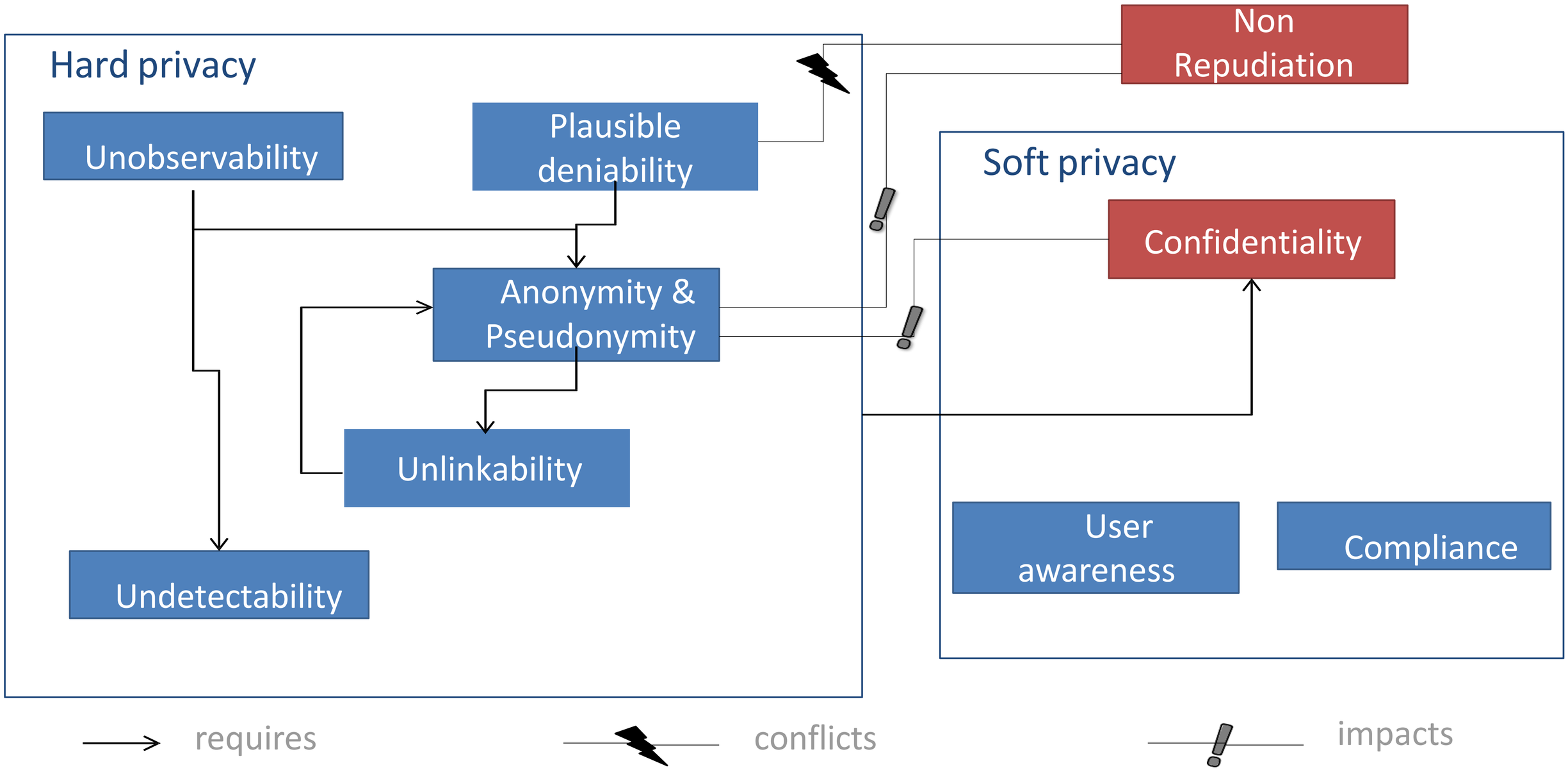
- Data minimization
  - Subject provides as little data as possible
  - Reduce as much as possible the need to “trust” other entities



