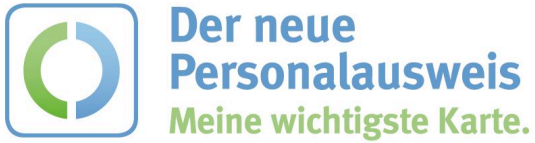
PersoApp

Secure and User-Friendly Internet Applications



Constitutive Meeting of the PersoApp Advisory Board
Berlin, September 4, 2013

Prof. Dr. Ahmad-Reza Sadeghi
Dr. Sven Wohlgemuth

Head of PersoApp Consortium
Technische Universität Darmstadt
Center for Advanced Security Research Darmstadt (CASED)

System Security Lab · Fraunhofer SIT · Technische Universität Darmstadt · CASED

Malicious Authentication leads to Breach of Confidentiality

HOME › NEWS › SECURITY

'Man in the Browser' malware defeats banks' two-step online authentication

By Shawn Knight
On February 7, 2012, 11:30 AM EST

21 Gefällt mir 8 +1 14 Tweet 20

A new breed of malware called a Man in the Browser (MitB) attack can successfully bypass a bank's two-step online authentication process. In most cases, the victim isn't even aware their account has been compromised until it's too late.

Once the malicious code finds its way to your computer, it lays dormant until the user navigates to a specific website – a secure bank. During the typical log in process, the malware is activated and acts as a middleman between the user and the bank's website. Most variants will ask the victim to reenter their credentials as part of an "enhanced security measure." If the victim falls for this prompt, the attacker then has full access to the bank account.

Authentication data of bank customers stolen

Customers are re-directed to a "secure bank" to enter username, password, etc.

- Attacker gets full access on bank account
- Bank customer is not aware of it
- Majority of web security software didn't detect this attack

http://www.techspot.com/news/47351-man-in-the-browser-malware-defeats-banks-two-step-online-authentication.html

PlayStation Network hack will cost Sony $170M

By Martyn Williams
May 23, 2011 06:57 AM ET 7 Comments

Share +1 Like 32 More

IDG News Service - Sony expects the hack of the PlayStation Network and will cost it ¥14 billion ($170 million) this financial year, it said Monday.

Unknown hackers hit the network gaming service for PlayStation 3 consoles in April, penetrating the system and stealing personal information from the roughly 77 million accounts on the PlayStation Network and sister Qriocity service. A second attack was directed at the Sony Online Entertainment network used for PC gaming.

Sony responded to the attacks by taking the systems offline. It called in several computer security companies to conduct forensic audits and rebuilt its security system.

Users in many countries are being offered a year-long identity-theft protection program and free games. The cost estimate includes those actions and associated legal costs, said Masaru Kato, Sony's CFO, at a

Unauthorized access on personal data of 77 million customers

- Target: Sony PlayStation Network
- Detection via file "Anonymous" on Sony Online Entertainment Servers
- Costs: $170M (incl. Identity theft insurance package for customers, improvement to network security, free access to content, ...)

http://www.computerworld.com/s/article/9216926/PlayStation_Network_hack_will_cost_Sony_170M

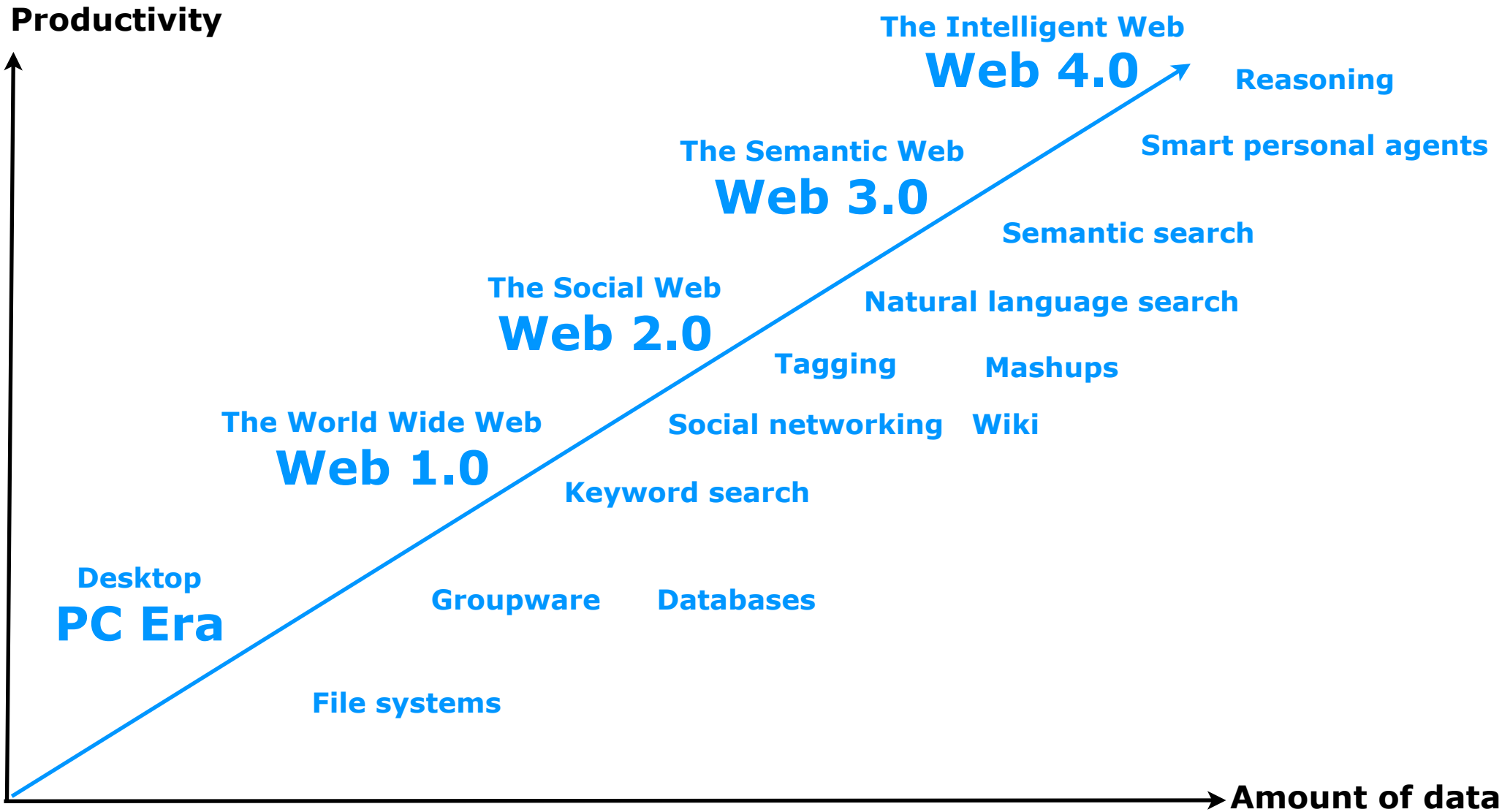
Agenda

I. From Login to Privacy Control

II. Extending Identity Infrastructure

III. PersoApp: Call for Participation

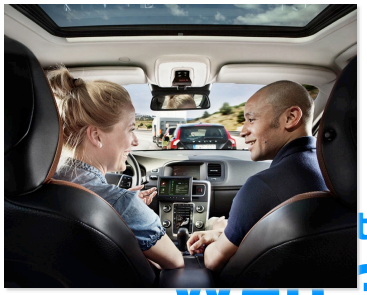
I. From Login to Privacy Control



Own figure based on Radar Networks & Nova Spivack, 2007; E. Brynjolfsson and A. McAfee, Race against the Machine, 2011.

