A Configurable Approach to Privacy Ontology and its Application to Mobile e-Health Services

Diego Garcia, M. Beatriz F. Toledo – *U. of Campinas, Brazil*

Miriam A. M. Capretz – *U. of Western Ontario, Canada*

Gordon S. Blair, Paul Grace, Carlos Flores – *Lancaster U., UK*

PrimeLife/IFIP Summer School

Nice, France, September 7-11, 2009

Outline

- Introduction
- Approach
- Ontologies
- Service Discovery
- Contributions
- Conclusions

Introduction

- e-Service privacy
- Consumer concern
  - Data misuse
- Improper management
  - Threat to e-Service wide acceptance

Introduction

- Application area
  - Specific issues
    - Service domain
    - Operating environment
- Privacy solutions
  - Targeted domain and environment issues
  - General issues

Introduction

- Public healthcare program
  - Providers employ workers to collect patients’ data remotely
  - Mobile devices to collect health data in the field
- Outpatient setting
  - Patients remotely monitored
  - Mobile technology to monitor health conditions and ensure medication regime adherence

Problem

- Ontologies for different domains and environments
  - Platform for Privacy Preferences (P3P) - Web
  - e-Commerce - policy benchmark
- Common concepts
  - Redefined
- Interoperability
  - Lack of shared vocabulary

Problem

- Discovery frameworks
  - Non-functional features
  - Privacy
    - Non-functional features in general
    - Proper solution for privacy management

Goals

- Ontological approach for different areas
- Consumer preferences for service discovery
- Application to m-Health

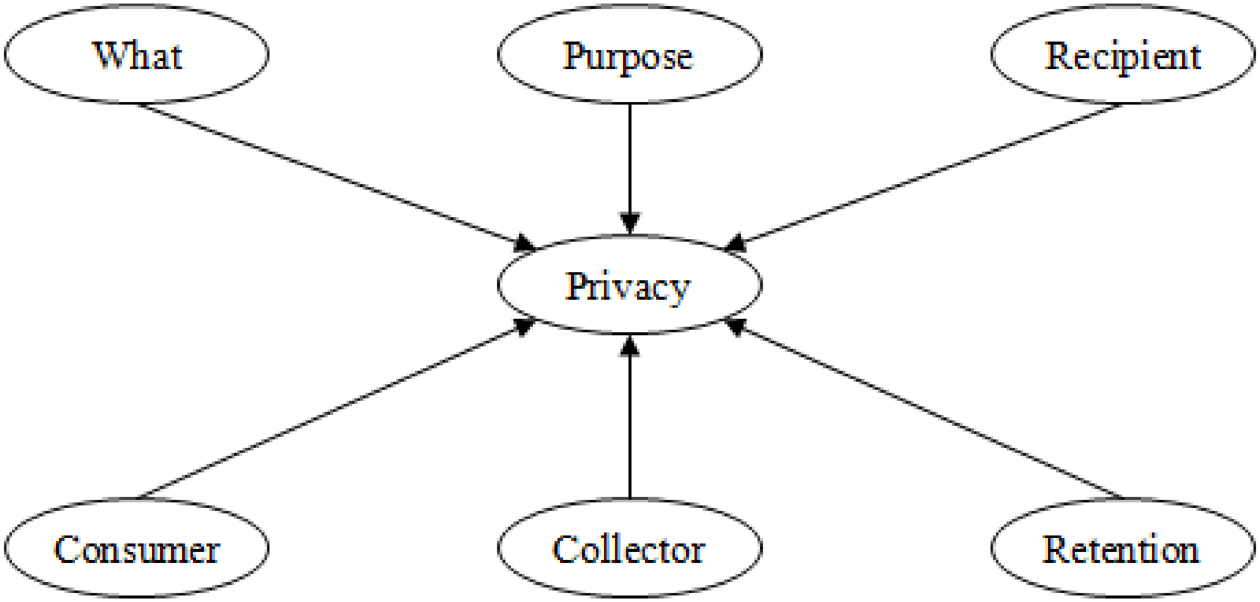
Approach

- Top-level concepts
- Specific concepts
  - Common specific vocabulary
- *Purpose*'s categorization
  - Data collection purposes in a given area

Base Ontology

- Regulations
  - European Union’s Data Protection Directive
- Principles
  - Openness
  - Collection and use limitation
- Ontology
  - Web Ontology Language (OWL)

Base Ontology



Base Ontology

- *What*
  - Data type categorization
    - Prescription
- *Collector*
  - Provider that collects data
    - Healthcare providers
- *Consumer*
  - Consumer’s characteristics
    - Patient’s age

