The Art of Intervenability for Privacy Engineering

Marit Hansen
Deputy Privacy and Information Commissioner
Schleswig-Holstein, Germany

marit.hansen@datenschutzzentrum.de

Workshop "Data Protection, Privacy, and Transparency" (DPPT'15)
Hamburg, 26 May, 2015

forum <privatheit> selbstbestimmtes_leben_in_der_digitalen_welt

ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Setting of ULD

- Data Protection Authority (DPA) for both the public and private sector
- Also responsible for freedom of information

Schleswig-Holstein	
State of Germany	
Flag / Coat of arms	
Coordinates: 54°28'12"N 9°30'50"E	
Country	Germany
Capital	Kiel
Government	
• Minister-President	Torsten Albig (SPD)
• Governing parties	SPD / Greens / SSW
• Votes in Bundesrat	4 (of 69)
Area	
• Total	15,763.18 km² (6,086.20 sq mi)
Population (2013-12-31)[1]	
• Total	2,815,955
• Density	180/km² (460/sq mi)

Source: en.wikipedia.org/wiki/Schleswig-Holstein

Source: www.maps-for-free.com

Home

Date: 26 May 2015
Co-located with: IFIPTM 2015 (http://s.ifiptm.org/conf2015)
Venue: University of Hamburg, Hamburg, Germany.

Overview

The protection of personal data and users' privacy is a major concern especially with technology advances that make the data accessible from anywhere. Research often focuses on the security of data and the prevention of data breaches. However, privacy and data protection extends beyond security mechanisms and links to several other concerns that relate not only to technological aspects but also societal and regulatory aspects that can affect greatly how we protect our data and maintain user privacy in the process. One major concern is lack of transparency on data protection measures taken by service providers and how these handle customer and consumer data. This affects consumers' trust for new technologies (e.g. cloud eco-system). Another concern comes from the recent Snowden revelations regarding state access to data held by private enterprises without the knowledge of those whose data it concerned (PRISM, TEMPORA). In all, a pressing question is how transparent information processing actually is, especially, when it comes to processing of personal data in complex environments, like cloud ecosystems. Companies need more than ever to prove to businesses and consumers how they handle their confidential and personal data. Transparency and accountability are gaining attention as a result.

Motivation for this talk

From the workshop description:

- "… Data Protection, Privacy, and Transparency …"
- "… Accountability …"
- Going hand in hand:

  Intervenability

ULD www.datenschutzzentrum.de

Overview of this talk

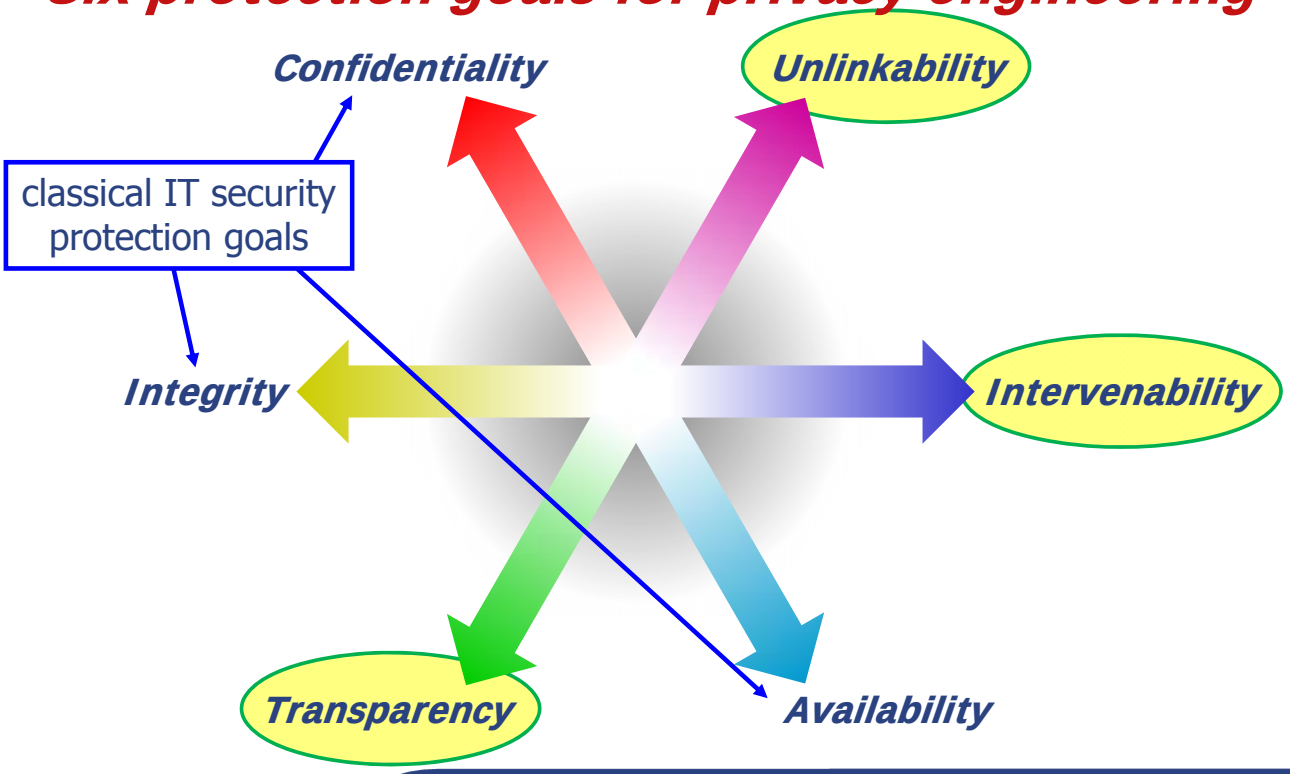
- Defining intervenability
  … as one protection goal for privacy engineering
- The roots of intervenability
- Related concepts
- How to implement intervenability
- Conclusion

DEFINING INTERVENABILITY

Defining intervenability (I)

- Intervenability: the possibility to intervene
  - Who?
  - Where?
  - When?
  - How?
- One of the six protection goals for privacy engineering

Six protection goals for privacy engineering




Protection Goals for Privacy Engineering

Protection goal "unlinkability"

The protection goal of

Unlinkability

is defined as the property that privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context.

Reference: Hansen/Jensen/Rost: Protection Goals for Privacy Engineering, Proc. 1st International Workshop on Privacy Engineering, IEEE, 2015


Protection Goals for Privacy Engineering

Protection goal "transparency"

The protection goal of

Transparency

is defined as the property that
all privacy-relevant data processing
– including the legal, technical,
and organisational setting –
can be understood and reconstructed at any time.

Reference: Hansen/Jensen/Rost: Protection Goals for Privacy Engineering, Proc. 1st International Workshop on Privacy Engineering, IEEE, 2015


Protection Goals for Privacy Engineering

Protection goal "intervenability"