I. From Login to Privacy Control

Productivity



The Intelligent Web
Web 4.0

Reasoning

Smart personal agents

tic Web
Web 3.0

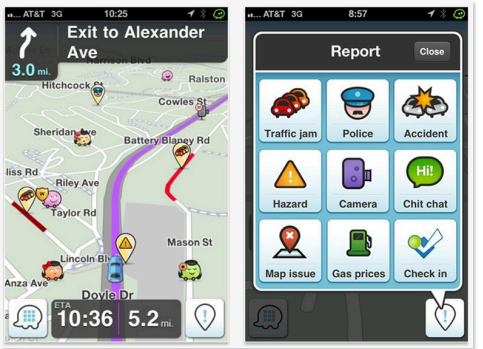
Semantic search

Natural language search

The Social Web
Web 2.0

Tagging

Mashups



The World Wide Web
Web 1.0

Social networking

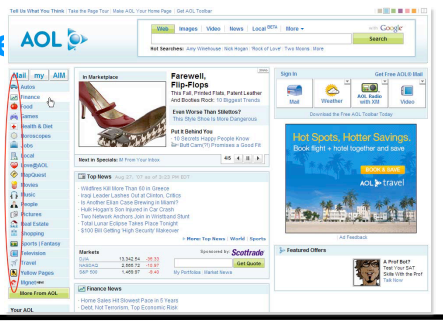
Wiki

Keyword search

Desktop
PC Era

Groupware

Database

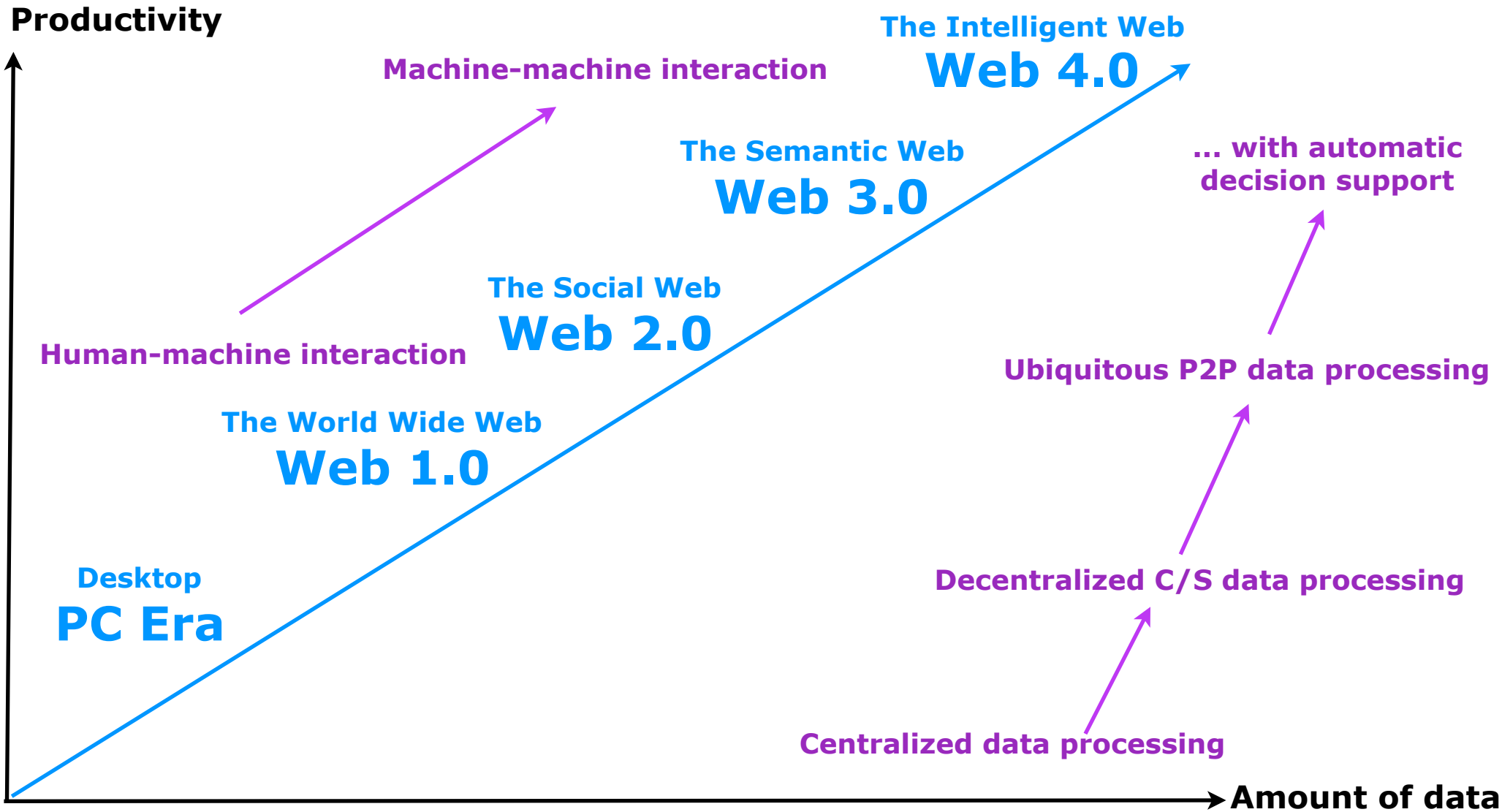


File systems

Amount of data

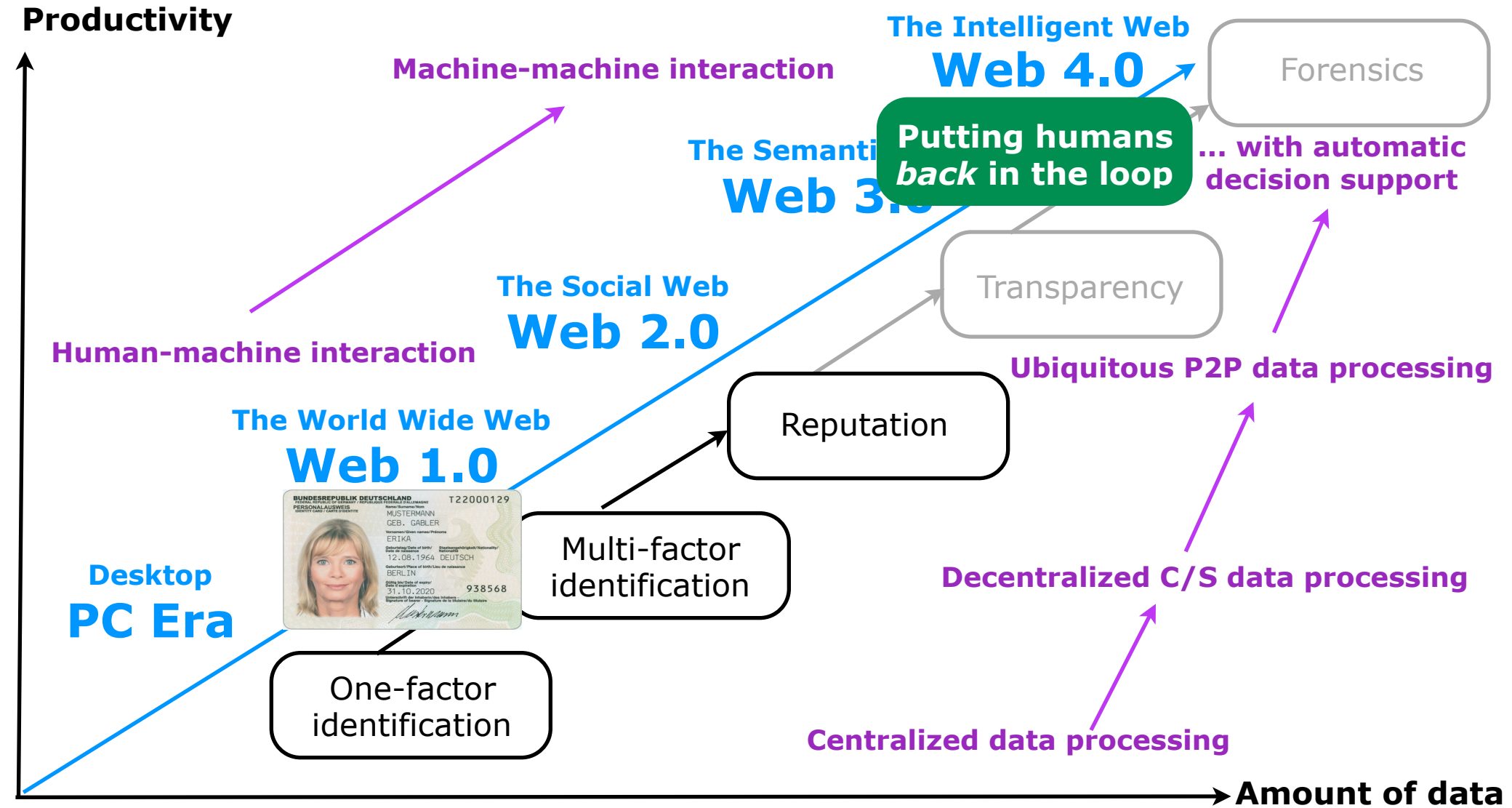
Own figure based on Radar Networks & Nova Spivack, 2007; E. Brynjolfsson and A. McAfee, Race against the Machine, 2011.

I. From Login to Privacy Control



Own figure based on Radar Networks & Nova Spivack, 2007; E. Brynjolfsson and A. McAfee, Race against the Machine, 2011.

I. From Login to Privacy Control



Own figure based on Radar Networks & Nova Spivack, 2007; E. Brynjolfsson and A. McAfee, Race against the Machine, 2011.

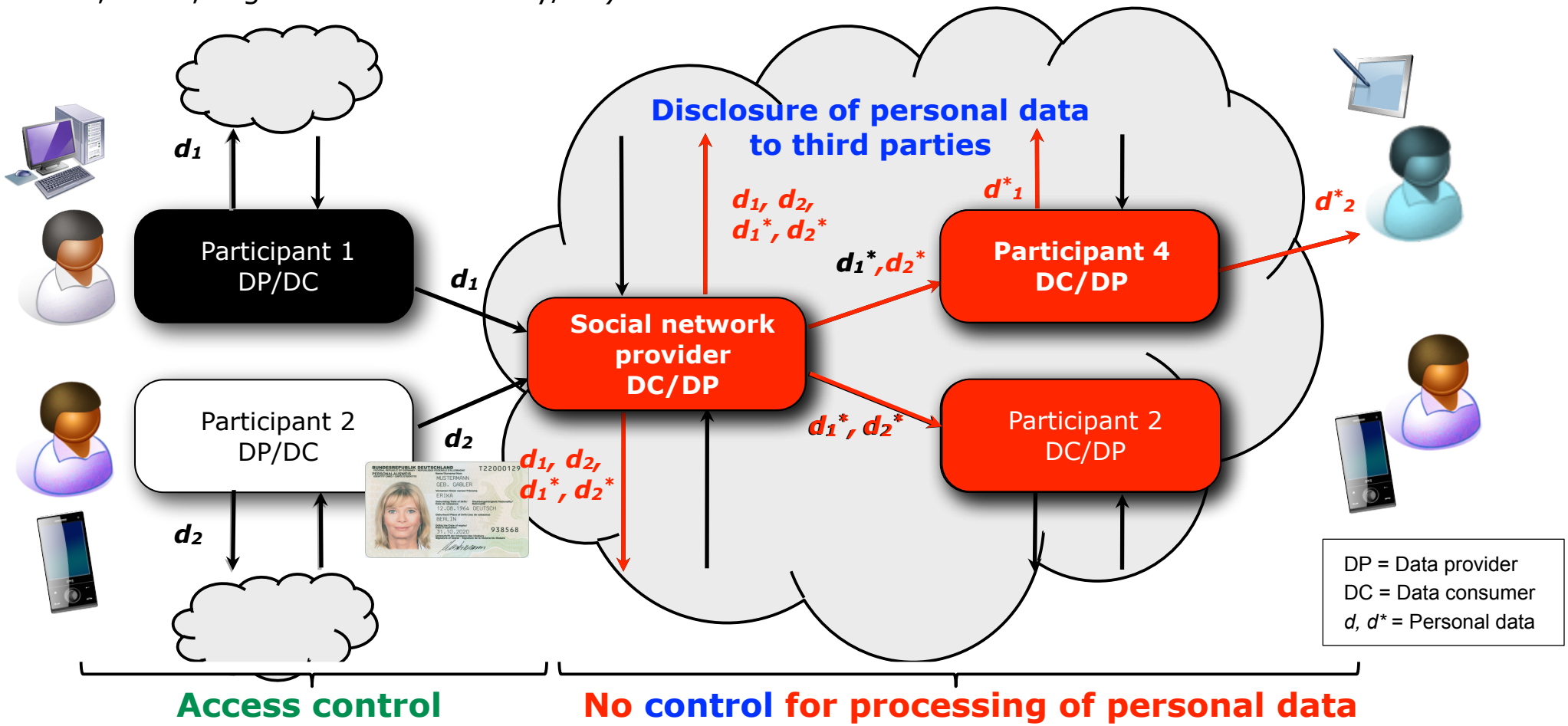
Login and Privacy

Example: Social Network

Privacy legislation:

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

(Westin, 1967; regulations of Germany/EU)



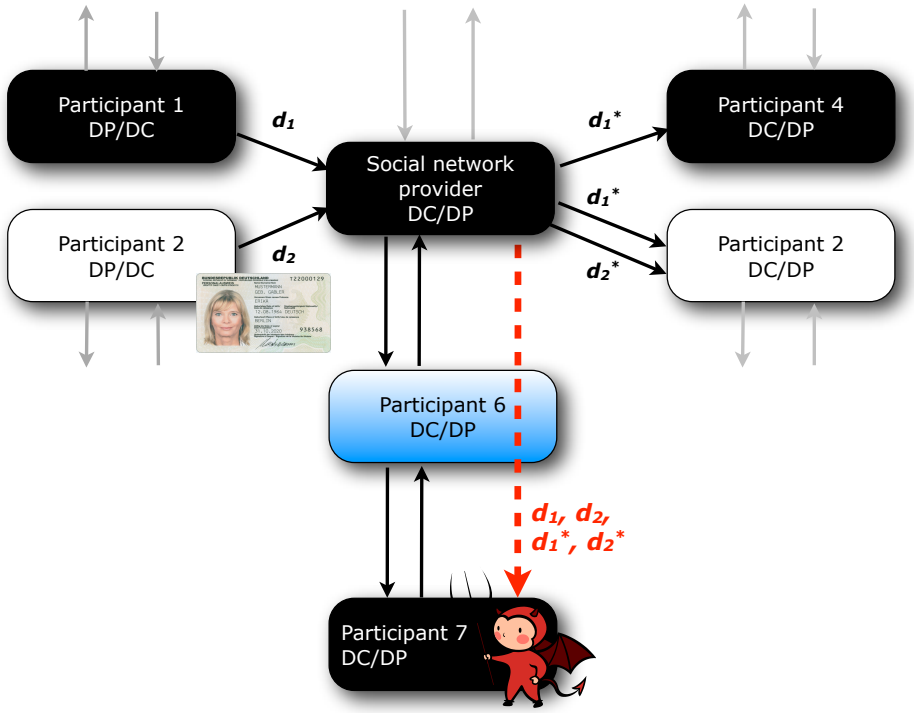
Own figure according to A. Pretschner, M. Hilty, and D. Basin, 2006; N. Sonehara, I. Echizen, and S. Wohlgemuth, 2011

