

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`

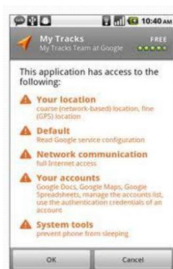


THE UNIVERSITY of EDINBURGH
informatics

- 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

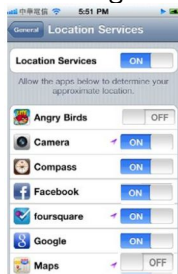
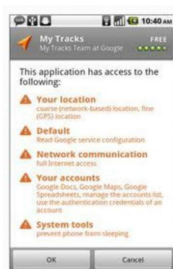
Assume Bob has a tracking app:



Motivation: Why context matters in privacy

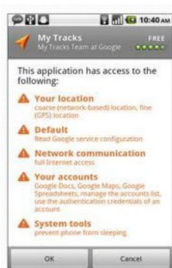
Bob's location settings:

Assume Bob has a tracking app:

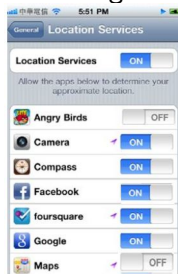


Motivation: Why context matters in privacy

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?**

The screenshot shows a mobile application interface for location settings, divided into several sections. Annotations in blue ovals with arrows point to specific parts of the interface:

- Aspects of Context** points to the "Select Resource to be Shared" section, which includes a "Location" dropdown menu and a "Granularity Level" dropdown menu set to "Room".
- Temporal Restrictions** points to the "Select Sharing Timings" section, which includes a "From: 9:30:00 AM To: 5:00:00PM" range and a "All Days" dropdown menu with options for "Weekdays", "Weekend", and "Monday".
- Context Restrictions** points to the "Except!" section, which includes a "Location" dropdown menu set to "Club Building 5/2" and an "Activity" dropdown menu set to "Dating Partying Classing".
- Generalization of Context** points to the "Select Resource to be Shared" section, specifically to the "Granularity Level" dropdown menu.

The interface also includes a "Select Requester and Sharing Access" section at the top, with a "Permitted" checkbox checked and a "Police" dropdown menu, and a "Prohibited" checkbox unchecked.

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 contexts¹
 - Capture new context-oriented privacy requirements
 - Use a formal language to represent privacy contexts

¹https://github.com/gideonbms/PROCI_ontology

Main Goal: Understand the role of contexts in privacy policy

- **Goal one:** Develop a novel ontology to represent privacy contexts¹
 - 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)

¹https://github.com/gideonbms/PROCI_ontology

Main Goal: Understand the role of contexts in privacy policy

- **Goal one:** Develop a novel ontology to represent privacy contexts¹
 - 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.