The protection goal of

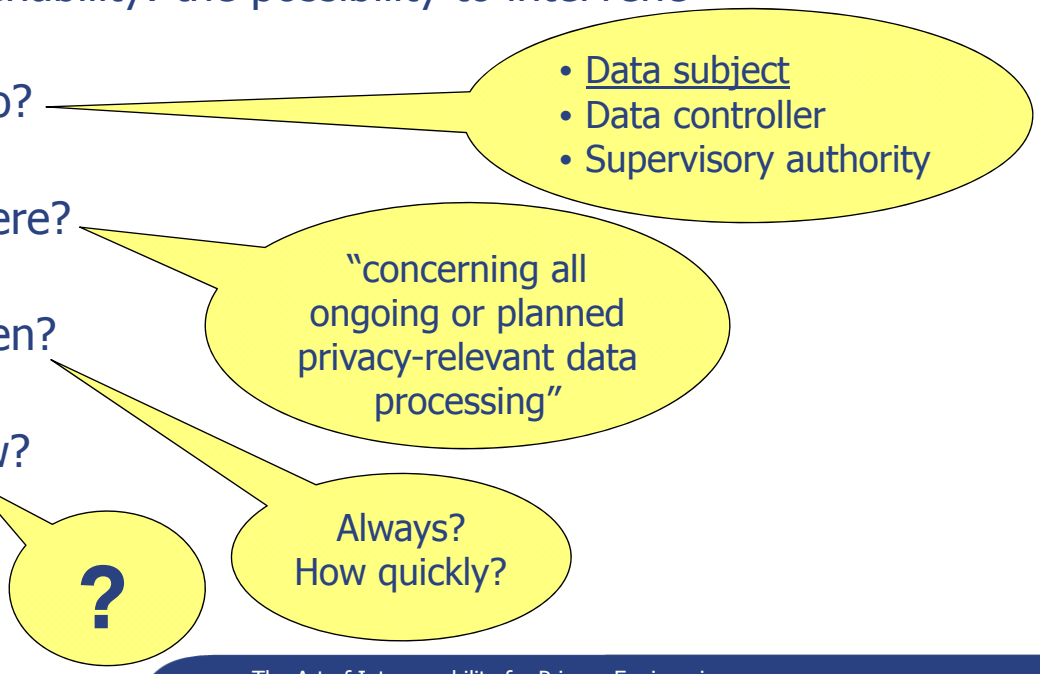
Intervenability

is defined as the property that
intervention is possible concerning all
ongoing or planned privacy-relevant
data processing.

Reference: Hansen/Jensen/Rost: Protection Goals for Privacy Engineering, Proc. 1st International Workshop on Privacy Engineering, IEEE, 2015

Defining intervenability (II)

- Intervenability: the possibility to intervene
  - Who?
  - Where?
  - When?
  - How?



THE ROOTS OF INTERVENABILITY

Intervenability as a requirement of democratic societies

- Precondition for a free & democratic communication order: the self-determined development of the individual

- "Rechtsstaat" (related to Rule of Law):
  "In a *Rechtsstaat* the citizens share legally based civil liberties and can use the courts. A country cannot be a liberal democracy without being a *Rechtsstaat*."

  https://en.wikipedia.org/wiki/Rechtsstaat

- The democratic constitutional state relies on the participation of all citizens;
  its legitimacy is based on respecting each person's individual liberty.

Right to informational self-determination

- Principle derived from the German Constitution by the German Federal Constitutional Court, 1983

- Capacity of the individual to determine in principle the disclosure and use of his/her personal data

- The data subject is to maintain control of his/her own data

Rights of EU citizens

- Voting:
  - Right of EU citizens to participate in municipal elections
  - Right of EU citizens to participate in European elections
- The right to petition the European Parliament
- The right to complain to the European Ombudsman
- Linguistic rights: the right to apply to the EU institutions in one of the official languages and to receive a reply in that same language

European Data Protection Principles

For personal data:

- Lawfulness, e.g. statutory provision or consent
- Purpose limitation
- Necessity
- Transparency
- Data subject rights
- Data security
- Accountability

Intervenability for data subjects + data controllers

*) EU Data Protection Directive 95/46/EC

Intervenability: data subject rights

Right of access (Art. 12 EU DPD*):
The right to obtain
from the controller:

- Personal data undergoing processing

As appropriate:

- Rectification
- Erasure
- Blocking

Article 12

Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

— confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

— communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

— knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

www.datenschutzzentrum.de

Intervenability: right to object

The data subject's right to object
(Art. 14 EU DPD):

- If the data controller bases the processing on "legitimate interests" (e.g. Art. 7 (f))