Misuse of Identity cannot be completely prevented

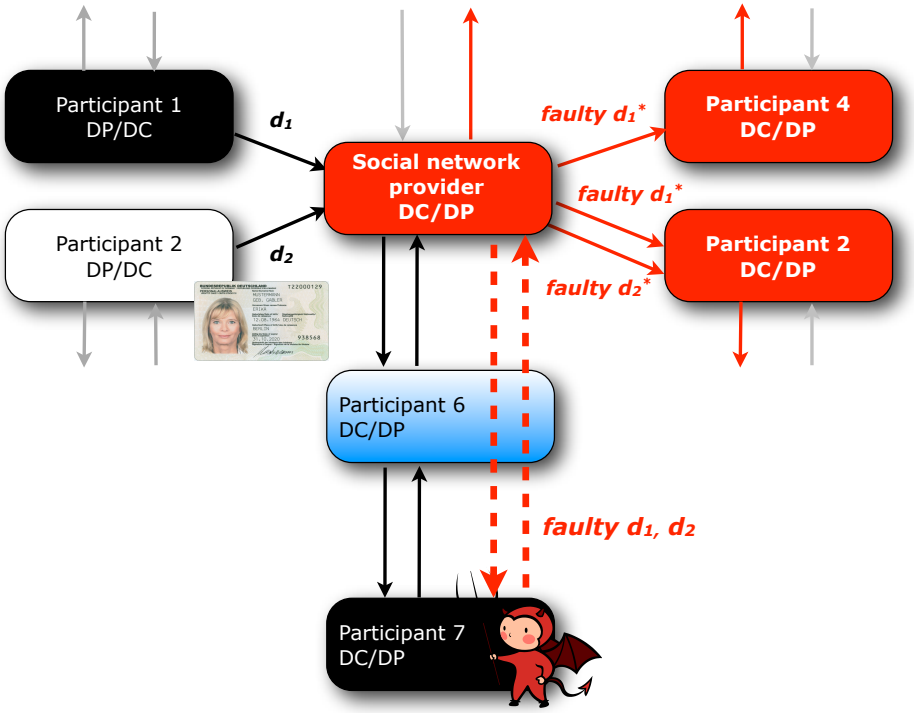
Example: Social Network

Web 2.0 IT systems: "Programming at run-time" - Dependencies emerge at run-time

Assumption: Each authorized IT system is proven to be secure



Case (a): Passive interference



Case (b): Active interference

- Desired dependencies imply vulnerabilities by undesired ones (covert channels, escalation of rights, …)[1]
- **Impossible to automatically detect all undesired dependencies[2]**

[1] B. Lampson 1973; R. White 1990; L. Davi, A. Dmitrienko, A.-R. Sadeghi, and M. Winandy 2010

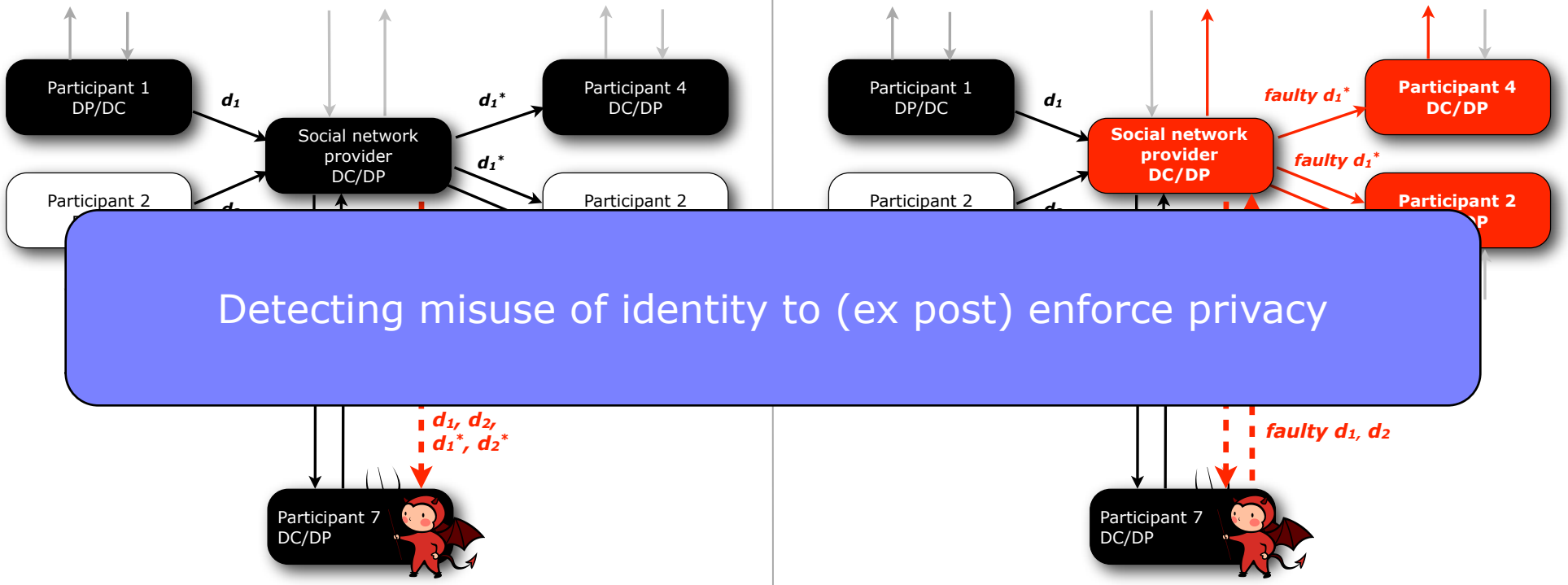
[2] C. Wang und S. Ju 2006

Misuse of Identity cannot be completely prevented

Example: Social Network

Web 2.0 IT systems: "Programming at run-time" - Dependencies emerge at run-time

Assumption: Each authorized IT system is proven to be secure



- Desired dependencies imply vulnerabilities by undesired ones (covert channels, escalation of rights, …)[1]
- **Impossible to automatically detect all undesired dependencies[2]**

[1] B. Lampson 1973; R. White 1990; L. Davi, A. Dmitrienko, A.-R. Sadeghi, and M. Winandy 2010

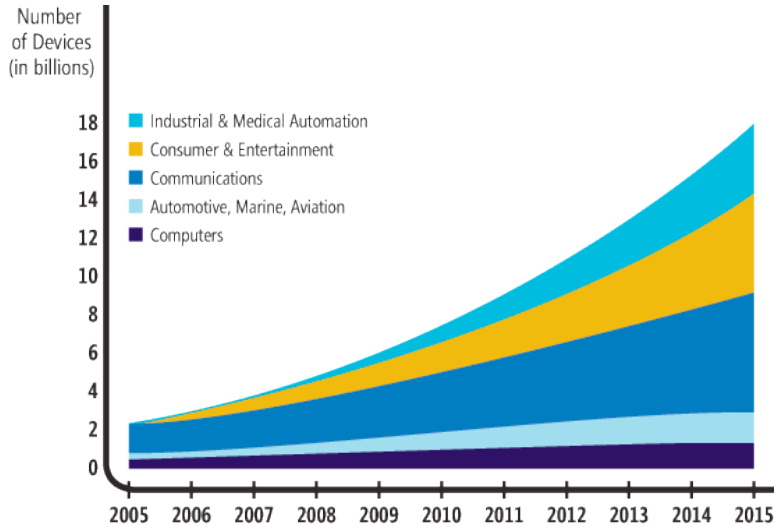
[2] C. Wang und S. Ju 2006

II. Extending Identity Infrastructure

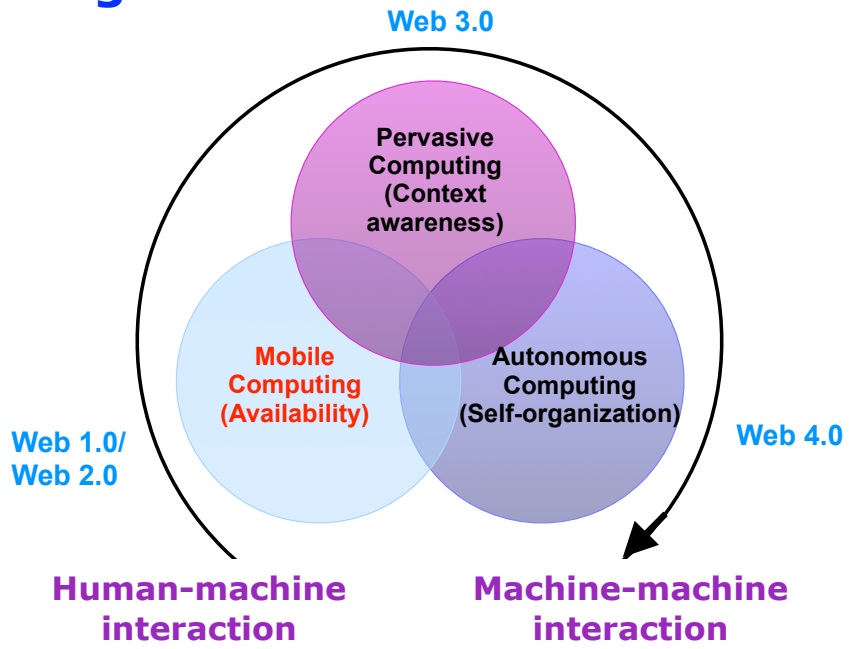
- Mobility
- Identity control
- Privacy control
- Privacy forensics

Mobility

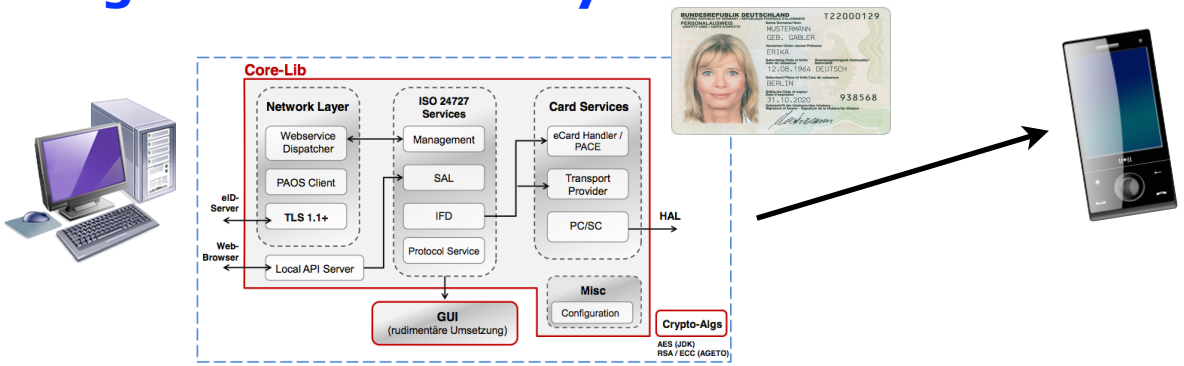
Connections and ubiquitous data processing increase