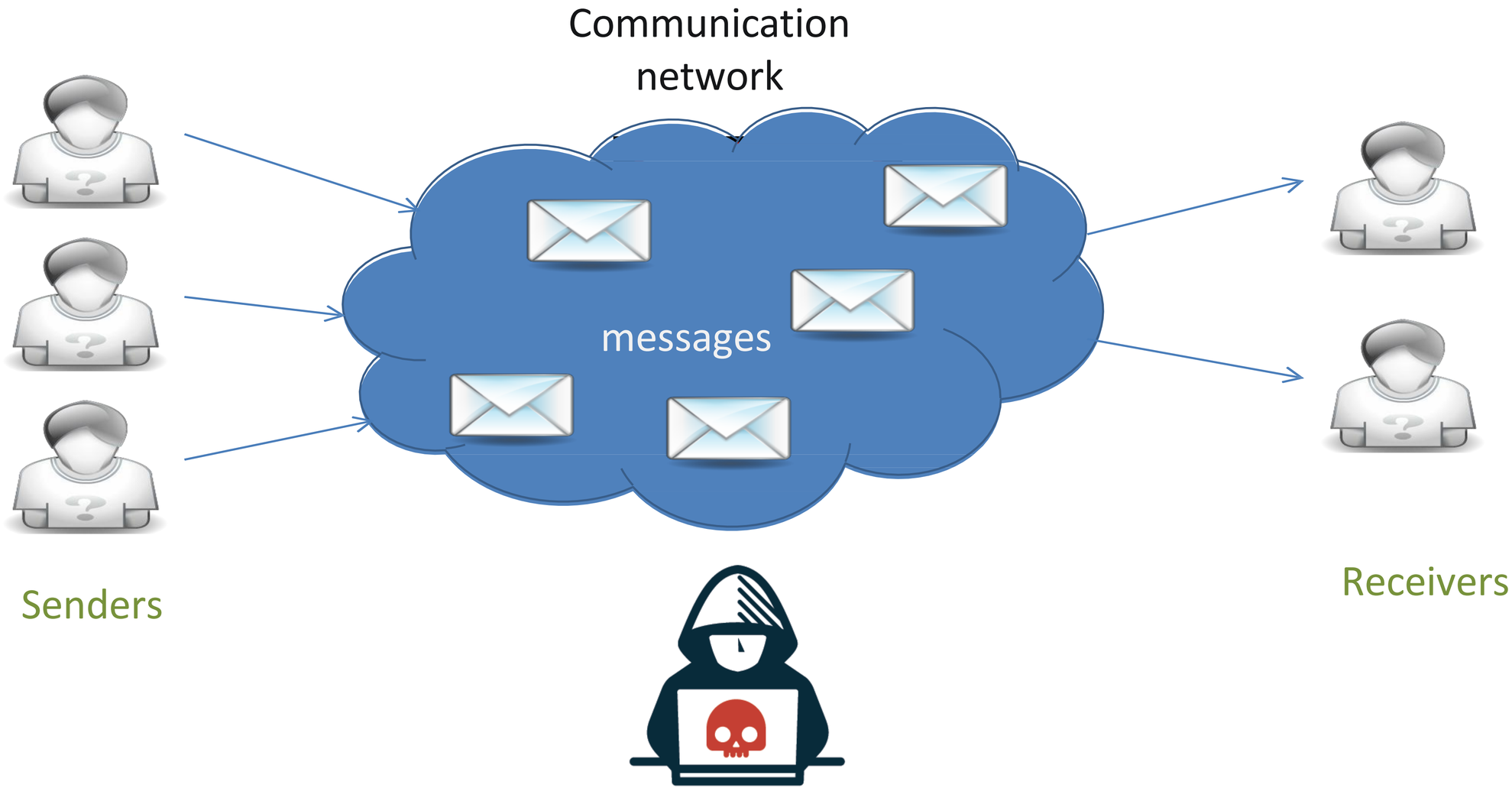
Soft privacy

- Data subject has already lost control of her data
  - In practice, very difficult for data subject to verify how her data are collected and processed