- Among others: direct marketing

SECTION VII

THE DATA SUBJECT'S RIGHT TO OBJECT

Article 14

The data subject's right to object

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

The Art of Intervenability for Privacy Engineering

Intervenability: automated individual decisions

Automated individual decisions (Art. 15 EU DPD):

Not allowed; exception possible if there are

"suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view"

Article 15

Automated individual decisions

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

Intervenability: giving and withdrawing consent

- "'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" (Art. 2 (h) EU DPD)

- Clarification by Art. 29 WP:
  "The notion of control is also linked to the fact that the data subject should be able to withdraw his consent. Withdrawal is not retroactive, but it should, as a principle, prevent any further processing of the individual's data by the controller."

Reference: Art. 29 WP: Opinion 15/2011 on the definition of consent, WP 187

Intervenability: lodge claims

Art. 28 EU DPD:

any person can lodge claims to the supervisory authority

Article 28

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

Intervenability: supervisory authority rights

Article 28

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

— investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

— effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

— the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

Article 17

Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

— the processor shall act only on instructions from the controller,

— the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

Data controllers' obligations

Security of processing
(Art. 17 EU DPD):

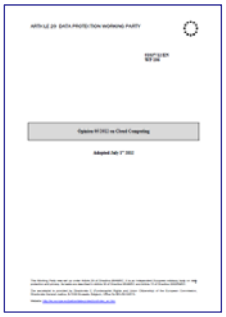
- "Appropriate technical and organizational measures"
- "choose a processor providing sufficient guarantees"
- "the processor shall act only on instructions from the controller"

Data controllers' obligations: cloud computing

- The cloud client must verify that the cloud provider does not impose technical and organisational obstacles to data subjects' rights

⇒ Contract between client and provider (including any subcontractor)

- The cloud client should check whether and how the provider guarantees the portability of data and services prior to ordering a cloud service.



Reference: Art. 29 WP: Opinion 05/2012 on Cloud Computing, WP 196

Intervenability in the General Data Protection Regulation

- Far more elaborated
- E.g. "withdrawal of consent", "effectiveness" for exercising one's rights

- Idea of data portability (for data subjects): probably gone

Amendment 113 Proposal for a regulation Article 18	
Right to Data Portability	*deleted*
1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.	
2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.	
3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	

ULD www.datenschutzzentrum.de

RELATED CONCEPTS

The Art of Intervenability for Privacy Engineering

Related concept: (Notice &) Choice

- Based on Fair Information Practice Principles (FIPPs)
- Sind the mid-1990s encouraged by the Federal Trade Commission (FTC)

- "Simplified Choice for Businesses and Consumers - companies should give consumers the option to decide what information is shared about them, and with whom. This should include a Do-Not-Track mechanism that would provide a simple, easy way for consumers to control the tracking of their online activities."

FTC Report "Protecting Consumers Privacy in an Era of Rapid Change", 2012

ULD www.datenschutzzentrum.de

Related concept: (Notice &) Choice

- Hasn't worked well in reality:
  - Lack of transparency
  - Choices are usually very limited (and at the same time maybe too complex)
  - A "take it or leave it" choice is usually no appropriate intervention
- Not sufficient

Side remark: intervenability ↔ transparency

- At best, intervenability bases on sufficient transparency
- But: lack of transparency may be a reason to intervene
- At least transparency about possibilities to intervene required
  - Potentially outside the IT system
  - If not provided by the data controller: legal options
  - Proof of point at issue required

