The SPECIAL Policy Log Vocabulary
A vocabulary for privacy-aware logs, transparency and compliance

Javier D. Fernández, Piero Bonatti, Wouter Dullaert, Sabrina Kirrane, Uros Milosevic, Axel Polleres

W3C Workshop on Privacy and Linked Data
18/04/2018
SPECIAL Overview

Aims

Data & Data Driven Services

Regulators

Legal Policies

Privacy Preferences

Contracts/Terms of use

Customers/Service Users

Companies/Service Providers

Privacy Preferences

Regulators

Legal Policies

Contracts/Terms of use

Customers/Service Users

Companies/Service Providers
SPECIAL Overview
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**
Privacy policy formalization

- Record usage policies
- SPECIAL is releasing the SPECIAL policy language
  - Based on OWL EL

“Heart rate and location data are collected and analysed to create a user profile for the purpose of issuing recommendations. Profiles are stored indefinitely in the EU by the data controller and released to third parties.”

EquivalentClasses(<http://company.org/consents/Recommendations>)
ObjectIntersectionOf(
  ObjectSomeValuesFrom( spl:hasData
    ObjectUnionOf(  
      ex:HeartRate sved:Location ))
  ObjectSomeValueFrom( spl:hasProcessing
    ObjectIntersectionOf(  
      svpr:Collect svpr:Analyze px:Profiling ))
  ObjectSomeValueFrom( spl:hasPurpose ex:Recommendation)
  ObjectSomeValueFrom( spl:hasStorage
    ObjectIntersectionOf(
      ObjectSomeValuesFrom( spl:hasLocation
        ObjectIntersectionOf(  
          sved:OurServers sved:EU ))
      DataSomeValuesFrom( spl:durationInDays
        DatatypeRestriction(  
          xsd:integer
          xsd:mininclusive "0"^^xsd:integer )))
  ObjectSomeValueFrom( spl:hasRecipient svr:AnyRecipient )))

ex:Recommendation rdfs:subClassOf svpu:Marketing
Transparency framework

- Record **data processing and sharing events**
- We have developed a vocabulary for the logs (SPLOG)
  - [http://purl.org/specialprivacy/splog](http://purl.org/specialprivacy/splog)
Transparency framework

- Record **data processing and sharing events**
- We have developed a vocabulary for the logs (SPLOG)
  - [http://purl.org/specialprivacy/splog](http://purl.org/specialprivacy/splog)

`befit:BeFitLog` a `splog:Log`;

- `dct:title` "Log of BeFitDatabaseEurope"@en;
- `dct:description` "This contains events on BeFitDatabaseEurope tracking devices geo-located in Europe"@en;
- `dct:issued` "2018-02-14"^^xsd:date;
- `prov:wasAttributedTo` befit:BeFitDatabaseEurope;
- `splog:processor` befit:Us.
Transparency framework

- Record **data processing and sharing events**
- We have developed a vocabulary for the logs (SPLOG)
  - [http://purl.org/specialprivacy/splog](http://purl.org/specialprivacy/splog)

```ttl
befit:entry3918 a splog:ProcessingEvent;
  dct:title "Collection of new device position"@en;
  splog:dataSubject befit:Sue ;
  dct:description "We collected a new position of your BeFit device in our database in Europe"@en;
  splog:transactionTime "2018-01-10T13:20:50Z"^^xsd:dateTimeStamp;
  splog:validityTime "2018-01-10T13:20:00Z"^^xsd:dateTimeStamp;
  splog:message "Tracking position by GPS... collected!" ;
  splog:eventContent befit:content3918 ;
```
Transparency framework

- Record data processing and sharing events
- We have developed a vocabulary for the logs (SPLOG)
  - http://purl.org/specialprivacy/splog

```
befit:content3918 a splog:LogEntryContent;
  dct:description "Location data are collected by a BeFit device only for the health purpose of the service"@en;
  spl:hasData ssvd:Location;
  spl:hasProcessing befit:SensorGathering;
  spl:hasPurpose befit:HealthTracking;
  spl:hasStorage [ has:location ssvl:OurServers ];
  spl:hasRecipient [ a svr:Ours ].

befit:SensorGathering rdfs:subClassOf svpr:Collect.
befit:HealthTracking rdfs:subClassOf svpu:Health.
```
Transparency framework

- Record data processing and sharing events
- We have developed a vocabulary for the logs (SPLOG)
  - [http://purl.org/specialprivacy/splog](http://purl.org/specialprivacy/splog)
- We have a running prototype (ESWC 2018)
Discussion

• lack of specific and standard **vocabularies** for representing **privacy-related events**
• It should be possible to describe the event content at different **granularities**
  • from a simple **taxonomy** (stating the type of data, processing, etc.), to the most fine-grained description of the **actual data** associated to the event;
• **Interoperability/standard APIs**
  • different systems within a company and/or different companies
The SPECIAL Policy Log Vocabulary
A vocabulary for privacy-aware logs, transparency and compliance

Javier D. Fernández, Piero Bonatti, Wouter Dullaert, Sabrina Kirrane, Uros Milosevic, Axel Polleres

W3C Workshop on Privacy and Linked Data
18/04/2018