THE PRIVACY REQUIREMENTS DILEMMA - NOW THE END-USER CAN SPECIFY PRIVACY REQUIREMENTS - BUT DOES (S)HE REALLY WANT TO?

Jörg Dörr
(presenting work of Manuel Rudolph)

May 2017
The Fraunhofer-Gesellschaft undertakes applied research of direct utility to private and public enterprise and of wide benefit to society.

Nearly 24,000 staff

66 institutes and research units

Financial Volume

Contract Research

2014

€2 billion

€1.7 billion

Major infrastructure capital expenditure and defense research

Almost 30% is contributed by German federal and Länder governments.

More than 70% is derived from contracts with industry and from publicly financed research projects,
Fraunhofer IESE
The research institution for software and systems engineering methods

- Founded in 1996, headquartered in Kaiserslautern
- approx. 240 employees
- Our solutions can be scaled flexibly and are suitable for companies of any size

Our most important business areas:
- Automotive and Transportation Systems
- Automation and Plant Engineering
- Health Care
- Information Systems
- Energy Management
- E-Government
Our Competencies / Research Areas

SOFTWARE-ENABLED INNOVATIONS

SCALABLE SYSTEMS ENGINEERING

Processes Architecture Requirements

GUARANTEED QUALITY

Safety Security UX

ES/CPS Smart Ecosystems IS/Mobile

SOFTWARE-ENABLED INNOVATIONS
Research Areas of Today’s Talk

SCALABLE SYSTEMS ENGINEERING
- Processes
- Architecture
- Requirements

GUARANTEED QUALITY
- Safety
- Security
- UX

SOFTWARE-ENABLED INNOVATIONS
- ES/CPS
- Smart Ecosystems
- IS/Mobile
BUSINESS TODAY IS ALL ABOUT DATA
SENSITIVE DATA – FROM PRIVATE PERSON AND THE COMPANIES

Business data
Process data
Product data

Intellectual property

Private data
Employee data
Contractor data
Personal data
What happens after data is released?

Legal Consequences

Reputation damage

Financial Losses

Legal Consequences

Reputation damage

Financial Losses

Usage Control
Data Leakage and Misuse
CONSEQUENCES: GO BIG OR GO HOME!

- Option 1: Companies respond with strong data protection mechanisms
  - infrastructure protection,
  - data leakage prevention,
  - organizational regulations (no USB sticks, no cloud storage)
  ➔ „Fort Knox“ Solution (black thinking)

- Option 2: Companies share their data and believe: shared data = lost data
  - nearly no data protection,
  - open data exchange,
  - careless data use
  ➔ „Open Data“ Solution (white thinking)
WHY NOT GOING A MIDDLE WAY?

- If companies want to use data as production factor, they have to …
  - control data usage,
  - protect data value, and
  - prevent data misuse.

- Sharing of data does not exclude the protection of the data value

- Conceptual Solution (supported by technology): **Data Usage Control**

**Share data, but keep control!**
Access control is not enough!

Usage control – a generalization of access control

- Fine-grained policies specify how data is handled after access has been granted

- Allows the user to keep control over his/her data
IND²UCE FRAMEWORK
INTEGRATED DISTRIBUTED DATA USAGE CONTROL ENFORCEMENT

- IND²UCE provides theoretical concepts and technological components for implementing data usage control
- EARTO innovation prize winner 2014

© Fraunhofer IESE
**POLICY SPECIFICATION**

- **Security policies** ...
  - describe *security behavior* of a software system demanded by a stakeholder
  - can be specified flexibly changed during operation of system or software
  - are specified by various stakeholders depending on the scenario

**Examples**

- Privacy – Facebook Privacy Settings: “Only friends may see my profile”
- Data Usage Control – Business to Customer: “When business documents are sent to customers, they must be deleted after opening them 3 times or latest after 14 days”

- Policy Administration Points (PAPs) are specification tools for security policies
Companies want their end users to specify their own security demands

EU-GDPR demands that users give consent to data usage (data sovereignty)

But companies don’t know how to enable non-experts to specify own security policies

User does not understand policies

Policies become too complex to be handled by the end user

Effects of policies on the target system are not transparent to the end user

(Customer statements from e.g., Bosch, Finanz Informatik, camLine, TMF e.V.)

→ Users need appropriate security policy specification interfaces (PAP)
POLICY AUTHOR TYPES ➔ SPECIFICATION PARADIGMS

- **Assumption**: Different specification paradigms are suitable for different policy author types.

- Policy author types differ in their level of security and domain knowledge.

- **Assumption**: Suitable specification paradigm → Higher acceptance and higher correctness rate of specified policies.

- **Research question**: How can policy author types be characterized?

- **Goal**: Acceptance by policy author and correctness of specified policies.

- **Predefined Security Policies**: No specification
- **Predefined Security Policies**: On-off Button
- **Selection from List of Predefined Policies**
- **Specification Wizard**
- **Security Policy Templates**
- **IND²UCE Policy Editor**

© Fraunhofer IESE
Security policies are technical and affect various elements in the security and privacy domain.

**Current Focus on Dupree’s Privacy Personas (seem to match best)**
Dupree identified five personas that behave differently when it comes to security practices.

- Key distinction factors
  - Knowledge of privacy and security
  - Motivation

- Each persona has between 9 and 13 characteristic traits

  - e.g., Lazy Expert: “Chooses convenience over security”, “Chooses being social over privacy” and “Write down passwords securely”

- Policy author to persona matching using persona descriptions with traits
Now **end-users are able (in principle) to specify** their security and privacy policies (requirements) at runtime.

An open question is **how to provide the best interface** (policy authoring point) to the different types of end-users.

We are open to a controversial discussion and hearing your opinion: **what are the key influencing factors** from your point of view?

- Domain Knowledge
- Security/Privacy Knowledge
- Bad Experience
- Personality
- Business / Private Setting
- ...