ULD www.datenschutzzentrum.de

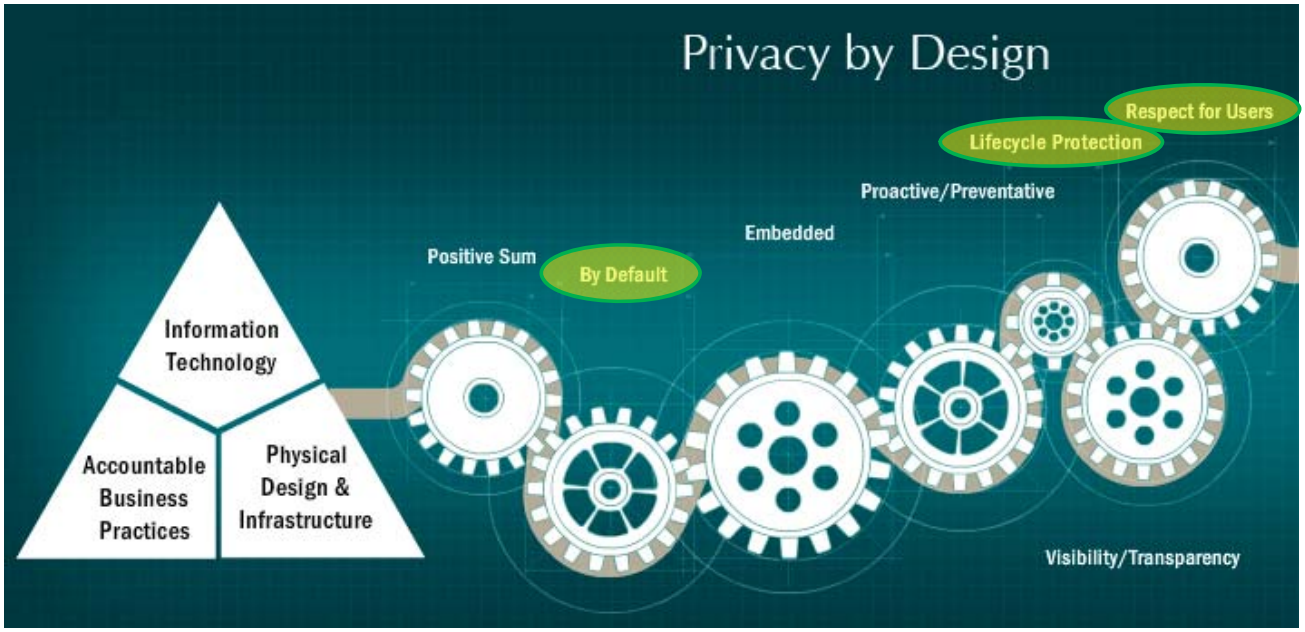
Intervenability and Multilateral Security

Concept for taking into account the interests of all stakeholders:

- All parties involved specify and express their individual interests and security goals
- Potential conflicts are recognised and negotiated
- Results are enforced

- Objectives:
  - Minimising necessary trust (instead: trustworthiness)
  - Empowering users (who are usually in a weak position)

Intervenability and Privacy by Design



http://privacybydesign.ca/

Intervenability and Privacy Engineering Research

- Intervenability is not prominent in privacy engineering literature
- Reasons for that:
  - Hard to formalise and to measure
  - Compared with data minimisation research far less proposed techniques and technologies
  - Can often not be solved within the IT system alone
  - Needs a running system with clear responsibilities (operator, users) – not on prototype level
  - Not one fixed solution, but process-oriented, taking into account the full lifecycle of system evolution

HOW TO IMPLEMENT INTERVENABILITY

Preparation for intervenability

- For individuals:
  - Control own disclosure of data if possible
- For data controllers:
  - Control own processing of data, in particular when being dependent on others
  - Take technical, organisational and legal measures
  - Plan for interventions:
    - Incident management, change management
  - E.g.: establish processes for data subject's rights