Base Ontology

- *Purpose*
  - Purpose for which data are collected
    - Healthcare program assessment
- *Recipient*
  - Entity to which data are disclosed
    - Identification information
    - Relationship between recipient and collector
- *Retention*
  - Time frame in which data are used
    - Specific time period
    - Time period needed to complete service

Extensions

- Approach
  - Ontologies for each area
- Extensions
  - m-Health
- Ontologies
  - Operating environment of mobile computing
  - Service domain of e-Health

Mobile Computing

- Threats to privacy
- Specific issues
- Mobile computing ontology
  - Concepts

Mobile Computing

- *Time*
  - Time of day when interaction occurs
    - Specific time
    - Working hours
- *Location*
  - Location where interaction occurs
    - Pharmacy
    - Address
- *Context*
  - Context of consumer when interaction occurs
    - Same area as medical doctor

Mobile Computing

- *Accuracy*
  - Data accuracy
    - Location precision does not enable identifying patient
- *Anonymity*
  - Anonymous use
    - Health information service

e-Health

- e-Health privacy
- Specific issues
- e-Health ontology
  - Concepts

e-Health

- *Effect*
  - Privacy-related effect of data change
    - Practice executed when patient updates data
- *Policy*
  - Recipient policy location
    - Policy of third party provider employed by healthcare provider

e-Health

- *Consequence*
  - Consequence of not providing optional data
  - Anonymous patients with restricted functionality
- *Stop*
  - Withdraw data collection access
  - Stop continuous collection of data on health condition

Service Discovery

- Service-oriented computing paradigm
  - Service publication and discovery architecture
    - Service discovery frameworks
- Roles
  - Provider
    - Publishes and delivers services
  - Consumer
    - Discovers and uses services
  - Registry
    - Provides publishing and discovering mechanisms

Service Discovery

- Services offering particular functionality
  - Descriptions include functional characteristics
- Privacy
  - Service discovery process
- Privacy ontologies enrich discovery process
  - Extending a service discovery framework

Service Discovery

- Each service has privacy policy
  - How it deals with its consumers' data
- Consumer has privacy preference
  - Requirements regarding privacy protection
- Provider publishes service policy
- Consumer sends preference to registry
- Compared during service discovery
  - Check if service meets requirements

Service Discovery

- Ontologies to demonstrate extension
  - Integrated into discovery framework
- Consumers and providers use them to specify preferences and policies
  - Referencing concepts from ontologies

Service Discovery

- Preferences and policies use discovery framework's service abstraction
  - Protocol-independent
  - Translates to/from service description languages
  - Defines property URI schema
    - Functionality, privacy policies, others

Service Discovery

1 property:type.Attr.Privacy.Base:What=Prescription

2 property:type.Attr.Privacy.Mobile:Location=Own

3 property:type.Attr.Privacy.Ehealth:Stop

Service Discovery

- Collection that includes threat to privacy
  - Location is monitored
  - Patient visited specialized medical centre
  - Patient’s health condition

Contribution

- Ontological approach
  - Specific ontology development
    - Base ontology extension
    - Standardization body
  - Interoperability across areas
    - Base concepts
    - Specific concept comparison

Contribution

- Service discovery extension
  - Privacy features
- Consumers
  - Service selection
  - Privacy preferences
- Step for e-Service acceptance

Contribution

- m-Health
- Opportunities
  - Mobile computing - context-aware services
  - e-Health - healthcare services through networks
- Privacy concerns
  - Article 29 Working Party
    - e-Health record processing
    - Patient rights safeguards

Contribution

- Another dimension to standardization efforts
- Healthcare vocabularies
  - Systematised Nomenclature of Medicine Clinical Terms (SNOMED CT)
  - Clinical practice
- Additional issues
  - Vocabulary definition

Contribution

- e-Health interoperability
- Roadmap projects
  - RIDE
  - SemanticHEALTH
- Clinical data model
  - Semantic interoperability

Conclusions

- Base ontology
  - Regulations
  - Interoperability
- Mobile computing and e-Health privacy
  - m-Health ontologies
- Top-level concepts
- Service discovery
- Other e-Service aspects

Future Work

- Consumer cannot find service that meets preference
  - Negotiation
- Tool to guide consumers specifying preferences
  - Preference templates
  - Template configuration

A Configurable Approach to Privacy Ontology and its Application to Mobile e-Health Services

Diego Garcia, M. Beatriz F. Toledo – *U. of Campinas, Brazil*

Miriam A. M. Capretz – *U. of Western Ontario, Canada*

Gordon S. Blair, Paul Grace, Carlos Flores – *Lancaster U., UK*

PrimeLife/IFIP Summer School

Nice, France, September 7-11, 2009