Policies, Policy Language and Vocabulary to Automatically Handle Privacy Issues in Future Personal and Professional Transportation

Dr. Martin Kurze, Deutsche Telekom

12 September, 2019

(acknowledging Sabrina Kirane, Piero Bonnattl & Rudy Jacob for their work/contribution)
ACKNOWLEDGEMENT: EU PROJECT „SPECIAL“: PROJECT PARTNERS AND CREDITS

This work is a result of H2020 project SPECIAL and was supported by

The project SPECIAL (Scalable Policy-awarE linked data arChitecture for privacy, trAnsparency and compLiance) has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 731601 as part of the ICT-18-2016 topic Big data PPP: privacy-preserving big data technologies.
Transportation is undergoing a fundamental change today:

From Mono-modality based on one vehicle owned by the person/company
to “multi-modal systems of shared vehicles, orchestrated by online-transportation service providers” (like UBER 😊).

⇒ data is potentially PII (personally identifiable information)

⇒ under special legal protection

⇒ high value for (re)use outside the transportation field.
THE SPECIAL APPROACH: POLICY LANGUAGE, VOCABULARY AND POLICY ENGINE

The H2020 project SPECIAL has already developed a rich framework for consent management and automated compliance checking that should be of interest for most of the participants to this workshop.

Funded by the European Union’s Horizon 2020 research and innovation programme under grant agreement N. 731601.
MAIN LEGAL BASE OF UTILIZING PII:

General Data Protection Regulation (GDPR)
Analysing & Modelling the GPDR

Lessons learned

ODRL was heavily guided by licensing use cases......

Therefore when modelling regulatory requirements we need to decide how closely we stick to the original model

[source: Sabrina Kirrane]
Usage policy language
The minimal core model

- Collected data
- Purpose of data collection and processing
- How is data processed
- Where are collected data and profiles stored
- For how long are the data stored
- Disclosure to third parties

Transparency Ledger

[Image of personal data]

[Logos of Oracle, Symantec, VMware, Amazon, Microsoft, SAP, Salesforce, Adobe]

[source: Sabrina Kirrane]
Usage policy language
Syntax and expressivity

- Usage policy language, which can be used to express both the data subjects’ consent, data controllers usage requests, fragments of the GDPR, and business policies
- The foundation of the policy language was the Minimal Core Model (MCM)
- We propose a new policy language that extensively re-uses standards based privacy-related vocabularies
- We are able to leverage existing Web Ontology Language (OWL) based reasoners out of the box
Usage policy language
SPECIAL resources

The SPECIAL Usage Policy Language
version 0.1

Unofficial Draft 06 April 2018

Editor:
Javier D. Fernández (Vienna University of Economics and Business)

Authors:
Piero Bonatti (Università di Napoli Federico II)
Sabrina Kirrane (Vienna University of Economics and Business)
Lina Menea Petrescu (Universität di Napoli Federico II)
Luigi Sambucetti (Università di Napoli Federico II)
Eva Schlehuber (ResearchLabs Landeszentrum für Dat.

This document is licensed under a Creative Commons Attribution 3.0 De.

Abstract
This document specifies usage policy language of SPECIAL both the data subject’s consent and the data usage policy by a computer, so as to automatically verify that the usage policy defined in this document is publicly available.

Vocabulary ...

The following is the formulation in functional syntax of the Usage Policy Language Ontology with identifier

http://www.specialprivacy.eu/langs/usage-policy#

The documentation can be found in Policy Language V1 (deliverable D2.1).

• Detailed in D2.1 Policy Language V1
• Available for download via the SPECIAL website
  https://www.specialprivacy.eu/langs/usage-policy
• An unofficial draft specification has been published online
  http://purl.org/specialprivacy/policylanguage
• Feeds into the standardisation efforts conducted in the W3C Data Privacy Vocabularies and Controls Community Group

Transparency and compliance checking platforms

- Data processing and sharing event logs are stored in the Kafka distributed streaming platform, which in turn relies on Zookeeper for configuration, naming, synchronization, and providing group services.
- We assume that consent updates are infrequent and as such usage policies and the respective vocabularies are represented in a Virtuoso triple store.
- The compliance checker, which includes an embedded
- A HermiT reasoner uses the consent saved in Virtuoso together with the application logs provided by Kafka to check that data processing and sharing complies with the relevant usage control policies.
- As logs can be serialized using JSON-LD, it is possible to benefit from the faceting browsing capabilities of Elasticsearch and the out of the box visualization capabilities provided by Kibana.

A Scalable Consent, Transparency and Compliance Architecture
Sabrina Kirrane, Javier D. Fernández, Wouter Dullaert, Uros Milosevic, Axel Polleres, Piero Bonatti, Rigo Wenning, Olha Drozd and Philip Raschke
Proceedings of the Posters and Demos Track of the Extended Semantic Web Conference (ESWC 2018)
CONCLUSIONS AND INVITATION TO COLLABORATE

Transportation and telecommunication are just two industries dealing with data, some of it “personal/private” in nature. A few questions and open issues are intended for discussion during the workshop. The following list is just a starting point for a hopefully lively discussion and exchange of experience:

• How to get “user consent” to exchange PII?
• Do we need “one huge universal” ontology (for transportation and privacy) or several smaller ones?
• Would a “policy model” be applicable for transportation too?
• Transparency for the data subject and privacy protection might contradict the “open” use of PII (such as location information for advances traffic management)
EU HORIZON2020 PROJECT „SPECIAL“ CONSIDERS THIS AN OPPORTUNITY FOR EUROPE, NOT A CHALLENGE

Together with academia, industry and even regulatory authorities, the consortium developed a solution for the needs above:

Basic concept: „sticky policies“ attached to data

- Policy language to express „rules“ how data (Personally Identifiable Data, PII) may or may not be used
- Policy engine to check (and enforce) compliance
- Full transparency and control for the user ("data subject")

More details on the web:
https://www.specialprivacy.eu/
ACKNOWLEDGEMENT: EU PROJECT „SPECIAL“:
PROJECT PARTNERS AND CREDITS

This work is a result of H2020 project SPECIAL and was supported by

The project SPECIAL (Scalable Policy-aware linked data architecture for privacy, transparency and compliance) has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 731601 as part of the ICT-18-2016 topic Big data PPP: privacy-preserving big data technologies.