Privacy and Transparency
Interoperability, Standards and Vocabularies

Axel Polleres
Ben Whittam Smith
1 year ago...

Project Launch:
SPECIAL (a Scalable Policy-awareE linked data arChitecture for prIvacy, trAnsparency and comPliance)

Axel Polleres, Vienna University of Economics and Business (WU Wien)

MyData 2017, Tallinn/Helsinki
30/08/2017

Horizon 2020
European Union funding for Research & Innovation

Regulators
Legal Policies
Data & Data Driven Services
Privacy Preferences
Customers/Service Users
Use Cases for Transparency and Interoperability:

- Companies: Ensuring Regulatory Compliance for Companies
- Regulators: Checking and enforcing GDPR
- Data Subjects: Personal Data Markets: from “Data Collection” to “Data Donations”

Different roles have different use cases.
Semantics/Interoperability

- Semantics:
  - Agreed structured vocabularies for describing and interchanging **Components of Personal Data Processing**
  - Enable standardized + **automated ways to implement and monitor GDPR compliance** checking

Room for Standardisation?
- Standard Vocabularies
- Standard Architectures+Compliance checking Algorithms
Components of Personal Data Processing (not exhaustive...)

Rules/Policies
- Consent
- Regulations

Purpose

Processing

Storage

Personal Data (categories, formats)
Regulatory Compliance for Big Companies

- Many heterogeneous systems that process personal data
- Potentially many different places that store and hold consent
- How to deal with GDPR data requests at scale?
- How to prove to the regulator and to the customer that personal data has been handled in compliance to consent only?
Regulatory Compliance for Small Companies

- No resources to build their own compliance infrastructure
- How to deal with GDPR data requests at scale?
- How to prove to the regulator and to the customer that personal data has been handled in compliance to consent only?

\[ \text{P4} \subseteq \text{P2} \]
Semantic Interoperability boils down to:
- What is a common core to address these use cases?
- How do we benefit them all at the same time?

Data Privacy Controls and Vocabularies
A W3C Workshop on Privacy and Linked Data
17–18 April 2018, WU Vienna, Vienna, Austria, Europe
https://www.w3.org/2018/vocabws/report.html
Semantic Interoperability boils down to:
- What is a common core to address these use cases?
- How do we benefit them all at the same time?

Rough workshop outcome / scoping:

1. Taxonomy of regulatory privacy terms (including all GDPR terms).
2. Taxonomy for personal data.
3. Taxonomy of purposes.
4. Taxonomy of disclosure/processing.
5. Metadata (e.g. related to processing details of anonymization)
7. Taxonomy of linkage operations.
8. Taxonomies of human behavior.
Semantic Interoperability boils down to:
- What is a common core to address these use cases?
- How do we benefit them all at the same time?

→ Foundation of a W3C Community Group (25th May 2018)

→ Collect concrete **Use cases**
→ Collect **Existing Vocabularies**
→ Align **Core Vocabularies**

1. Taxonomy of regulatory privacy terms (including all GDPR terms).
2. Taxonomy for personal data.
3. Taxonomy of purposes.
4. Taxonomy of disclosure/processing.
5. Metadata (e.g. related to processing details of anonymization)
7. Taxonomy of linkage operations.
8. Taxonomies of human behavior.
Semantic Interoperability boils down to:
- What is a common core to address these use cases?
- How do we benefit them all at the same time?

⇒ Foundation of a W3C Community Group (25th May 2018)

- Collect concrete Use cases
- Collect Existing Vocabularies
- Align Core Vocabularies

⇒ We need your input!
⇒ Join DPVCG!

https://www.w3.org/community/dpvcg/wiki/Use-Cases, Requirements, Vocabularies

Vocabularies [edit]
- CDMM Consent Ontology
- COEL
- Data Protection Ontology by Bartolini et. al
- GDPRov
- GDPRExt
- IEEE 7012
- ODRL
- P3P
- P-Plan
- Privacy Preference Ontology
- PROV-O
- SPECIAL Usage Policy
- SPECIAL Policy Log
Starting Point: Use Cases/Vocabularies from SPECIAL

Ben Whittam Smith, Axel Polleres

MyData2018, Helsinki
Three Distinct Use Cases:

**THOMSON REUTERS**
Know-Your-Customer services for the banking industry

**proximus**
Recommendation engine for subscribers

**T**
Service quality monitoring
One Compliance Solution:

Processing requires **PERMISSIONING**

Permissions must be compliant with the **GDPR**

Permissions must be compliant with **Consent**

i.e., **COMPLIANCE** is a logical operation
KYC Permissions (AKA Processing Steps)

1. To take documentary evidence of identity and generate identity attributes

2. To store identity attributes

3. To screen against mandated datasets

4. To validate screening results

5. To store, share, and generate risk flags from validated results

6. To share and store risk assessment
If we can show completeness and correctness of execution then we can decentralise the holding of PI

Access is controlled by Smart Contracts
What to Standardise:

- Core Logic
- Core Vocabulary
- Compliance Services

Against What Criteria:

- Completeness and Correctness: \( \subseteq \)
- Market adoption
SPECIAL’s view on Core Interoperability Components:

Rules/Policies: SPECIAL Usage Policy Language (SPL)  
• Rules/Policies: SPECIAL Usage Policy Language (SPL)  
• Purposes: W3C P3P  
• Processing: W3C ODRL  
• Storage: W3C P3P, (OASIS COEL?)  
• Data: W3C P3P, (OASIS COEL?)  
• Recipients: W3C P3P  

SPECIAL namespaces:

@prefix spl: <http://www.specialprivacy.eu/langs/usage-policy#>.  
@prefix svpu: <http://www.specialprivacy.eu/vocabs/purposes#>.  
@prefix svpr: <http://www.specialprivacy.eu/vocabs/processing#>.  
@prefix svd: <http://www.specialprivacy.eu/vocabs/data#>.  
@prefix svr: <http://www.specialprivacy.eu/vocabs/recipients#>.  
@prefix splog: <http://www.specialprivacy.eu/langs/splog#>.  
...
The data controller will collect financial and judicial information from public sources and analyse it for “know your customer” purposes. This information will be stored on the controller’s servers and released to specific third parties.
Use Cases/Vocabularies from SPECIAL: Example (OWL)

```
ObjectIntersectionOf(

  ObjectSomeValueFrom( spl:hasData
    ObjectUnionOf( svd:Financial svd:Judicial ))

  ObjectSomeValueFrom( spl:hasProcessing
    ObjectUnionOf( tr:Collect-public svpr:Analyze ))

  ObjectSomeValueFrom( spl:hasPurpose tr:KYC )

  ObjectSomeValueFrom( spl:hasStorage
    ObjectIntersectionOf(
      ObjectSomeValueFrom(spl:hasLocation spl:ControllerServers)
      DatatypeRestriction( xsd:integer xsd:mininclusive "0"^^xsd:integer ))

  ObjectSomeValueFrom( spl:hasRecipient svr:AnyRecipient )
)
```
Call for Action: Join DPVCG!

• More use cases matter!
• Existing efforts for interoperability/vocabularies matter!

Joining is easy!
→ The group is Open to everyone!
→ Just create a W3C account

https://www.w3.org/community/dpvcg/

• Maybe discuss in more detail in one of the upcoming Open Space sessions...