Engaging Content
Engaging People

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Privacy Preserving Personalisation

Ramisa Hamed

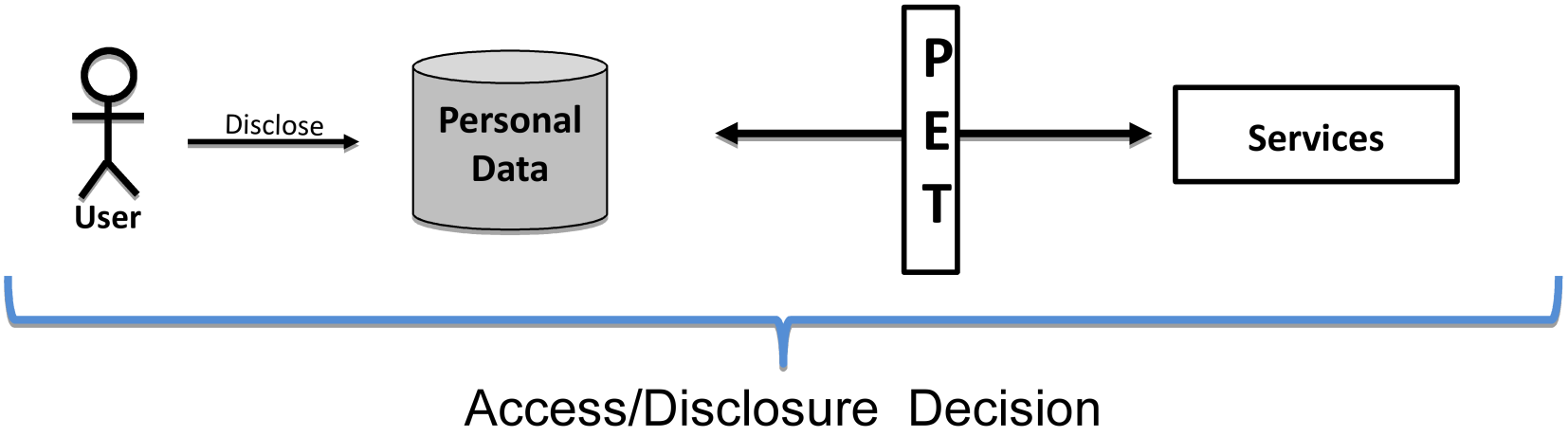
ramisa.hamed@adaptcentre.ie

W3C Workshop on Privacy and Linked Data

18th Apr. 2018

Ireland's European Structural and Investment Funds Programmes 2014-2020
Co-funded by the Irish Government and the European Union
European Union
European Regional Development Fund
SFI Science Foundation Ireland

The ADAPT Centre is funded under the SFI Research Centres Programme (Grant 13/RC/2106) and is co-funded under the European Regional Development Fund.



Problems:

- Lack of user understanding for system-made(automatic) disclosure decisions
- Lack of runtime(active) user engagement in making disclosure decisions

Research aims

1. To empower users in disclosure decision

   Help users for increasing control over accessing to their personal data by
   - Understanding disclosure decision
   - Active engagement

2. To balance between automatic disclosure decision and active user engagement

Steps

1. **Characteristics and Taxonomy of Personal Data**

2. **Scrutable Disclosure Decision**
   - Making Automatic Disclosure Decision
   - Explaining Automatic Disclosure Decision
   - Expressing Disclosure Decision in Natural Language

3. **Active User Engagement**
   - Evaluating consequence
   - Recommending action
   - Confirming access