Privacy properties



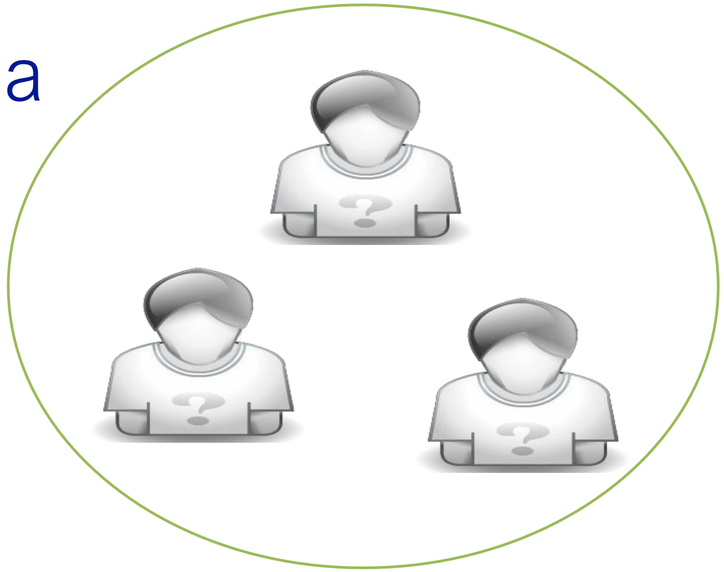
The setting



Anonimity

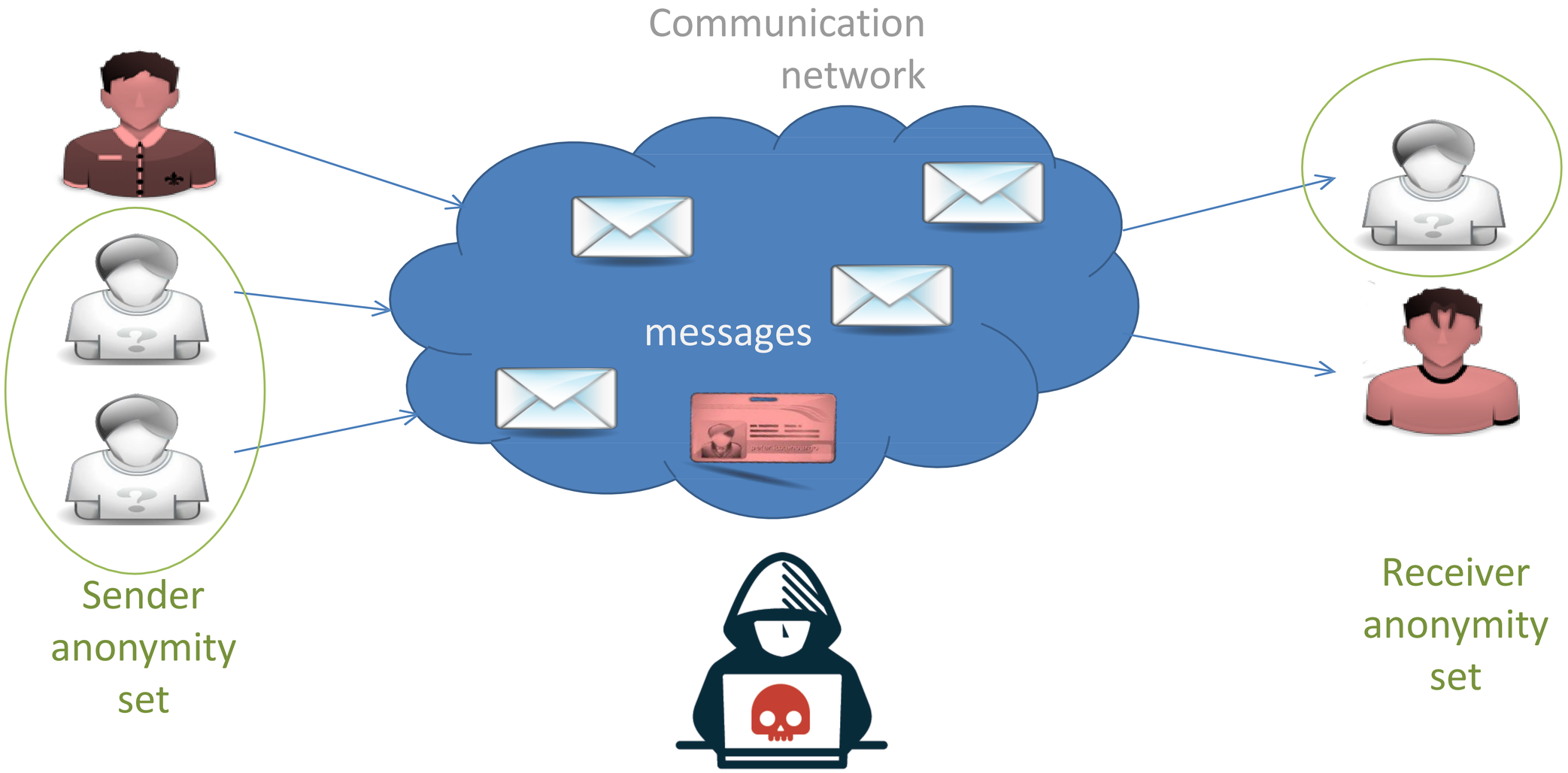
- *An attacker cannot sufficiently identify the subject within a set of subjects, the anonymity set (Pfitzmann)*
- Hiding link between identity and action / piece of information