Source: John Gantz, The Embedded Internet, Methodology and Findings, IDC, January 2009



Migration to mobility

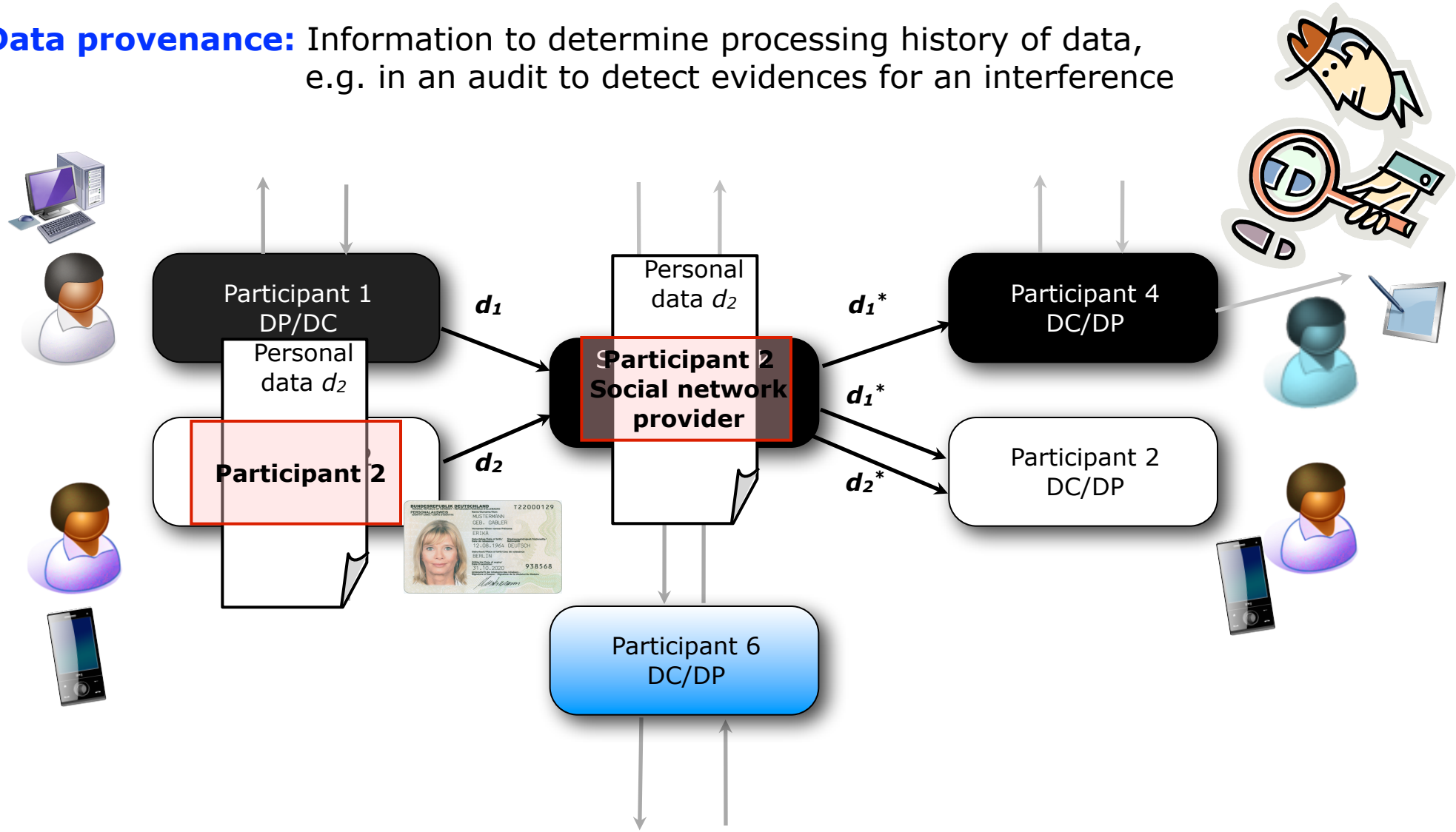


- Smartphone as personal digital assistant
- Sony Xperia with USB reader
- Android 4.04 (V1)
- Pre-release
- Open source software library
- Security concept and review

Identity Control

Transparency: Detecting misuse of identity by understanding disclosure of personal data

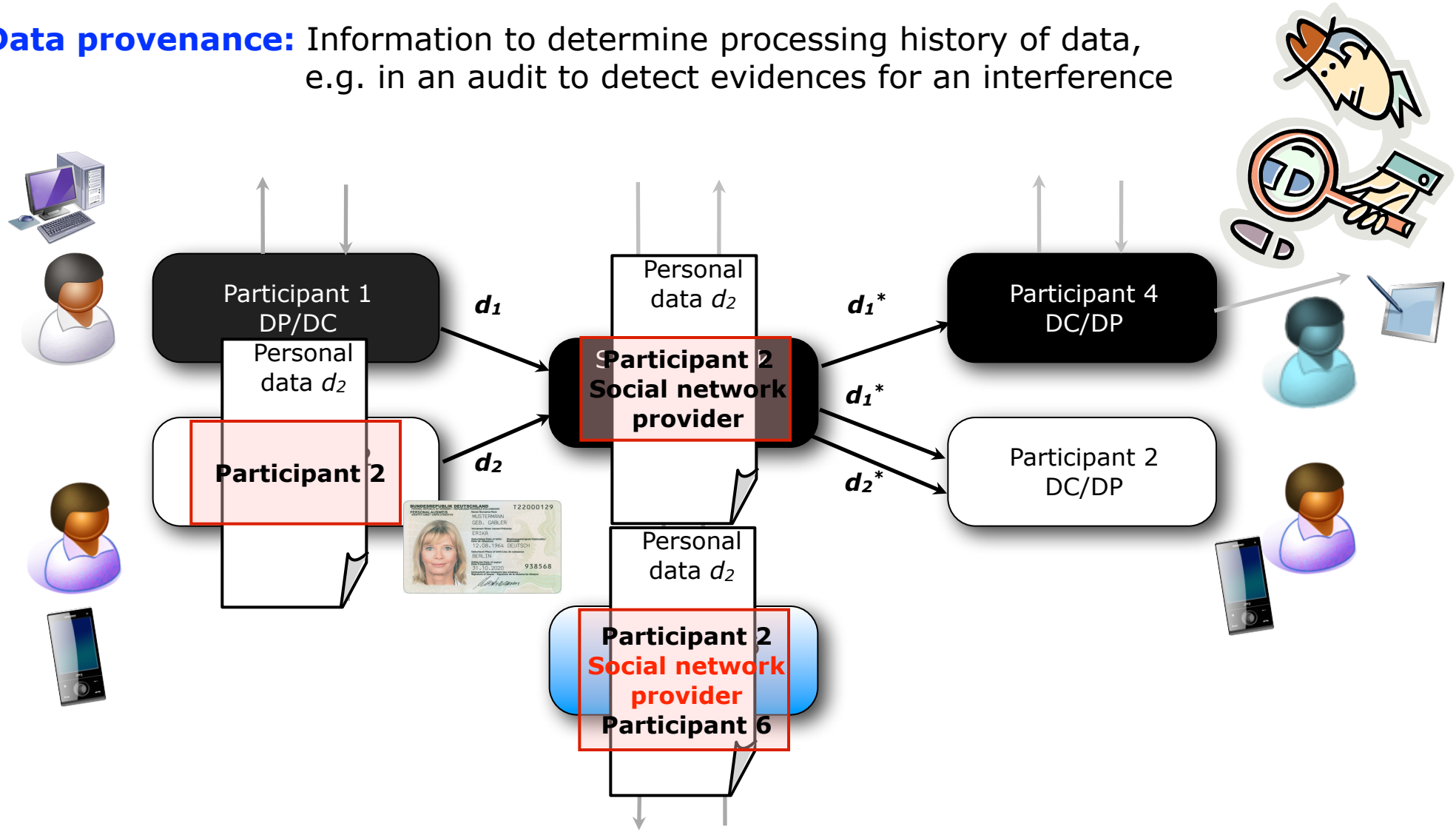
Data provenance: Information to determine processing history of data,
e.g. in an audit to detect evidences for an interference



Identity Control

Transparency: Detecting misuse of identity by understanding disclosure of personal data

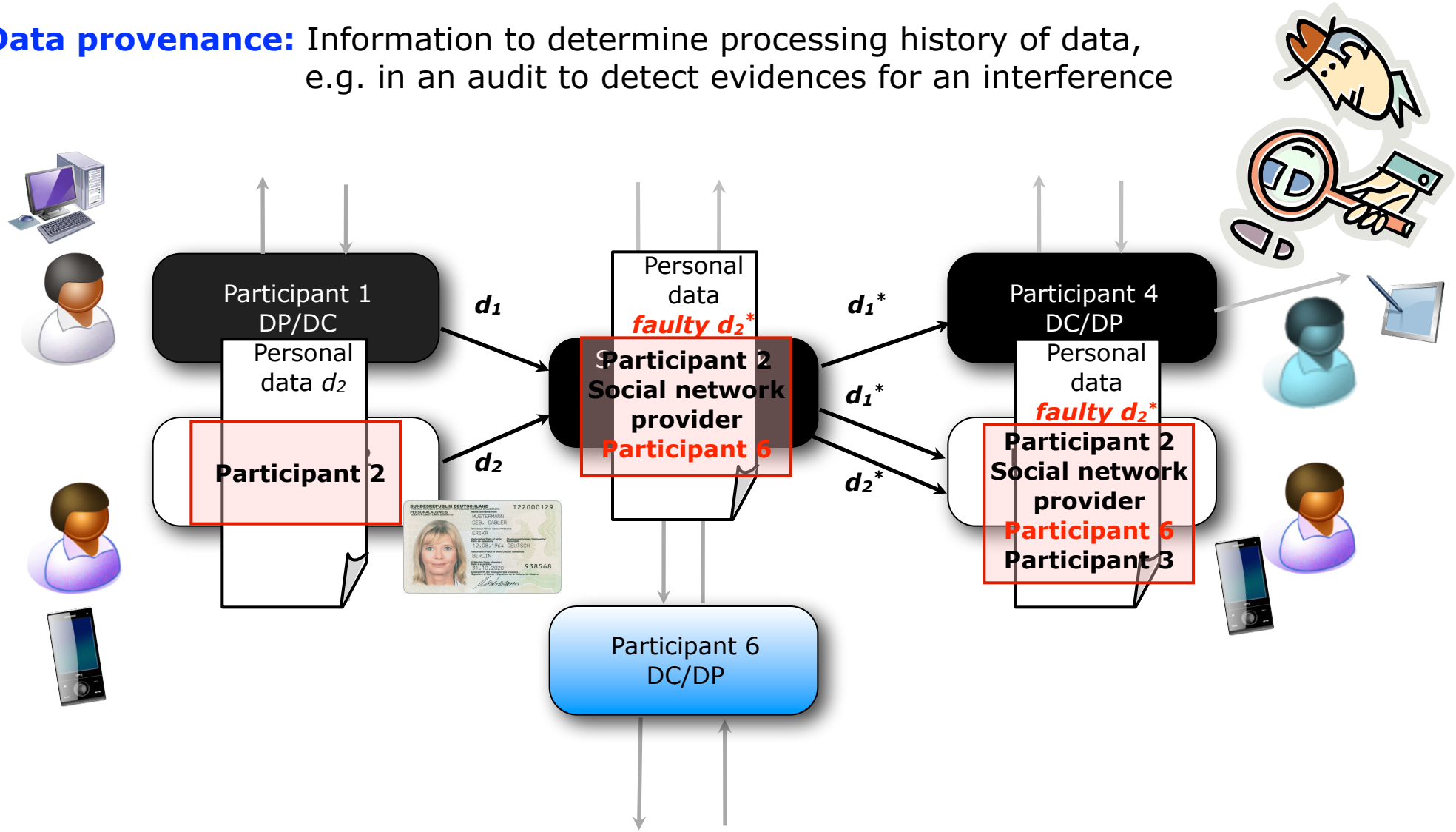
Data provenance: Information to determine processing history of data, e.g. in an audit to detect evidences for an interference



