Technical aspects vs. Innovation challenges of Enabling and Enhancing Privacy

Axel Polleres
(Thanks for their contributions to: Sabrina Kirrane, Erwin Filtz, Sushant Agarwal, Javier Fernandez,...)

http://polleres.net

Twitter: @AxelPolleres
Where I am coming from, collaborators...

- **Privacy & Sustainable Computing Lab**
- [http://www.privacylab.at/](http://www.privacylab.at/)
- Launched September 2016, launch event with various important stakeholders: technologists, standardization, activists...
- Goal: setting new standards in research, education and practice to address ethical issues in computing.

Dr. Sabrina Kirrane (Lab Director)  
Prof. Sarah Spiekermann (co-founder)  
Prof. Axel Polleres (co-founder)
Privacy in the EU: all about the upcoming GDPR, various national and European research efforts...

Draft of the regulation
7/22/2012

Revisions in the draft
3/12/2013

Discussions in the EU Council
5/19/2014

Trilogue starts
6/24/2015

EU Council finalises the chapters
8/6/2015

Trilogue agrees
12/17/2015

Comes into force
5/15/2018

Horizon 2020
European Union funding
for Research & Innovation
Main technical challenges (prioritized from our point of view)

1. Informed Consent & Policies
2. Transparency, Deletion
3. Subjectivity
4. Anonymization

Last, but not least, and for all these challenges: Protection vs. Innovation?
Consent & Policies

GDPR requirements:

<table>
<thead>
<tr>
<th>Article #</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Conditions for consent</td>
<td>Controllers should be able to demonstrate the 'freely given' consent from data subjects and should provide the right to withdraw consent any time</td>
</tr>
</tbody>
</table>

Opt-in, consent declarations
- Demonstrate consent
- Freely given
- Clearly distinguishable
- Withdraw consent at any time

Discussion:
- How to guarantee opt-in has been understood? Policy templates, “Privacy Icons”
- Research proposes that opt-out, interactive processes, and partial consent are more intuitive than opt-in by monolithic consent forms
- Giving consent online has many behavioural and UI components!
- Can I delegate consent to a personal agent?
  - How to express and execute consent policies in provable machine readable form?
  - Would that legally hold?
Transparency, Access, Rectification, Deletion

<table>
<thead>
<tr>
<th>Article #</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Transparent information, communication and modalities for the exercise of the rights of the data subject</td>
<td>To provide info related to processing in concise, transparent, intelligible and easily accessible form, using clear and plain language..</td>
</tr>
<tr>
<td>15</td>
<td>Right of access for the data subject</td>
<td>Right to access personal data which is collected and processed and to know which data is processed</td>
</tr>
<tr>
<td>16</td>
<td>Right to rectification</td>
<td>Right to ask controllers to rectify any inaccurate personal data regarding them</td>
</tr>
<tr>
<td>17</td>
<td>Right to erasure (“right to be forgotten”)</td>
<td>Right to ask controllers to delete their personal data</td>
</tr>
<tr>
<td>18</td>
<td>Right to restriction of processing</td>
<td>Right to ask controllers to restrict processing of personal data</td>
</tr>
</tbody>
</table>

Trust via Transparency
• Concise, transparent, intelligible and easily accessible information about processing
• Using clear and plain language
• Standardized icons (machine-readable)

Discussion:
• Develop agreed models to present transparency data in a standardized manner, allowing the user to access the data collected about them in an integrated manner (e.g. Linked Data, PROV, extensions...)
• Open questions in terms of deletes (e.g. feasibility of Hard deletes in cloud environments) vs. transparency demands.
• Protocols to store transparency information (*Blockchain is not the only option*)
Subjectivity

- Ambiguity/Room for interpretation in the GDPR
- e.g. conflicting(national) laws with the GDPR
- Different national interpretations

**Discussion:**
- Metrics for e.g. understandability of privacy terms
- Standardization?
- *Investigate/analyze case law*
Anonymization for Innovation?

Which K should we use for K-Anonymity? K-Anonymity is not enough! Best practices and industry strength tools needed!

The GDPR does not apply to anonymous data where the data subject is no longer identifiable.

The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.
Our current solution approach: The SPECIAL project

https://www.specialprivacy.eu/
Our current solution approach: The SPECIAL project

Objectives

- Policy management framework
  - Gives *users control* of their personal data
  - Represents *access/usage policies and legislative requirements* in a machine readable format

- Transparency and compliance framework
  - Provides information on how data is *processed* and with whom it is *shared*
  - Allows data subjects to take *corrective action*

- Scalable policy-aware Linked Data architecture
  - Build on top of the Big Data Europe (BDE) platform *scalability and elasticity mechanisms*
  - Extended BDE with *robust policy, transparency and compliance protocols*
- **Big Data Europe** scalability and elasticity
- **PrimeLife** policy languages, access control policies, release policies and data handling policies
Summary and input for discussion:

- **Technical support** for privacy should be understood as an innovation driver/asset, not an obstacle!
  - Many opportunities for tools and algorithmic support
  - E.g.
    - formalizing and reasoning about Policies + data analytics about case law (=**Rules + Data Science**)
    - **UIs, Standards**, Best Practices
    - **Linked Data** for Privacy!

- Take the enterprise view of Big Data analysis into account!
- **Harmonization** on Privacy law alone is not enough, but also on the national interpretations and conflicting laws!

- Thank you!