Dissertations- und Forschungsprojekt

EMIDD – Einwilligungsmanagement im Internet der Dinge

Max-R. Ulbricht | ISE@TUB | Workshop „Privacy, Datenschutz & Surveillance“, HIIG
Agenda

Motivation
Technical Infrastructure
Open legal Questions
OpenSense

A participatory open sensor data platform.

by ISE
Legal Requirements

Article 4 (GDPR)

Definitions

(11) ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her; [...]
Consent for:

1. Storing Data
2. Disclose aggregates for statistical reasons
Need Realtime Data for personal weather forecast.

Realtime Data for all sensors near „Ostbahnhof“

From Frank & Friends?

Nope!
Problem: purpose limitation

Article 5 (GDPR)
Principles relating to processing of personal data

1. Personal data shall be:

   [...] [\ldots]

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes[\ldots]
Problem: purpose limitation

Ergo:

For every „new“ processing purpose without existing consent the institution that wants to process the data has to request consent of the respective data subject before the processing.

→ Leads to Broad Consent
Problem: purpose limitation

„[...] classical mechanisms used to obtain individuals’ consent may be difficult to apply in the IoT [...]}. In practice, today, it seems that sensor devices are usually designed neither to provide information by themselves nor to provide a valid mechanism for getting the individual’s consent.“

ARTICLE 29 DATA PROTECTION WORKING PARTY
„Opinion 8/2014 on the on Recent Developments on the Internet of Things“
Problem: purpose limitation

„Yet, new ways of obtaining the user’s valid consent should be considered by IoT stakeholders, including by implementing consent mechanisms through the devices themselves. Specific examples, like Privacy Proxies and Sticky Policies, are mentioned [...]。“
Sticky Policies

Privacy Preferences stucked on Encrypted Data

Data Holder

+ information about respective TA

Decryption Key

Trusted Authority
Sticky Policies

Advantages:
• No access without interaction with a Trusted Authority (TA) possible
• TA can log all accesses

Drawbacks:
• Strong dependance on interaction with a third institution (TA)
• Additional steps required during data collection (encryption of the data set, transferring keys to TA, ...)
• No prevention / detection of violations of the codified rules after access is granted
Privacy Proxy?

„ A way to offer a data subject real control on how data must be processed [...] by being able to express preferences, including getting and revoking consent and purpose limitation choices [...]. [...] data requests are confronted with predefined policies governing access to data [...] . By defining sensor and policy pairs, third parties requests for collection or access to sensor data would be authorised, limited or simply rejected. “

ARTICLE 29 DATA PROTECTION WORKING PARTY
„Opinion 8/2014 on the on Recent Developments on the Internet of Things“
"We are engineers, we build systems"
S. Tai, ISE-Motto

How would I build a Privacy Proxy?
“ [...] third parties requests for [...] access to sensor data would be authorised, limited or simply rejected [...]”

“ [...] predefined policies governing access to data [...]. By defining sensor and policy pairs [...]”

“ [...] express preferences, including getting and revoking consent and purpose limitation choices [...]”
Data Holder

Hippocratic Access Model

• Data Upload
• Preferences

User Interaction

Policy Proxy

Policy Provider

External Application

External Application

External Application

Data Holder

User Interaction

Policy Provider

External Application

External Application

External Application
Data Holder

• Data Upload
• Preferences

User Interaction

Policy Proxy

Policy Provider

Data Holder

PIP

PDP

PEP

•

external Application

external Application

external Application

17
Scenario: Fitness Data

User-System

Policy Provider
- PIP

Policy Proxy
- PDP
- PEP

User Interaction
- Data Upload
- Preferences

PAP

Service-Provider-System

Data Holder
Scenario: Participatory Sensing

User-System

User Interaction
- Data Upload
- Preferences

Policy Proxy

Policy Provider

Service-Provider-System

Policy Proxy

Policy Provider

Data Holder

(opensense.network)
Privacy Preferences

This data can be processed for purposes of:

• Research
  o General
  o Specific
    o Urban development
    o Medical research
    o ...
  • Demographic investigations
    o General
    o Specific
    o ...