Technical approach

Purpose a framework

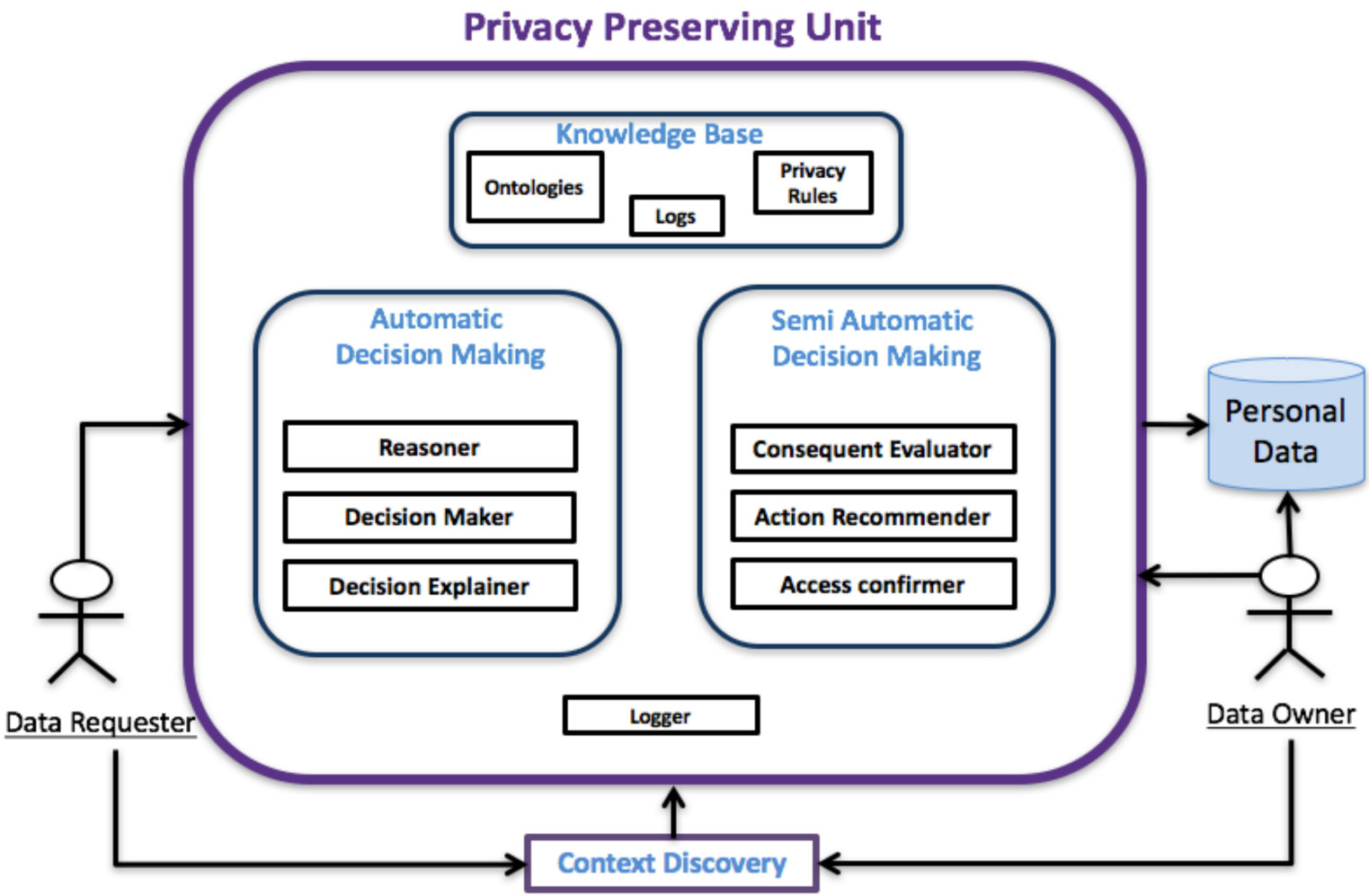
Ontological access control model

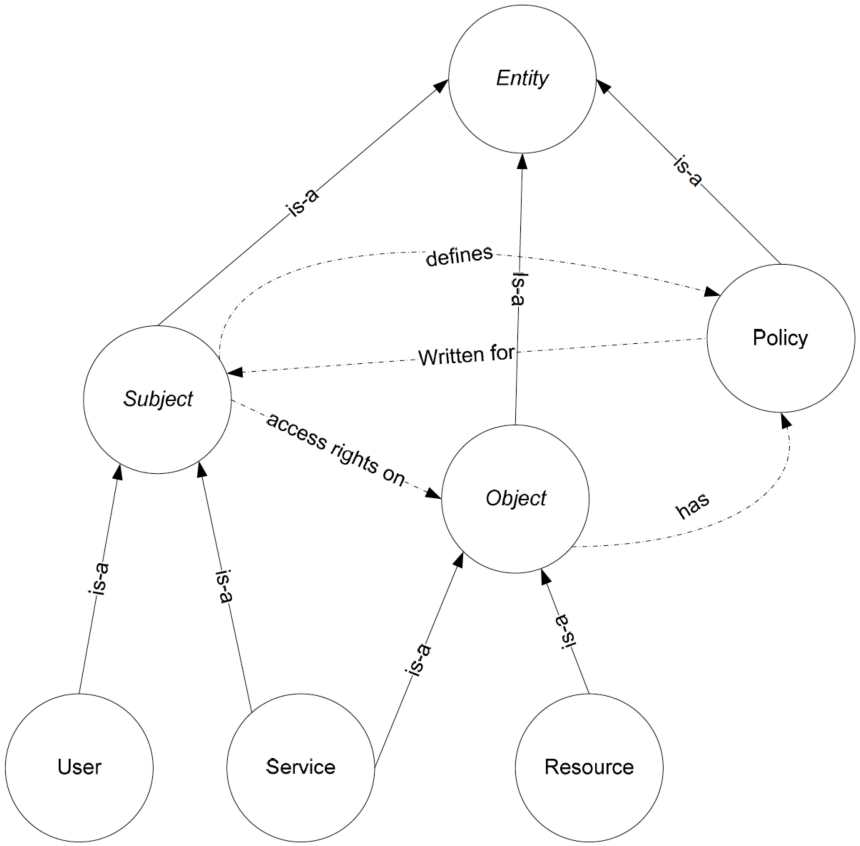
Use advantage of semantic web technologies – reasoning

- Ontologies for modelling – OWL – using protégé
- Semantic rules for privacy policies – SWRL
- Using model in Apache Jena API