- Examples:
  - Reader of a web page, person accessing a service
  - Sender of an email, writer of a text
  - Person to whom an entry in a
  - database relates
  - Person present in a physical location



Anonimity Set

Anonimity Set with respect to an attacker

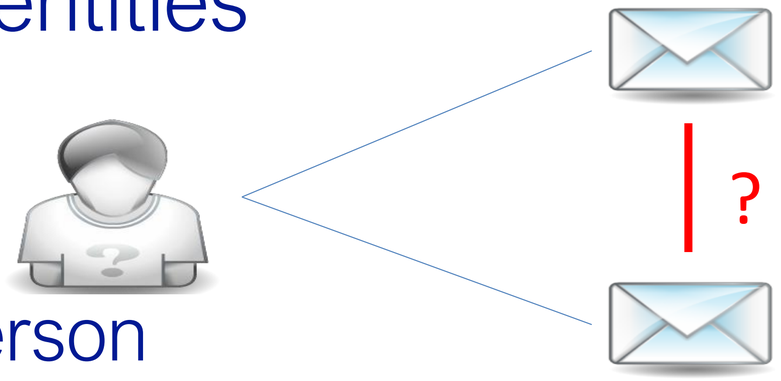


Pseudonymity

- *A pseudonym is an identifier of a subject other than one of the subjects real names.*
- *Pseudonymity is the use of pseudonyms as identifiers. (Pfitzmann)*
- Pseudonymity is the entire field between anonymity and identifiability

Unlinkability

- *Within a system, the attacker cannot sufficiently distinguish whether two or more items of interest (IOI) are related or not (Pfitzman)*
- Hiding link between two or more actions / identities /pieces of information
- Examples:
  - Two anonymous letters written by the same person
  - Two web page visits by the same user
  - Entries in two databases related to the same person
  - Two people related by a friendship link
  - Same person spotted in two locations at different points in time

