CONTEXT: Understanding the Role of Contexts in Managing Privacy Online

Gideon Ogunniye, Nadin Kökciyan

School of Informatics, University of Edinburgh, UK.

g.ogunniye@ed.ac.uk
• Motivation: Why context matters in privacy
• Goal one:
  • Develop a novel ontology for privacy
• Goal two:
  • Develop an agent-based PET for automated privacy reasoning
• Summary
Motivation: Why context matters in privacy

Assume Bob has a tracking app:

![Image of tracking app settings]

- Problem: It might be inappropriate to share a user's location information if exposing the user to danger.
- Privacy preferences are diverse and context-dependent.
Motivation: Why context matters in privacy

Assume Bob has a tracking app:

Bob’s location settings:

- Problem: It might be inappropriate to share a user’s location information if exposing the user to danger.
- Privacy preferences are diverse and context dependent.
Motivation: Why context matters in privacy

Assume Bob has a tracking app:

Bob’s location settings:

- **Problem**: It might be inappropriate to share a user’s location information if exposing the user to danger.
- **Privacy preferences are diverse and context dependent.**
Motivation: Why context matters in privacy policy

- A user context should capture the information that describes the situation of a user either directly or indirectly.
Motivation: Why context matters in privacy policy

- **A user context** should capture the information that describes the situation of a user either directly or indirectly.
- **What do we need?**

**Figure 1:** Bob’s location settings
Main Goal: Understand the role of contexts in privacy policy

- **Goal one:** Develop a novel **ontology** to represent privacy contexts\(^1\)
  - Capture new context-oriented privacy requirements
  - Use a formal language to represent privacy contexts

\(^1\)https://github.com/gideonbms/PROCI_ontology
Main Goal: Understand the role of contexts in privacy policy

- **Goal one**: Develop a novel ontology to represent privacy contexts
  - Capture new context-oriented privacy requirements
  - Use a formal language to represent privacy contexts
- **Goal two**: Develop an agent-based PET for automated privacy reasoning
  - Model use-case scenarios
  - Implement the proposed agent-based PET using Semantic Web Technologies (SWT)

---

1 [https://github.com/gideonbms/PROCI_ontology](https://github.com/gideonbms/PROCI_ontology)
Main Goal: Understand the role of contexts in privacy policy

- **Goal one:** Develop a novel **ontology** to represent privacy contexts\(^1\)
  - Capture new context-oriented privacy requirements
  - Use a formal language to represent privacy contexts
- **Goal two:** Develop an **agent-based PET** for automated privacy reasoning
  - Model use-case scenarios
  - Implement the proposed agent-based PET using Semantic Web Technologies (SWT)
- **Example:**
  - An agent-based PET that automates privacy decision-making in a medical context.

\(^1\)https://github.com/gideonbms/ROCI_ontology
Goal One: Capture new context-oriented privacy requirements

RQ: What are the privacy requirements captured in the existing IoT ontologies?

Figure 2: Research Methodology in Three Steps
Goal One: Capture new context-oriented privacy requirements

Figure 3: A Taxonomy of Privacy Requirements [1]

Goal One: Use a formal language to represent privacy contexts

PROCI: Privacy Ontology Based on Contextual Integrity

- Theory of Contextual integrity (CI)[2], understands privacy in a social context, by defining norms that govern appropriate information flows
- We reuse classes and properties from three ontologies; COPri, Aegis and PPIoT

Goal Two: Model use-case scenarios

Professional context:
- Bob works for a firm
- He uses his smartphone to log in hours
- The smartphone keeps track of his data
- His data is shared with phone network provider
- An Admin Officer, Line Manager, Health and Safety Manager can request for Bob’s data

Cloud services

Privacy requirements

Conflicting, incomplete/partial

Applying CI for appropriate information flow

Contextual informational norms/rules:
- Appropriate information = “meet expectation” e.g., It might be in “B’s” best interest for “PNP” to share his location data with “HSM” without his consent but not with “BLM”

Legitimate, morally justifiable norms
- Are individual preferences, ethical and political principles, contextual values, purposes protected?

Norms can be controversial

The justification of a norm may need to be explained/argued

Actors:
- Bob (B),
- Bob’s Line Manager (BLM),
- Health and Safety Manager (HSM)
- Police (P),
- Phone network provider (PNP)

Information Type:
- What types of information are involved?

Transmission principles:
- What are the constraints involved?


Gideon Oggunniye, Nadin Kökciyan
School of Informatics, University of Edinburgh
CONTEXT: Understanding the Role of Contexts in Managing Privacy Online
Goal Two: An agent-based PET

- To develop an agent-based PET to:
  - represent the **dynamism** of privacy preferences and expectations
  - reason about contexts, norms and privacy preferences
  - reason about **conflicting** privacy preferences
  - **communicate** privacy decisions and provide **explanations** on the decisions
In our approach:

- We exploit Semantic Web Technology to manage the interactive setting of users’ privacy preferences.
  - SWT enables a lightweight communication between a user and the Third Parties (TP) that request access to the user’s private data.
  - The user and TP are represented as agents.
Goal Two: Implement the PET using SWT (Ongoing)

In our approach:

- We exploit Semantic Web Technology to manage the interactive setting of users’ privacy preferences.
  - SWT enables a lightweight communication between a user and the Third Parties (TP) that request access to the user’s private data.
  - The user and TP are represented as agents.
- For reasoning:
  - We employ an Argumentation Theory (ASPI+)[4] to model negotiation and persuasion between agents to resolve conflict of opinions.

In our approach:

- We exploit Semantic Web Technology to manage the interactive setting of users’ privacy preferences.
  - SWT enables a lightweight communication between a user and the Third Parties (TP) that request access to the user’s private data.
  - The user and TP are represented as agents.
- For reasoning:
  - We employ an Argumentation Theory (ASPIC+)\[4\] to model negotiation and persuasion between agents to resolve conflict of opinions.

Summary

- **The theory of CI helps to**: understand privacy preferences and expectations and the norms of information transmission in a given context.
- **Argumentation-based dialogues** is a promising mechanism to:
  - represent and reason about the contextual norms of contextual integrity;
  - capture the dynamics of privacy contexts;
  - reason about uncertain, incomplete and conflicting privacy preferences.

Next plan:

A conference paper will be submitted to the 9th International Conference on Computational Models of Argument (COMMA) by 29th April 2022.
The theory of CI helps to: understand privacy preferences and expectations and the norms of information transmission in a given context.

Argumentation-based dialogues is a promising mechanism to:
- represent and reason about the contextual norms of contextual integrity;
- capture the dynamics of privacy contexts;
- reason about uncertain, incomplete and conflicting privacy preferences.

Next plan:
- A conference paper will be submitted to the 9th International Conference on Computational Models of Argument (COMMA) by 29th April 2022.