- Semantic reasoning for inference – Pellet
- Appling appropriate SPARQL queries to return the result for access decision
- Using OwlExplanation[1] to explain inferred axioms
- Using Triple2NL[2] to convert triples into natural language

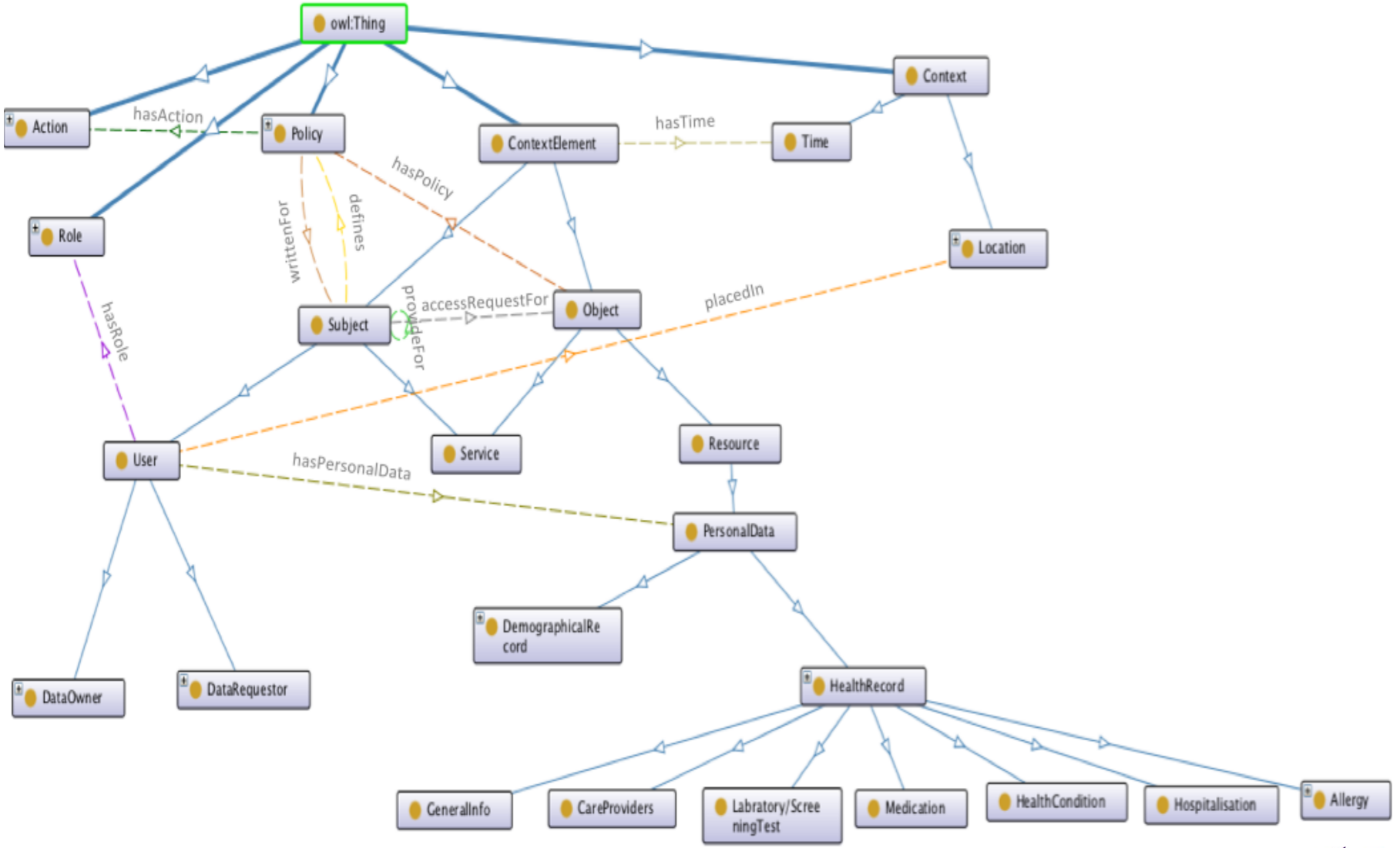
1 Horridge, M., Parsia, B., & Sattler, U. (2009).