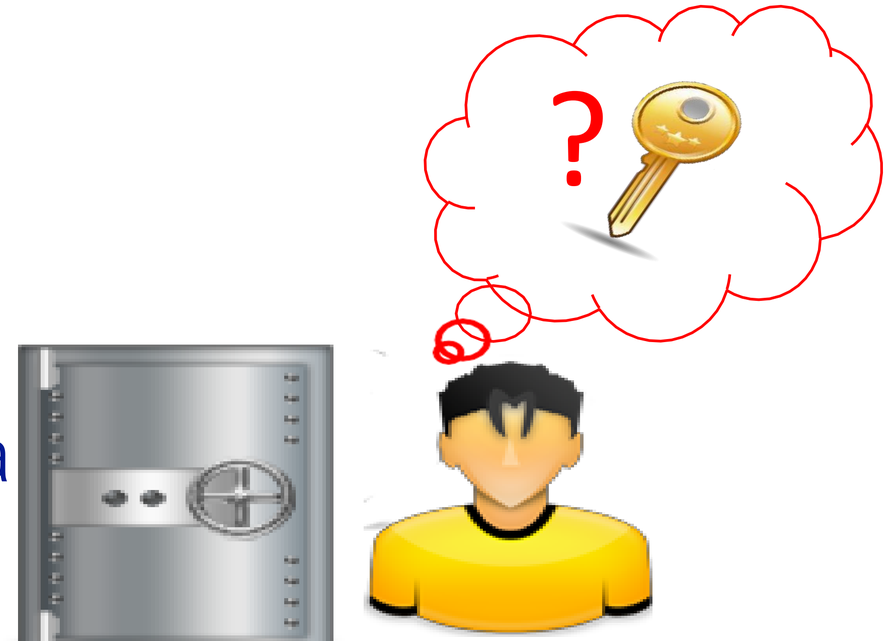


Undetectability

- **Undetectability:** The attacker cannot sufficiently distinguish whether it exists or not (Pfitzmann)
- **Unobservability**:
  - undetectability of the IOI against all subjects uninvolved in it and
  - anonymity of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI (Pfitzmann)
- Hiding user activity
- Examples:
  - Impossible to see whether someone is accessing a web page
  - Impossible to know whether an entry in a database corresponds to a real person
  - Impossible to distinguish whether someone or no one is in a given location

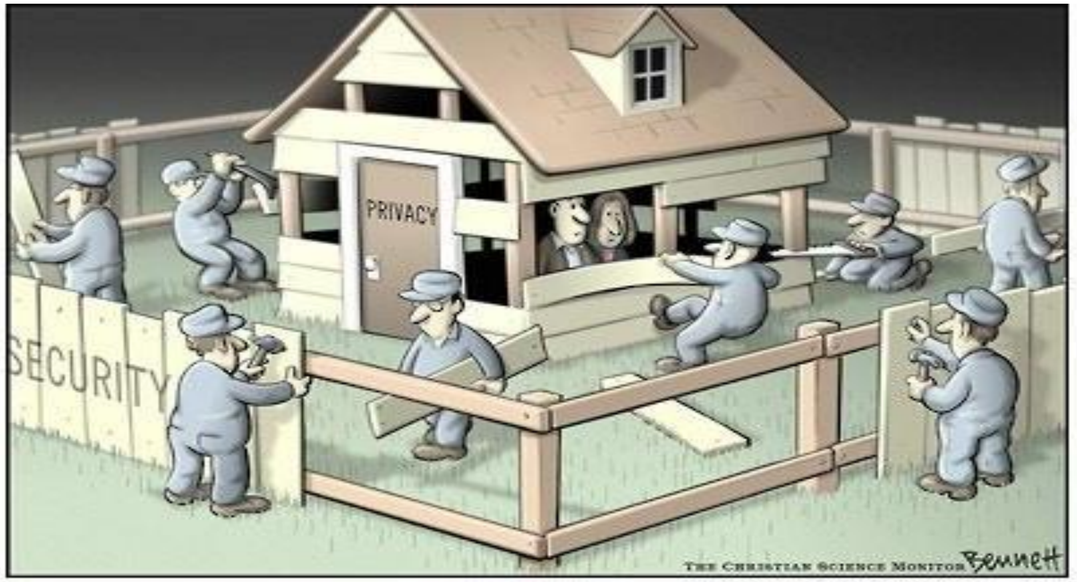
Plausible Deniability

- Not possible to prove user knows, has done or has said something
- Examples:
  - Resistance to coercion:
    - Not possible to prove that a person has hidden information in a computer
    - Not possible to know that someone has the combination of a safe
  - Possibility to deny having been in a place at a certain point in time
  - Possibility to deny that a database record belongs to a person
  - Off-the-record conversations



Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information *(NIST)*



Compliance

- It is related to legislation on data protection
- General Data Protection Regulation specifies the principles for processing personal data within EU

Awareness

- Users should be made aware of the consequences of sharing information

- Suggested solution: Feedback & awareness tools

Resources

- Daniel J. Solove. A Taxonomy of Privacy. Available at: https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf
- Enisa report on Privacy and Data Protection by Design – from policy to engineering 2014