Identity Control

Transparency: Detecting misuse of identity by understanding disclosure of personal data

Data provenance: Information to determine processing history of data,
e.g. in an audit to detect evidences for an interference



Identity Control based on German ID Card

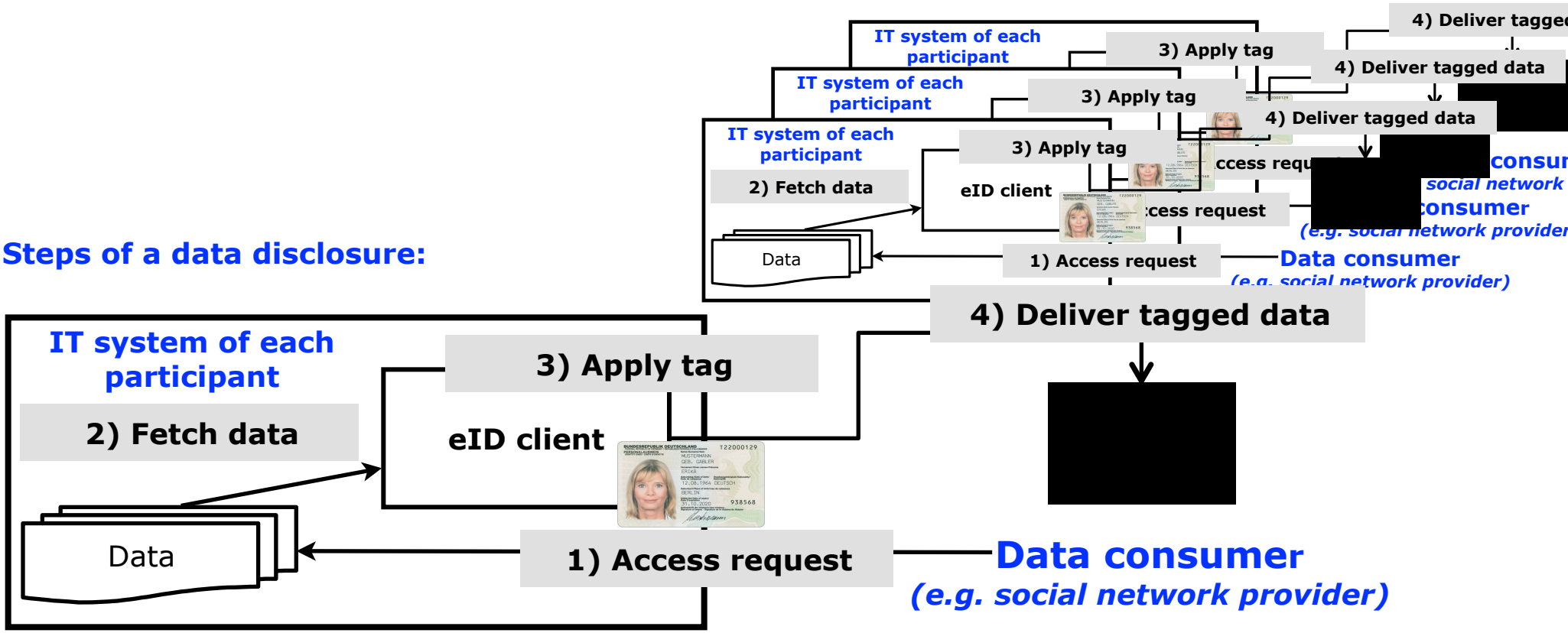
Binding data provenance information as a tag to data

- Online identification with German national ID card

In addition: eID client must enforce

- Disclosed data is tagged with updated provenance information
- Provenance information is authentic (e.g. secure logging, digital watermarking, ...)

Steps of a data disclosure:



Identity Control based on German ID Card

Binding data provenance information as a tag to data

- Online identification with German national ID card

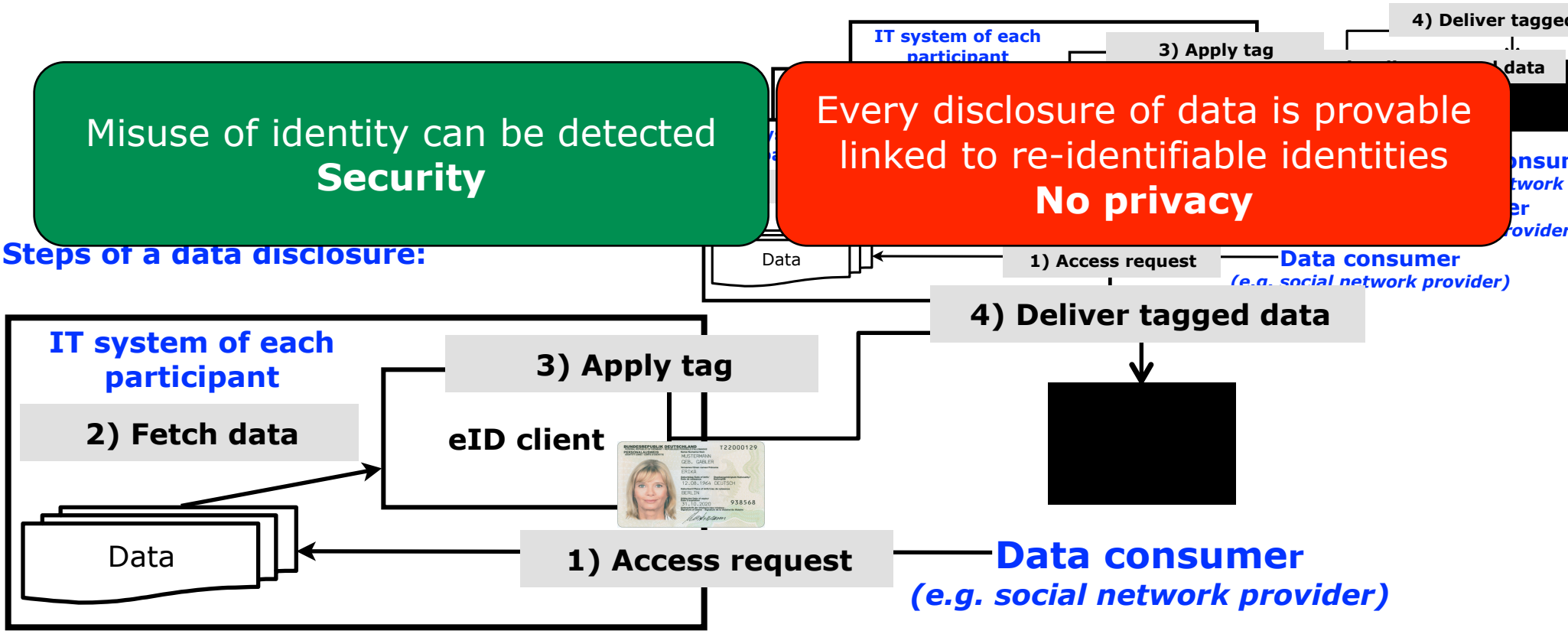
In addition: eID client must enforce

- Disclosed data is tagged with updated provenance information
- Provenance information is authentic (e.g. secure logging, digital watermarking, ...)

Misuse of identity can be detected
Security

Every disclosure of data is provable linked to re-identifiable identities
No privacy

Steps of a data disclosure:

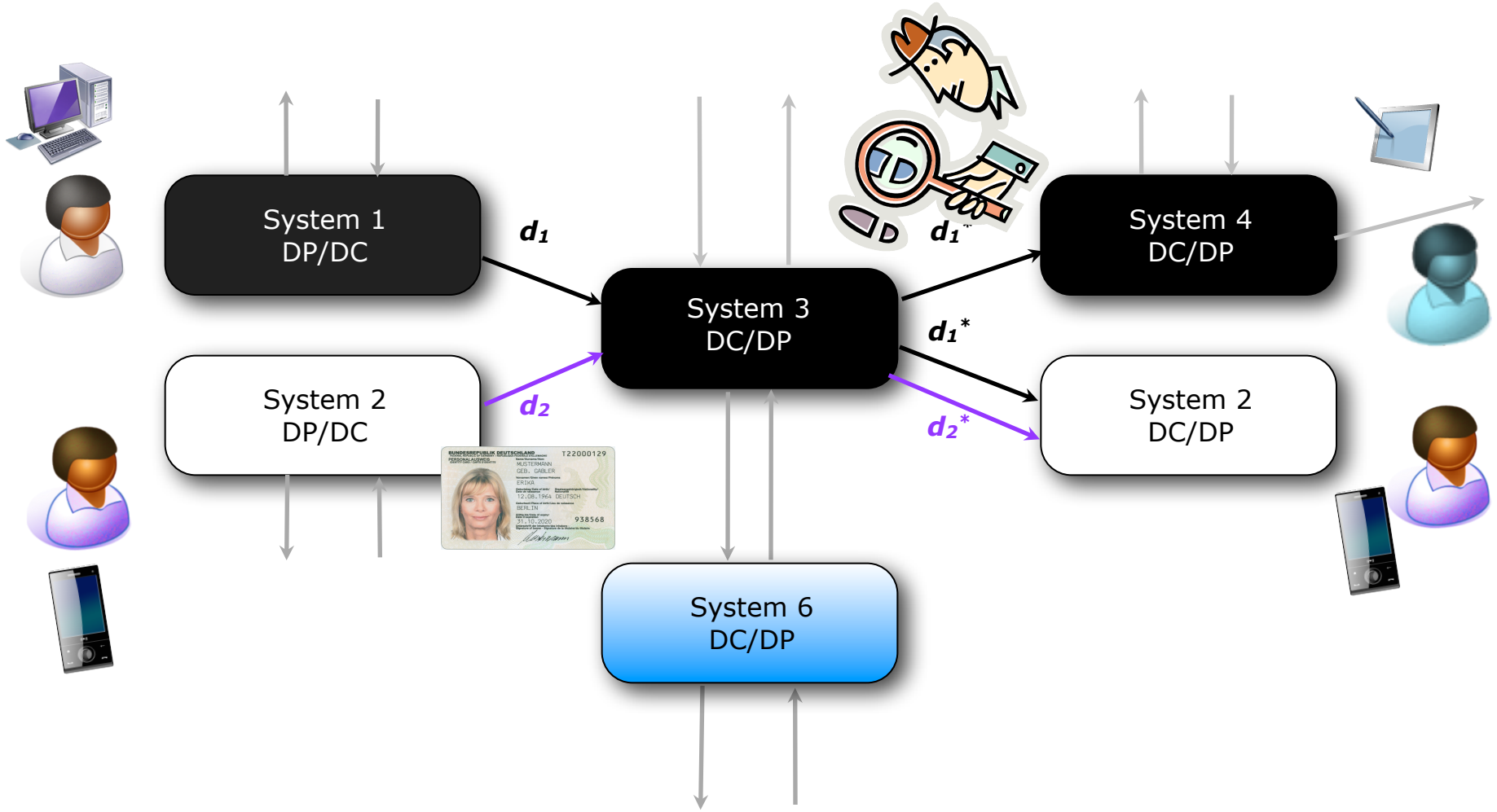


Privacy Control

Security and Privacy: Isolating disclosure of personal data by obligations according to SLA