„Pre“-consent for categories of purposes and potential utilizers
System (of technical artefacts) that enables Informational Self-Determination a lá Westin (1967, p. 7):

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

→ Is this system legally valid?
(wrt. GDPR, ...
Open legal Questions
Research Question

Can consent be given to generalized categories of possible utilizers and future purposes?
Ask a lawyer?

ICO guidance for consent in the GDPR
Posted on March 2, 2017

By Jo Pedder, Interim Head of Policy and Engagement.

Back in January I wrote about our plans for GDPR guidance in 2017 and our commitment to help organisations improve their practices and prepare for the GDPR.
Ask a lawyer?

What information should you include?

Consent must be *specific and informed*. You must as a minimum include:

- the name of your organisation and the names of any third parties who will rely on the consent – consent for categories of third-party organisations will not be specific enough;
- why you want the data (the purposes of the processing);
- what you will do with the data (the processing activities); and
Legally valid (?) Workaround

Idea:
“Split” Consent...

<table>
<thead>
<tr>
<th>Traditional Consent</th>
<th>Data Processing Contract</th>
</tr>
</thead>
<tbody>
<tr>
<td>“I give your organisation my consent to the processing of personal data relating to my person for the purpose X”</td>
<td>“On my behalf release my personal data stored by you to following categories of third-party organisations for data processing for purposes Y, Z, G under following conditions: ...”</td>
</tr>
</tbody>
</table>
Kontakt

Max-R. Ulbricht
Technische Universität Berlin
Information Systems Engineering
mu@ise.tu-berlin.de
@maroulb
BackUp
Data Holder

Hippocratic Access Model

Policy Proxy

User Interaction
- Data Upload
- Policy Specification

Policy Provider

External Application

External Application

External Application

Data Holder
Details

Technologies:
- Python
- Flask (_V0.1 nameko)
- pymongo
- MongoDB

Functionalities
- GET: take id, query DB, return policy
- POST: take policy, insert into DB
Details

Technologies:

• Python
• Flask (\_V0.1 nameko)
• SQLite

Functionalities

• GET: take id, ask "policy provider" for policy, get User Data from DB, adapt policy, return modified User Data
• POST: take data, insert into DB
Details

Technologies:
- Python
- Flask
- Jinja2

Functionalities
- GET: take Username, ask “Policy Proxy” for User Data, get User Data and show it
- POST: ???

Question: How to obtain legally valid Consent?
Inspiration: XACML (OASIS standard)
Key Differences

oasis XACML-PEP:

• Pure Access Control
  ➢ Binary Decision:
    ▪ Permit
    ▪ Deny
    ▪ Deny 2: Not Applicable (no policy or rule found)
    ▪ Deny 3: Indeterminate (some error occurred during evaluation)

• Extensible with (non-standard, unspecified) optional obligations (non-enforceable by PEP)

CoMa-PEP:

• Not (only) Access Control:
  ➢ Differentiated Decision:
    ▪ Permit
    ▪ Deny
    ▪ Aggregated Values (different grades of aggregates)
    ▪ Selected Values (subset)

⇒ Enforceable Obligations

• (reduced Message Roundtrips)
What’s next?

Comparison of CoMa Architectures:

1. Centralized Approach → Platform
2. Decentralized Approach → (Micro-) Services
3. Peer 2 Peer Approach → Policy Ledger
Data Holder

Hippocratic Access Model

User Interaction
- Data Upload
- Policy Specification

Policy Provider

Policy Proxy

External Application

External Application

External Application
User Interaction

- Data Upload
- Policy Specification

Policy Proxy

Public Policy Ledger

Data Holder

External Application

External Application

External Application