The OWL Explanation Workbench : A toolkit for working with justifications for entailments in OWL ontologies, 1, 1–5.


Privacy Preserving Unit
Knowledge Base
Ontologies
Logs
Privacy Rules
Automatic Decision Making
Reasoner
Decision Maker
Decision Explainer
Semi Automatic Decision Making
Consequent Evaluator
Action Recommender
Access confirmer
Logger
Personal Data
Data Requester
Data Owner
Context Discovery



1 Imran-Daud, M., Sanchez, D., & Viejo, A. (2016). Ontology-based Access Control Management: Two Use Cases. *Proceedings of the 8th International Conference on Agents and Artificial Intelligence*, *1*(Icaart), 244–249.


owl:Thing
Context
Action
hasAction
Policy
ContextElement
hasTime
Time
hasPolicy
writtenFor
defines
Role
Location
hasRole
Subject
providesFor
accessRequestFor
Object
placedIn
User
Service
Resource
hasPersonalData
PersonalData
DemographicalRecord
DataOwner
DataRequestor
HealthRecord
GeneralInfo
CareProviders
Labratory/ScreeningTest
Medication
HealthCondition
Hospitalisation
Allergy

Semantic rules for privacy policies - SWRL

plc-1: *Dr. Erik as Julie's family doctor can access and modify her health record.*

DataOwner(?do) ^ DataRequestor(?dr) ^ HealthRecord(?hr) ^ DemographicalRecord(?dmr1) ^ DemographicalRecord(?dmr2) ^ Policy(?plc)^ hasPersonalData(?do, ?dmr1) ^ hasPersonalData(?dr, ?dmr2) ^ name(?dmr1, "Julie") ^ name(?dmr2, "Dr. Erik") ^ hasRole(?dr, gp) ^ providerFor(?dr, ?do) ^ hasPersonalData(?do, ?hr) ^ accessRequestFor(?dr, ?hr) ^ hasPolicy(?hr,?plc)-> has Action(?plc,"modify")

SPARQL query that shows who have access to which data based on which policy

```
PREFIX ns: <http://www.semanticweb.org/ramisa/ontologies/2017/7/basicOntology#>
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
SELECT DISTINCT ?dtR  ?RequesterName ?RequesterRole  ?AccessedData ?Action ?dtO ?OwnerName ?Policy
WHERE {
        ?dtR rdf:type ns:DataRequestor.
        ?Policy rdf:type ns:Policy.
        ?dtO rdf:type ns:DataOwner.
        ?AccessedData rdf:type ns:PersonalData.
        OPTIONAL{?dtR ns:hasPersonalData ?dem.
                ?dem ns:name ?RequesterName}
        ?dtR ns:hasRole ?RequesterRole.
        ?Policy ns:writtenFor ?dtR.
        ?dtR ns:accessRequestFor ?AccessedData.
        ?AccessedData ns:hasPolicy ?Policy .
        ?Policy ns:hasAction ?Action.
        ?Policy ns:description ?PolicyDescription.
        ?dtO ns:hasPersonalData ?dem1.
        ?dem1 ns:name ?OwnerName.
        ?dtO ns:hasPersonalData ?AccessedData.
}
```