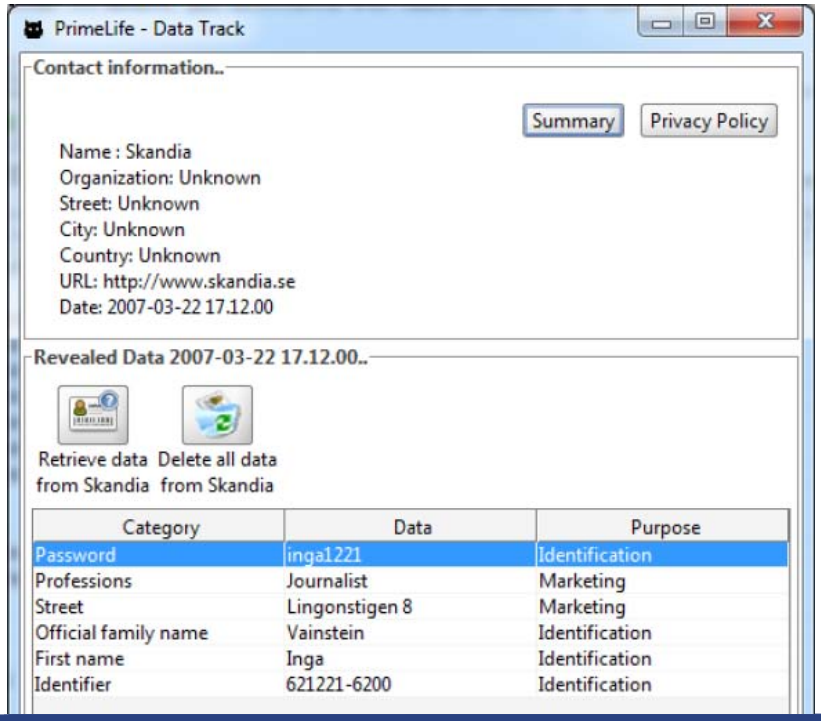
Intervenability technique: support for exercising data subject rights

On the basis of the "Data Track" (user-side history function) users can more easily get

- Access

and request

- Rectification
- Erasure

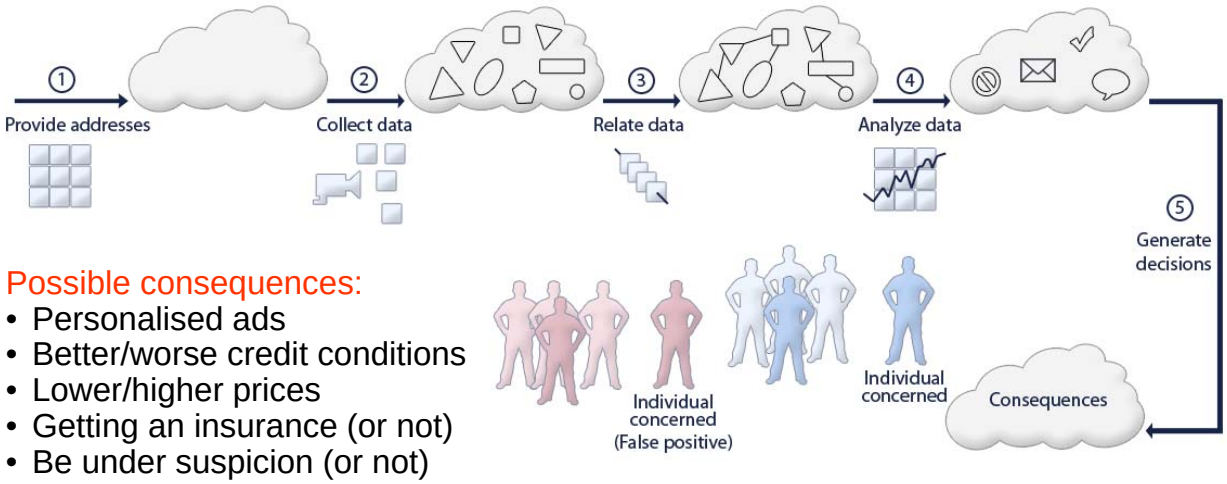


Reference: PrimeLife project (D4.2.2, D2.2, PrimeLife Book)

Difficult problem: data collection

Data flow model: enriching information

At each step, different parties (with different responsibilities) can be involved.