Isolation: **Pseudonymous** online identification of the German national ID card

In addition: eID client must specify isolation by non-linkable delegation of rights

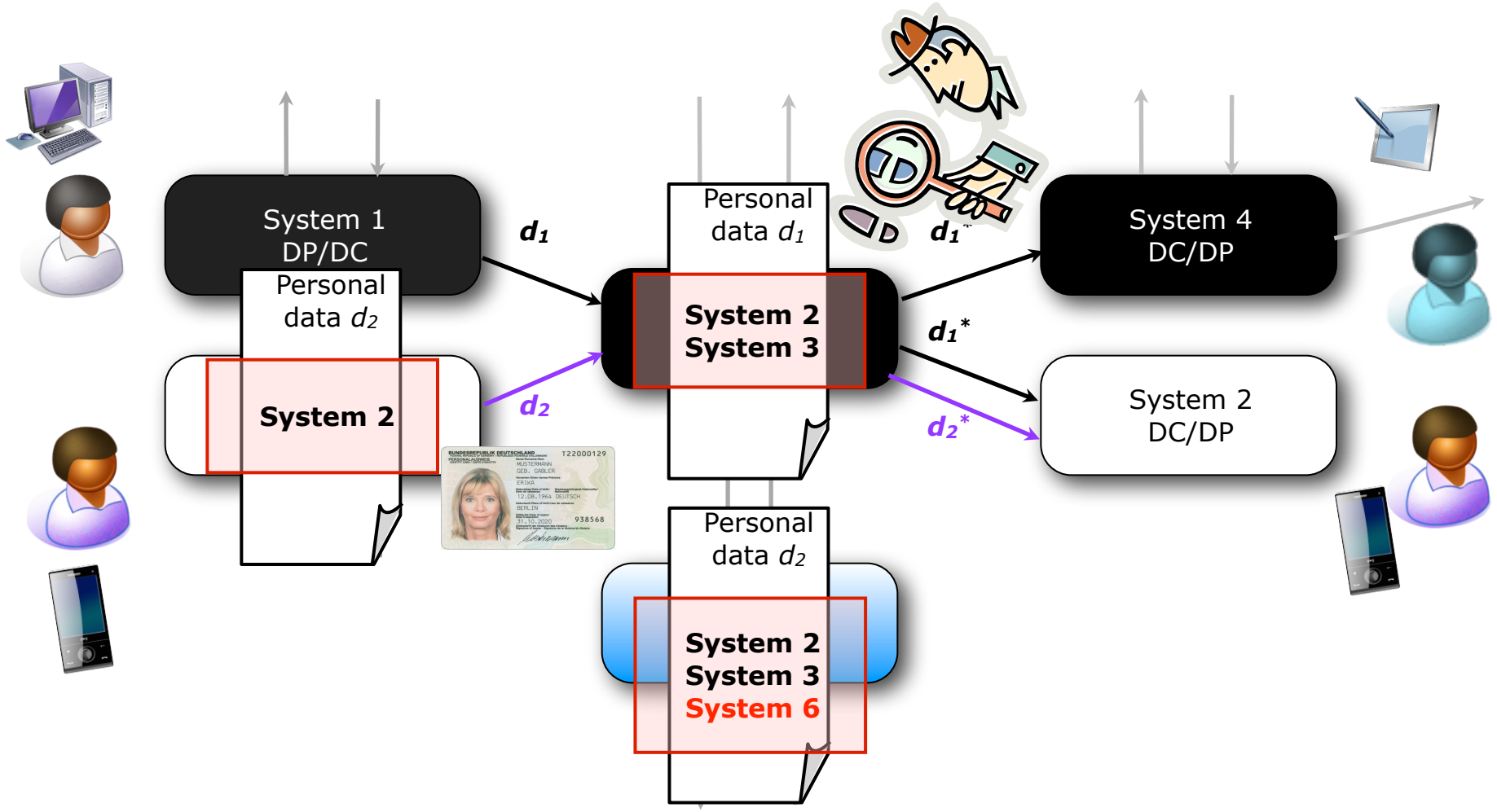


Privacy Control

Security and Privacy: Isolating disclosure of personal data by obligations according to SLA

Isolation: **Pseudonymous** online identification of the German national ID card

In addition: eID client must specify isolation by non-linkable delegation of rights

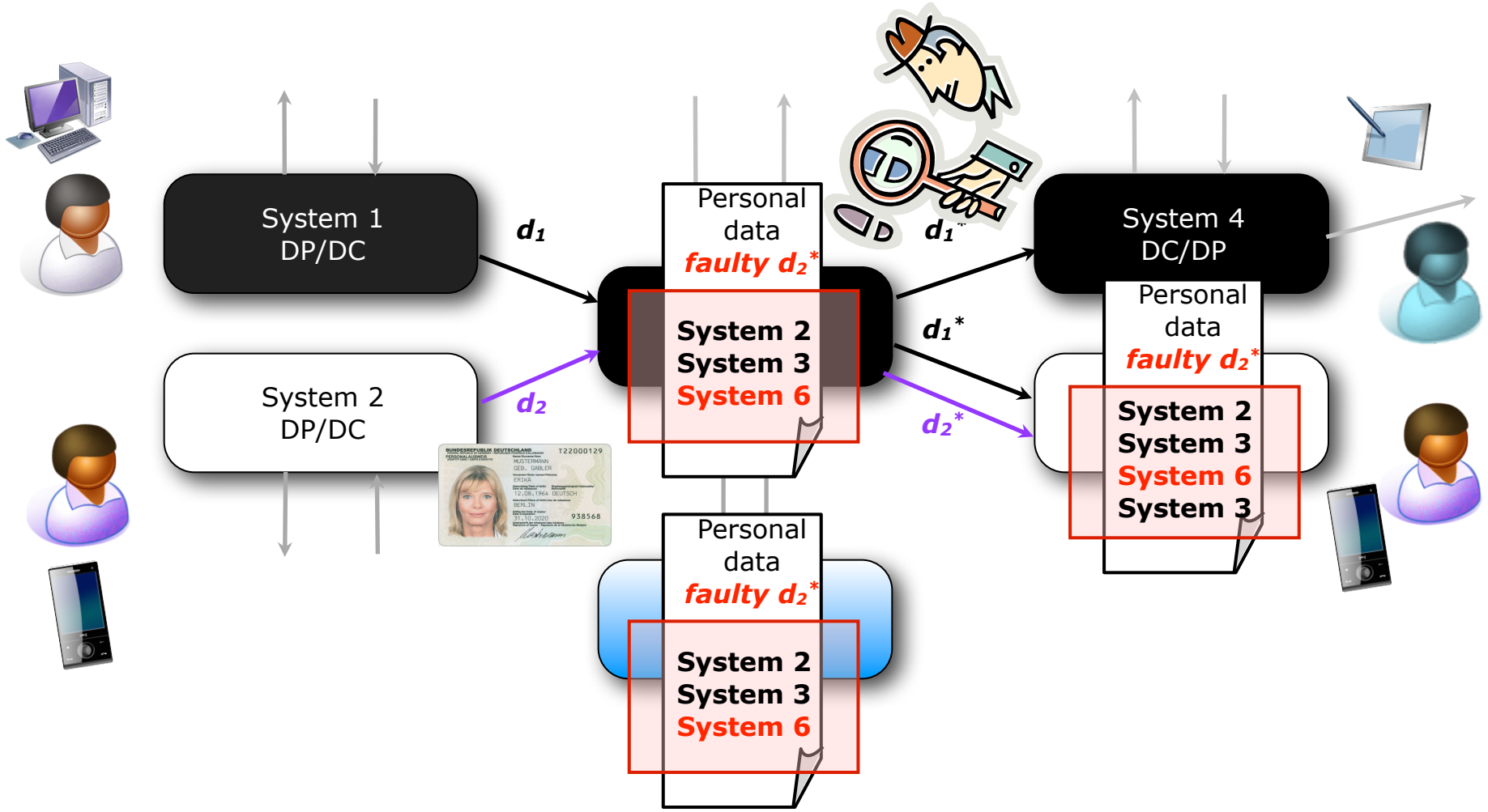


Privacy Control

Security and Privacy: Isolating disclosure of personal data by obligations according to SLA

Isolation: **Pseudonymous** online identification of the German national ID card

In addition: eID client must specify isolation by non-linkable delegation of rights