RequesterName	RequesterRole	RequestedData	Action	OwnerName	PolicyDescription
"Dr. Murphy"	ns:specialist	"Allergy Record"	ns:modify	"Julie"	"Each specialist, Which located in assigned patient location, can modify her/his health record."
"Dr. Erik"	ns:gp	"Health Record"	ns:modify	"Julie"	"Dr. Erik as Julie's family doctor can access and modify her health record."

Disclosure decision – asserted axiom

:dtR-1 rdf:type :DataRequestor.
:dtR-1 :hasPersonalData :demR-2.
:demR-2 :name “Dr. Erik”.

:dtO-1 rdf:type :DataOwner.
:dtO-1 :hasPersonalData :demR-1.
:demR-1 :name “Julie”.

:hr-1 rdf:type :PersonalData.
:dtO-1 :hasPersonalData :hr-1.
:dtR-1 :accessRequestFor :hr-1.
:hr-1 :hasPolicy :plc-1.
:hr -1 :description “Health Record”

:plc-1 rdf:type :Policy.
:plc-1 :writtenFor :dtR-1.
:plc-1 :hasAction “modify”.
:plc-1 :description “Dr. Erik as Julie’s family doctor can access and modify her health record.”.

Disclosure decision – inferred axiom

:dtR-2	rdf:type	:DataRequestor.
:dtR-2	:hasPersonalData	:demR-3.
:demR-3	:name	“Dr. Murphy”.
:dtO-1	rdf:type	:DataOwner.
:dtO-1	:hasPersonalData	:demR-1.
:demR-1	:name	“Julie”.
:alg-1	rdf:type	:PersonalData.
:dtO-1	:hasPersonalData	:alg-1.
:dtR-1	:accessRequestFor	:alg-1.
:alg-1	**:hasPolicy**	**:plc-2.**
:alg-1	:description	“Allergy Record”
:plc-2	rdf:type	:Policy.
:plc-2	:writtenFor	:dtR-2.
:plc-2	:hasAction	“modify”.
:plc-2	:description	“Each specialist, which located in assigned patient location, can modify patient’s health record.”.

OwlExplanation for inferred axioms


```
[Explanation <ObjectPropertyAssertion(<ns:hasPolicy> <ns:alg-1> <ns:plc-2>)>
        SubClassOf(<ns:Allergy> <ns:HealthRecord>)
        DLSafeRule( Body(ClassAtom(<ns:Allergy> Variable(<ns:alg>))
                                    ClassAtom(<ns:DataOwner> Variable(<ns:do>))
                                    ClassAtom(<ns:HealthRecord> Variable(<ns:alg>))
                                    ClassAtom(<ns:HealthRecord> Variable(<ns:hr>))
                                    ObjectPropertyAtom(<ns:hasPersonalData> Variable(<ns:do>) Variable(<ns:alg>))
                                    ObjectPropertyAtom(<ns:hasPersonalData> Variable(<ns:do>) Variable(<ns:hr>))
                                    ObjectPropertyAtom(<ns:hasPolicy> Variable(<ns:hr>) Variable(<ns:plc>)))
                                Head(ObjectPropertyAtom(<ns:hasPolicy> Variable(<ns:alg>) Variable(<ns:plc>))) )
        ObjectPropertyAssertion(<ns:hasPersonalData> <ns:dtO-1> <ns:alg-1>)
        ClassAssertion(<ns:HealthRecord> <ns:hr-1>)
        ObjectPropertyAssertion(<ns:hasPersonalData> <ns:dtO-1> <ns:hr-1>)
        ClassAssertion(<ns:Allergy> <ns:alg-1>)
        ClassAssertion(<ns:DataOwner> <ns:dtO-1>)
        ObjectPropertyAssertion(<ns:hasPolicy> <ns:hr-1> <ns:plc-3>)
]
```

Thank you