¹https://github.com/gideonbms/PROCI_ontology

Goal One: Capture new context-oriented privacy requirements

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

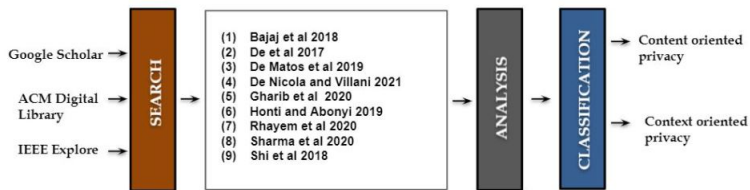


Figure 2: Research Methodology in Three Steps

Goal One: Capture new context-oriented privacy requirements

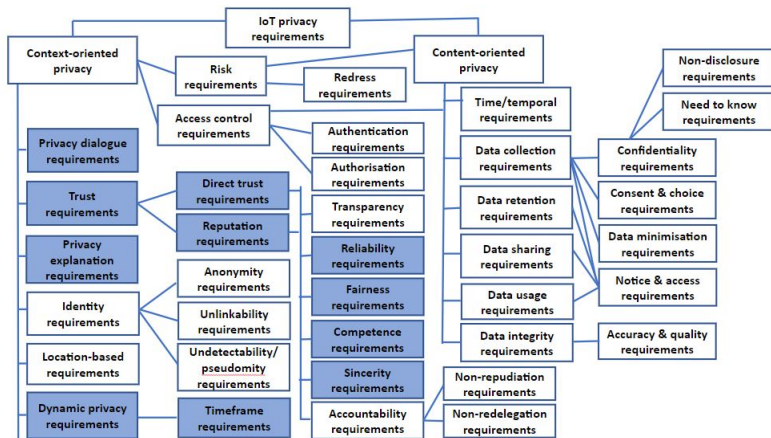


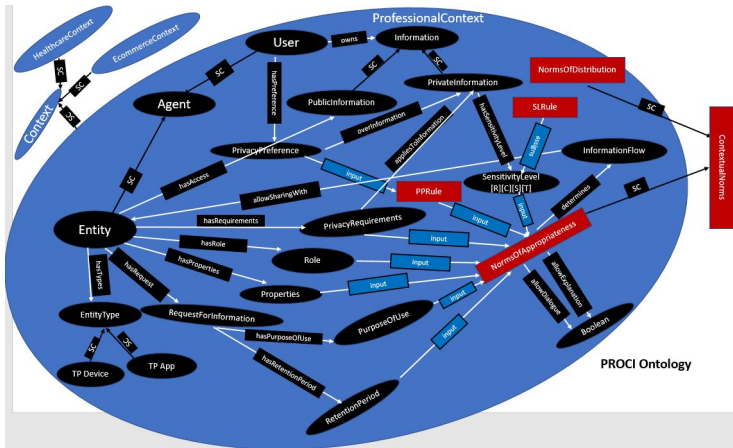
Figure 3: A Taxonomy of Privacy Requirements [1]

[1] Ogunniye, G., & Kökciyan, N. (2022). A Survey on Understanding and Representing Privacy Requirements in IoT. In: Journal of Artificial Intelligence Research (2022). Under review.

Goal One: Use a formal language to represent privacy contexts

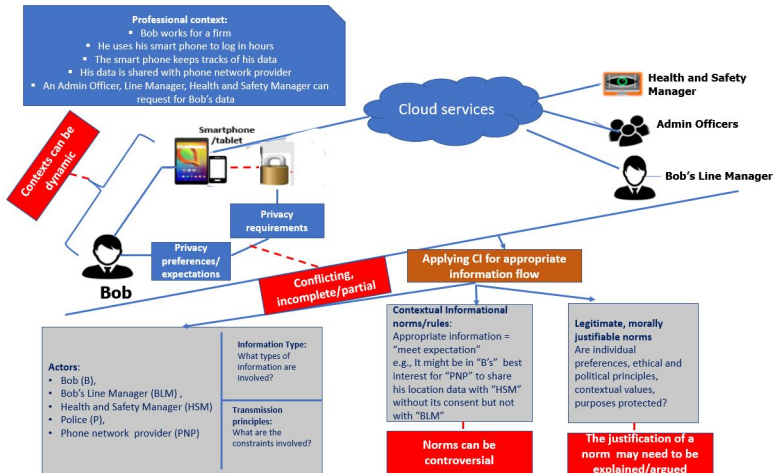
PROCI: Privacy Ontology Based on Contextual Integrity

- 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*



[2] Nissenbaum, H. (2004). Privacy as contextual integrity. Wash. L. Rev., 79, 119.

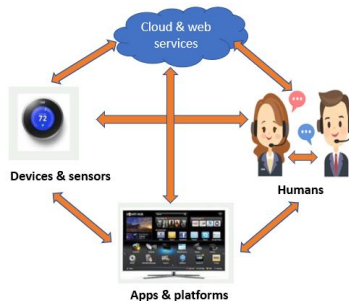
Goal Two: Model use-case scenarios



[3] Ogunniye, G., & Kökciyan, N. (2021). Argumentation-based Dialogues for Privacy Policy Reasoning. CI Symposium '21, September 30-October 01, 2021, Chicago, USA

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



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.

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 (ASPIC+)[4] to model negotiation and persuasion between agents to resolve **conflict of opinions**.

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 (ASPIC+)[4] to model negotiation and persuasion between agents to resolve **conflict of opinions**.

[4] Modgil, S., & Prakken, H. (2014). The ASPIC+ framework for structured argumentation: a tutorial. *Argument & Computation*, 5(1), 31-62.

- **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.

- **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.