Possible consequences:

- Personalised ads
- Better/worse credit conditions
- Lower/higher prices
- Getting an insurance (or not)
- Be under suspicion (or not)
- …

How can individuals intervene?

Reference: Marit Hansen: Linkage Control – Integrating the Essence of Privacy Protection into IMS, Proc. eChallenges 2008, 1585-1592

Intervenability technique: help desk

- Helpful: single point of contact
  - Even in complex settings with many stakeholders involved
  - Important: accessibility
- But avoid: single point of data collection

Source: tsaiproject

Source: Mark Hillary

- Authentication:
  - Authentication of individual needed? How?
  - Authentication of help desk: necessary

Intervenability technique: stop processes

Source: Jeffrey

Scenario: Ambient Assisted Living

- Homes equipped with sensors and video cameras (even bed sensors)
- Monitoring service will react in case of an emergency, e.g. if a person tumbles and doesn't get up again
- Implementation does not allow deactivation of sensors and cameras because of liability reasons
- *Privacy of the inhabitant?*
  Privacy of guests or care takers?

- Intervenability would require possibility to temporarily deactivate sensors/cameras – but this would mean a shift of liability

Intervenability technique: choice of (de-)activation

 Source: Playing Futures: Applied Nomadology

Intervenability technique: permanent deactivation

Source: Antonio Campos Domínguez

Intervenability technique: self-defence against face recognition

BBC

22 January 2013 Last updated at 12:50 GMT

'Privacy visor blocks facial recognition software'

A pair of glasses dubbed a "privacy visor" has been developed to thwart hidden cameras using facial-recognition software.

The prototype spectacles have been designed by scientists at Tokyo's National Institute of Informatics.

The glasses are equipped with a near-infrared light source, which confuses the software without affecting vision.

Law enforcers, shops and social networks are increasingly using facial-recognition software.

Prof Isao Echizen said: "As a result of developments in facial recognition technology in Google images, Facebook et cetera and the popularisation of portable terminals that append photos with photographic information [geotags]... essential measures for preventing the invasion of privacy caused by photographs taken in secret and unintentional capture in camera images is now required."

The glasses are not necessarily high fashion

Related Stories

Watchdog fears HD CCTV backlash

Project "Privacy Visor": http://research.nii.ac.jp/~iechizen/official/research-e.html#research2c

http://www.bbc.com/news/technology-21143017

Intervenability technique: one-time activation with break glass

Source: Axel Schwenke

- Break-glass procedures known in healthcare: facilitation of a privileged access in emergency cases
- Logging of privileged access
- This is the exception, not the rule!
- Related: manual override of automated decisions

Intervenability: employ the legal system ...

- Lodge a claim
- Submit a dispute for arbitration
- Go to court

- Helpful: proof concerning the point at issue

⇒ engineering task to provide all parties involved with evidence

... or the fourth estate: press & media

- Publish in blogs or in open letters
- Involve journalists

Source: www.stockmonkeys.com

Intervenability: implementation techniques for controllers

- Process definitions: change management etc. (including changing components, subcontractors, …)
- Configuration menu: activation / deactivation
- Support for exercising rights to access, rectification, erasure, object, …
- Help desks
- Stop button for processes
- Break-glass / alert procedures
- Manual override of automated decisions
- Internal and external control bodies that request changes (employee associations, supervisory authorities, …)

The more planning and support, the less need for the data subject's self-defence

Challenge: intervenability and usability

Source: TeppoTK

Source: free photos

Conclusion

- Intervenability: important protection goal for system design
  - Political systems
  - Legal systems
  - IT systems
- Different kinds of intervenability, depending on perspective: data subject, data controller, supervisory authority, …
- Intervenability techniques go beyond IT solutions; however, IT design influences possibilities for intervention

Thank you for your attention!

Marit Hansen
marit.hansen@datenschutzzentrum.de