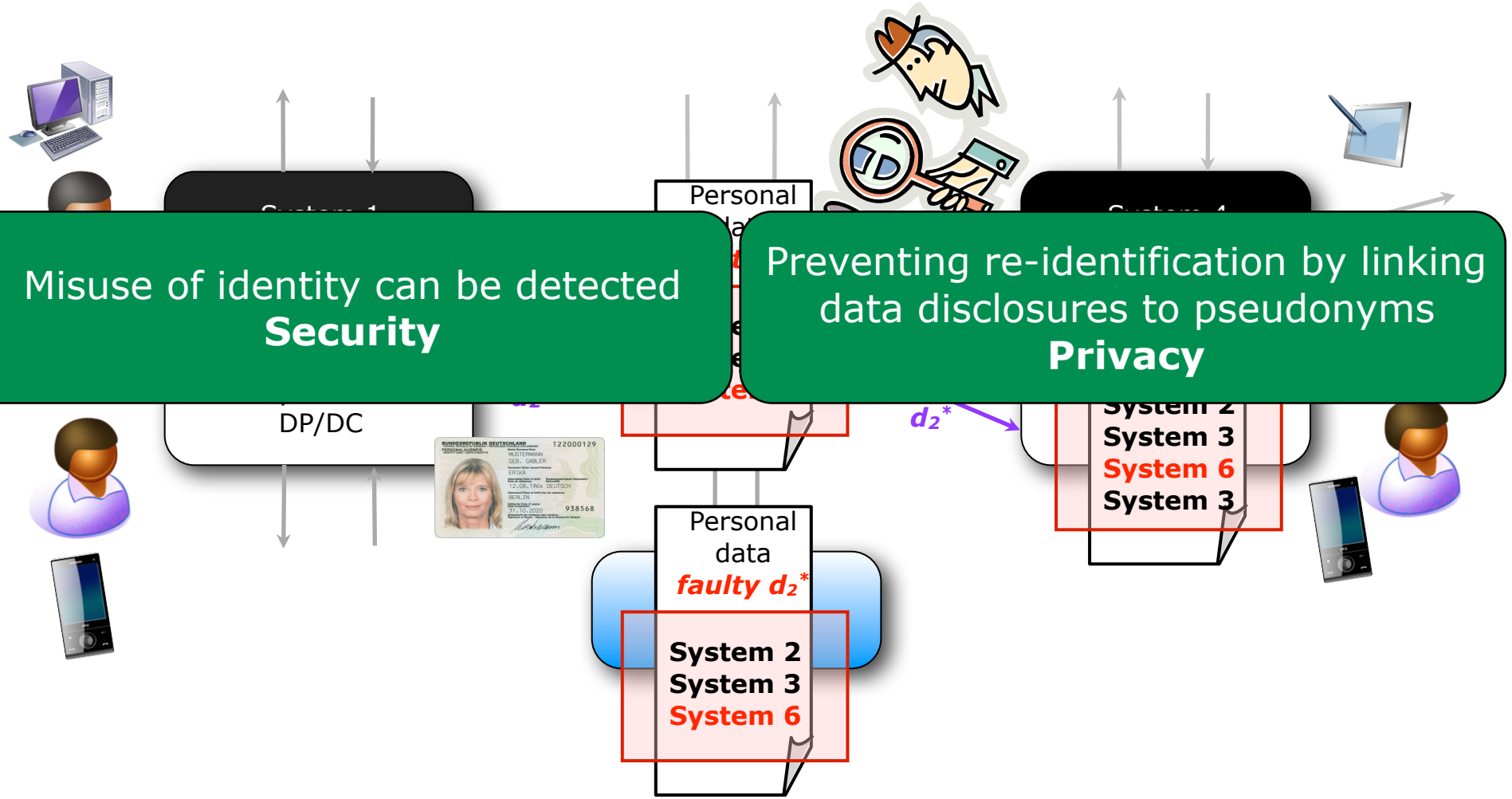


Privacy Control

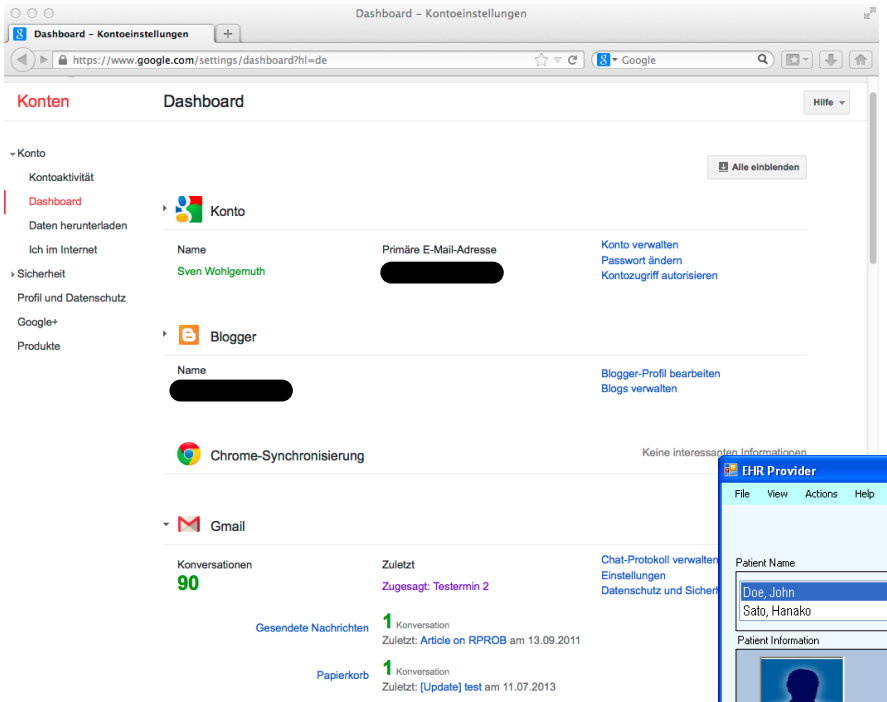
Security and Privacy: Isolating disclosure of personal data by obligations according to SLA

Isolation: **Pseudonymous** online identification of the German national ID card

In addition: eID client must specify isolation by non-linkable delegation of rights

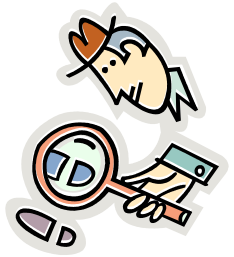


Example: Identity Control, Privacy Control



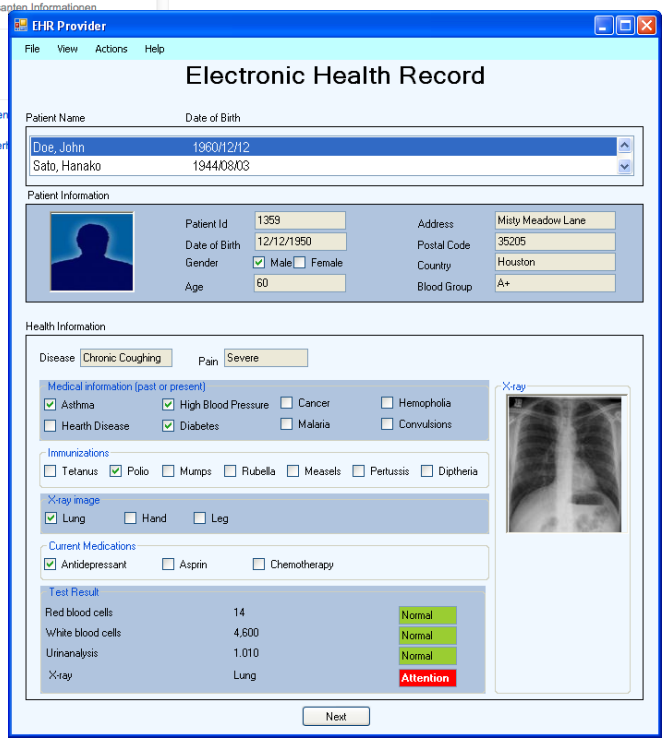
Google Dashboard

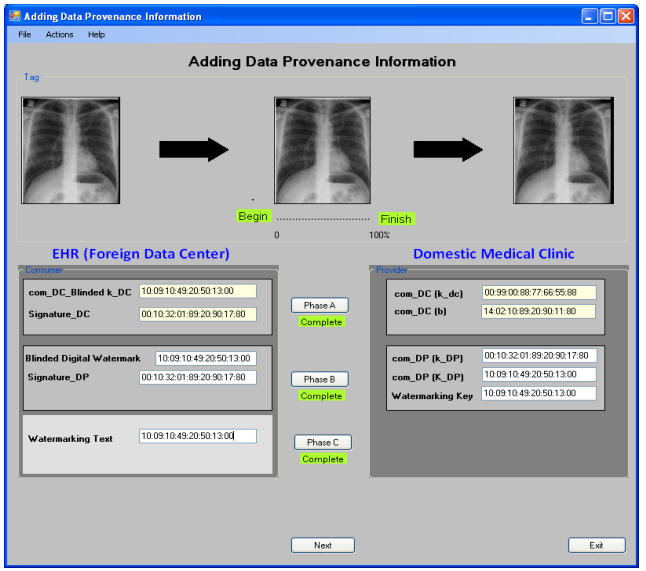
- Overview on services and some data used with Google account
- Does not contain information about participant from other sources



Exemplary data tagging

- Adding data provenance to personal images

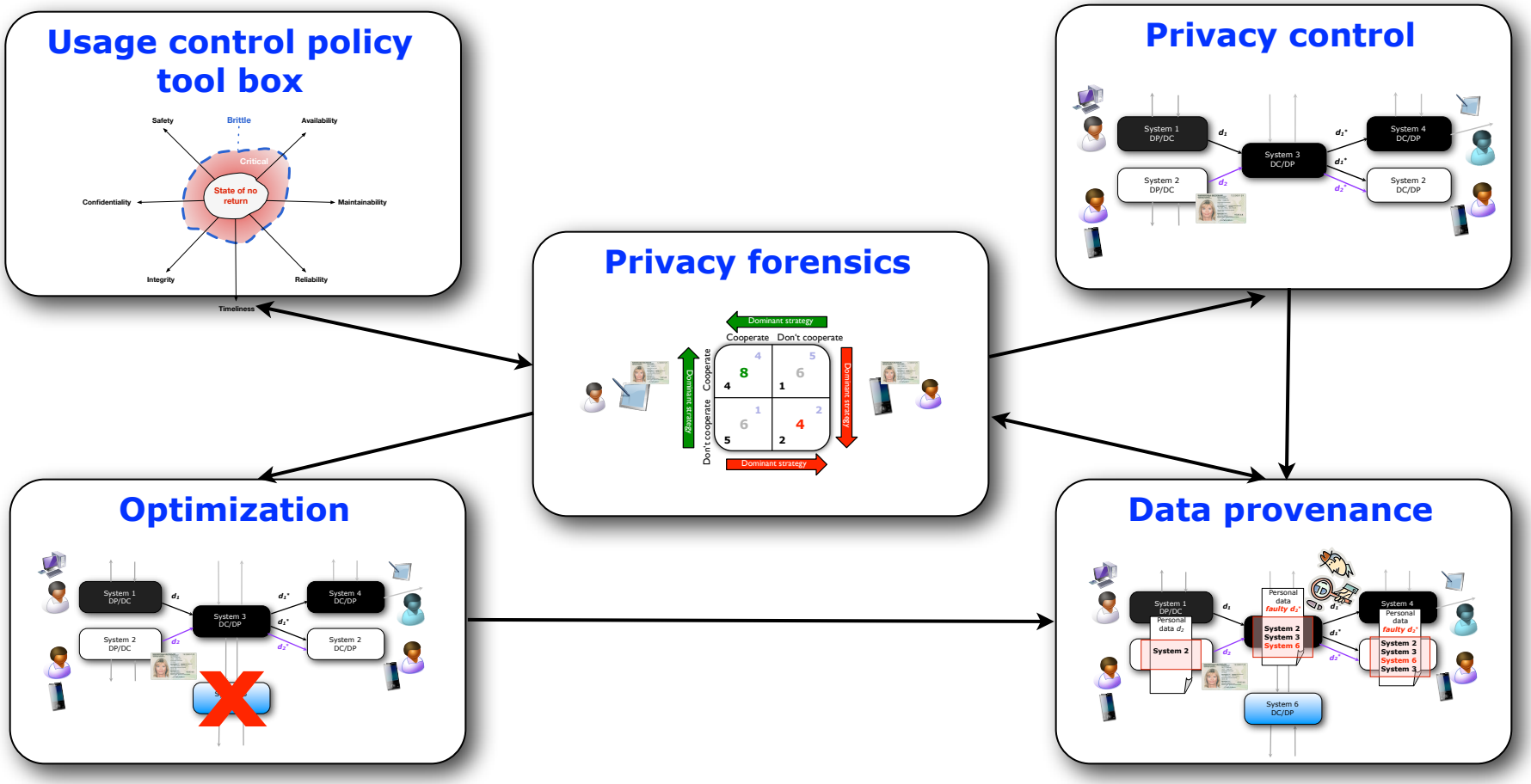




Privacy Forensics

Problem: Trust relationship leading to non-cooperating equilibrium due to unknown liability

Increasing trust by coordinating and measuring privacy control for acceptable equilibriums



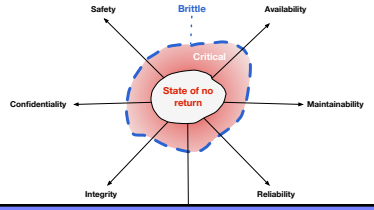
Privacy Forensics

Problem: Trust relationship leading to non-cooperating equilibrium due to unknown liability

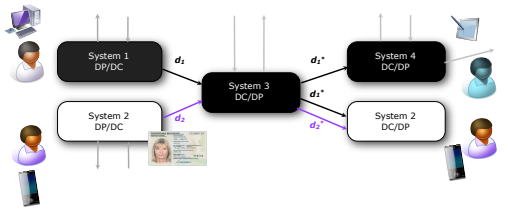
Increasing trust by coordinating and measuring privacy control for acceptable equilibriums

eID client assesses evidences on interferences (for each system)

Usage control policy tool box



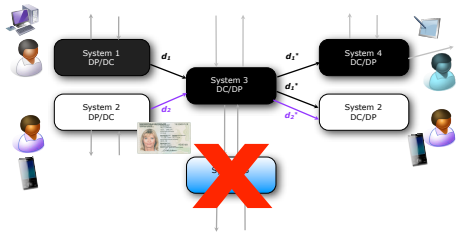
Privacy control



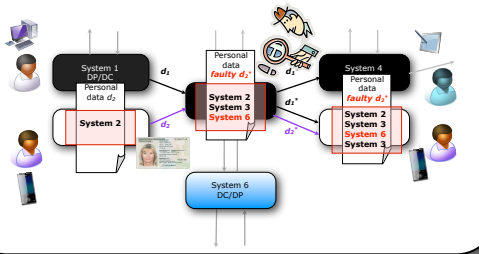
Privacy forensics

Privacy is an evidence for reliable data processing.
New German national ID card can be used as a trust anchor for privacy in social networks

Optimization



Data provenance

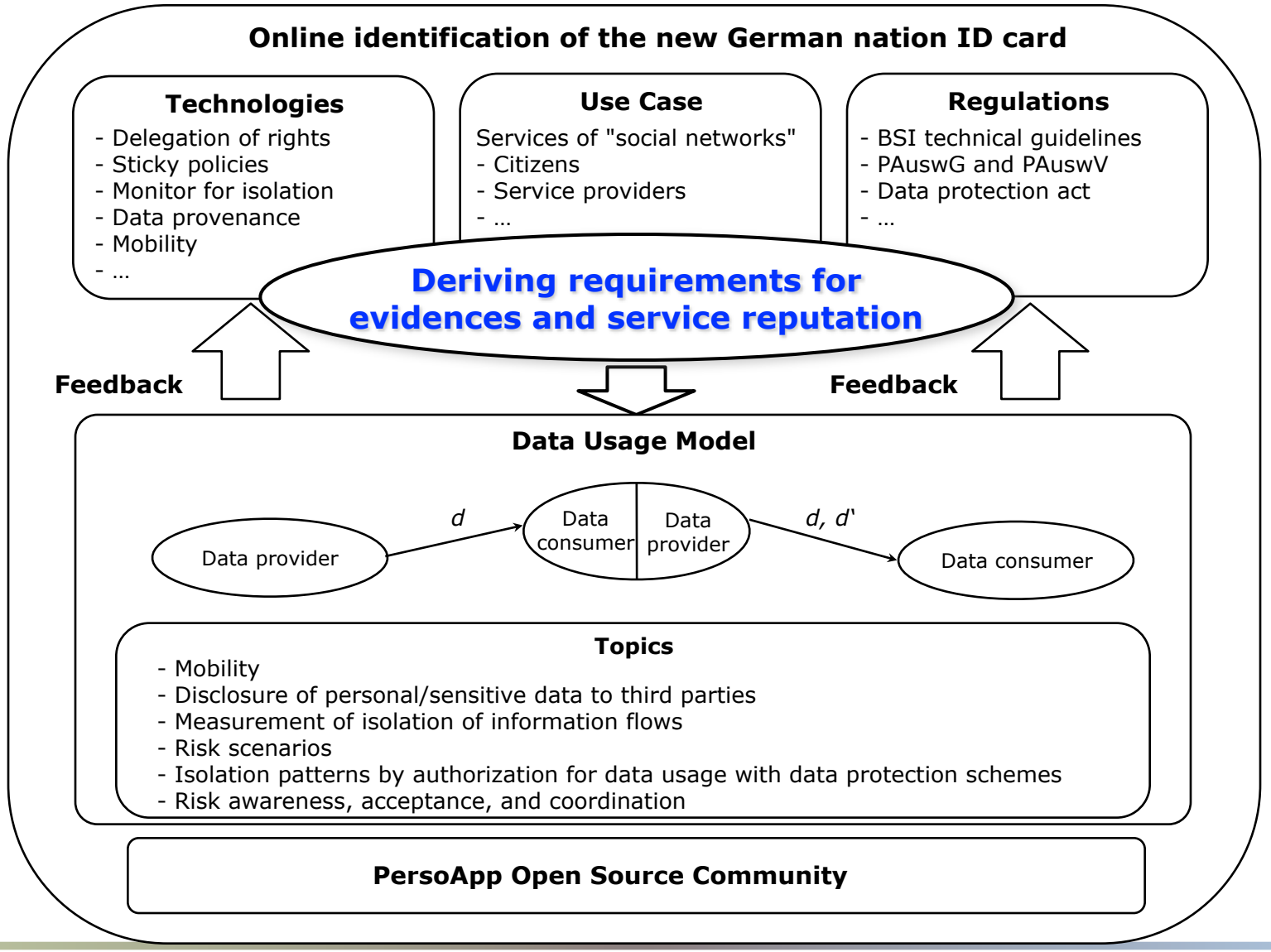


Key Messages

- PersoApp open source software library needs to be migrated to mobility to support Web 2.0 and further
- Transparency by data provenance to detect misuse of identity, since misuse cannot be completely prevented
- Privacy control with non-linkable delegation of rights based on the new German national ID card to detect misuse of identity and preserve privacy
- Privacy forensics to decide on liability of misuse of identity, since misuse can be malicious or originate from a hidden dependency

III. PersoApp: Call for Participation

Requirements for security and privacy in "social networks"



Milestones

M1 (PM7, October 2013): Major Release A1 („Publication“)

- Technical infrastructure and services
- Pre-release and open source software library Major Release A1 available
- Implementation of PersoApp processes

M2 (PM19, October 2014): Major Release A3 („Initial acquisition“)

- Publication of Major Release A3 for one use case
- Validated requirements for this use case

M3 (PM31, October 2015): Major Release A5 („Adaption“)

- Publication of Major Release A5 for another use case
- Validated requirements for this other use case

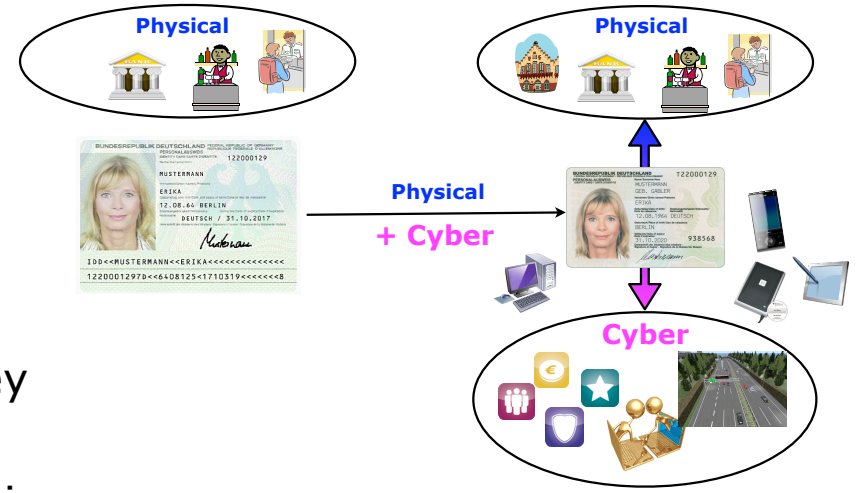
M4 (PM33, December 2015): Hand-over to the Community („Transfer“)

- Transfer event (technology transfer)
- Guideline for secure and user-friendly Internet applications with the online identification of the new German national ID card

Call for Apps

eID client for social networks supporting

- Identity control
- Privacy control
- Privacy forensics



We offer

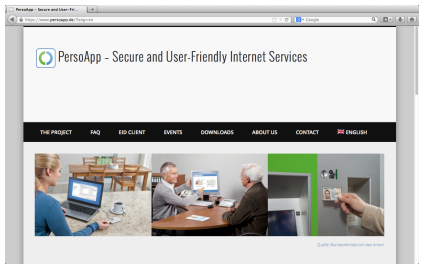
- User-oriented requirement identification by survey
- Development of use case in particular for Apps
- Open source software library for online identification
- Integration of extensions by feature requests
- Guidelines for integrating and evaluating PersoApp software library in Apps
- Dissemination by workshops, talks, teaching, and PersoApp Internet portal

We are interested in

- Apps for, e.g., mobile participation in a social network
- Security and privacy requirements of service providers and service users

Let us know your ideas via www.persoapp.de

Cooperate via PersoApp!



Internet Portal at https://www.persoapp.de
- Forum
- Pre-Release
- Demo and test service
- Documentation
- Event calendar

Code Repository at https://persoapp.googlecode.com/
- SVN repository
- Issue tracker

E-Mail Listings
- Contact: persoapp@trust.cased.de
- Project leaders: persoapp-projects@trust.cased.de
- Software developers: persoapp-devel@trust.cased.de
- Project members: persoapp-broadcast@trust.cased.de
- Steering committee: persoapp-steering@trust.cased.de
- Advisory board: persoapp-advisory@trust.cased.de

Twitter at https://www.twitter.com/persoapp
- Publication of news and interaction about PersoApp

Questions

1. Which risks would you accept due to non-authentic data/non-availability of data?

2. What kind of risks on your data would you accept to benefit from social networks, since vulnerabilities cannot be prevented?

3. Would you accept complete transparency of your IT system to your users to support trust by deriving evidences on correct information flows?

4. Would you accept restriction of availability of data even this would lead to correct information flow in a social network?

5. If safety would become more important than privacy, would you accept loss of privacy/ control on your data?