REPHRAIN

Protecting citizens online

A Survey on Understanding and Representing Privacy Requirements in the Internet-of-Things

Gideon Ogunniye, University College London

Nadin Kokciyan, University of Edinburgh

February 2023

UK Research and Innovation · University of Bristol · UCL · The University of Edinburgh · King's College London · University of Bath

Journal of Artificial Intelligence Research 76 (2023) 163-192 Submitted 06/2022; published 01/2023

A Survey on Understanding and Representing Privacy Requirements in the Internet-of-Things

Gideon Ogunniye G.OGUNNIYE@UCL.AC.UK
Department of Science, Technology, Engineering and Public Policy (UCL STEaPP), University College London, London, WC1E 6JA, UK

Nadin Kökciyan NADIN.KOKCIYAN@ED.AC.UK
School of Informatics, University of Edinburgh, Edinburgh, EH8 9AB, UK

Abstract

People are interacting with online systems all the time. In order to use the services being provided, they give consent for their data to be collected. This approach requires too much human effort and is impractical for systems like Internet-of-Things (IoT) where human-device interactions can be large. Ideally, privacy assistants can help humans make privacy decisions while working in collaboration with them. In our work, we focus on the identification and representation of privacy requirements in IoT to help privacy assistants better understand their environment. In recent years, more focus has been on the technical aspects of privacy. However, the dynamic nature of privacy also requires a representation of social aspects (e.g., social trust). In this survey paper, we review the privacy requirements represented in existing IoT ontologies. We discuss how to extend these ontologies with new requirements to better capture privacy, and we introduce case studies to demonstrate the applicability of the novel requirements.

1. Introduction

People interact with online systems (such as websites and mobile applications) to be authenticated using their credentials or responding to cookie dialogues before they start getting the service they need from service providers. Each service is associated with a privacy policy that defines the privacy settings that will be in effect, and these privacy policies are defined according to regulations such as the General Data Protection Regulations (GDPR) (Voigt & Von dem Bussche, 2017). However, it has been shown that users generally ignore the details embedded in privacy policies to use the systems with which they interact (Utz et al., 2019). Hence, users need intelligent tools to assist them in making privacy decisions and keeping their sensitive information private, if possible.

Handling privacy becomes even more challenging when we look at the Internet of Things (IoT) (Sicari et al., 2015). Kökciyan and Yolum (2020) define IoT as a domain: (i) which is a *dynamic* domain where new devices can be deployed constantly, (ii) where human-device interactions can be *large*, and (iii) where IoT devices can be very *heterogeneous* with varying capabilities. IoT devices can be deployed in private and public spaces. For example, smart home technology requires *digital housekeeping*, including residents having a complete knowledge of the deployed devices, locating the devices, managing access and security, managing digital media, and restoring when technology breaks down (Tolmie

©2023 AI Access Foundation. All rights reserved.

et al., 2007). However, technology-facilitated abuse in an intimate partner violence (IPV) context where smart home technology can be exploited to harm, monitor and dominate victims has been the subject of prior research (Tanczer, López-Neira, & Parkin, 2021). Rodriguez-Rodriguez et al. (2020) emphasize that IoT devices can be prone to attacks, given that most of these devices are affordable and could be easily deployed by end users. On the other hand, governments deploy IoT devices in public spaces (e.g., streets) for various reasons (e.g., protection of citizens), and users may not be aware that their data are being collected and shared with others without their consent (Naeini et al., 2017).

From a user perspective, it is almost impossible to estimate the number of IoT devices that one interacts with. Each deployment setting brings different privacy challenges, and IoT devices continue collecting and sharing data silently; where users have little knowledge about possible effects such data practices could bring. It is unrealistic and ineffective to expect that users would give their informed consent for every interaction. Therefore, we follow the vision of the development of privacy assistants that could automatically preserve user privacy. Colnago et al. (2020) shows that users are willing to adopt privacy assistants that could make some of the decisions on their behalf. To deploy privacy assistants in real-world settings, privacy assistants should incorporate privacy requirements in sociotechnical systems. In this paper, we argue that privacy assistants could use ontologies to represent privacy requirements, reason about privacy decisions, and help users make privacy decisions in IoT. Ontologies are powerful representations in the modeling of entities and their relationships in a structured manner (McGuinness et al., 2004), and are ideal for privacy assistants who need to make context-based privacy decisions all the time.

Motivation. We first identify the privacy requirements inherent in IoT systems by reviewing state-of-the-art ontologies and the privacy requirements they represent. We observe that state-of-the-art ontologies are not sufficient to represent social aspects of privacy (i.e., social requirements), such as trust in IoT devices that may change over time. Figure 1 illustrates an example scenario to show why social aspects of privacy requirements are crucial to model privacy in IoT. This scenario is described as follows:

> **Example 1** Bob uses a smartwatch that sets reminders of his medication. The smartwatch is connected to his electronic health records to remind him of the time to take scheduled doses. In the case of emergency, the smartwatch can send a message to caregivers to respond before a costly and destructive hospitalization is required. In addition, the smartwatch can call other entities such as Emergency Service Providers depending on the nature of the emergency and Police for crime prevention. These entities can request Bob's data from the smartwatch without his consent. However, Bob would like to share his sensitive information (e.g., medical records) with entities that are trustworthy. Bob's medical and health records are stored on a remote server or cloud service until Bob deactivates his account.

In the context of privacy, we make the following observations: (i) *Bob*'s privacy preferences and expectations specify how, what, and who can collect, store, process, and disseminate his data. (ii) To prevent privacy breaches, privacy requirements (such as access control, anonymity, and confidentiality, among others) must be explicitly specified and implemented by devices collecting *Bob*'s data. Software and privacy policies are frequently updated; hence, to keep track of the changes and for *Bob* to update his privacy preferences, there is a need for constant communication between *Bob* and these devices. (iii) There are

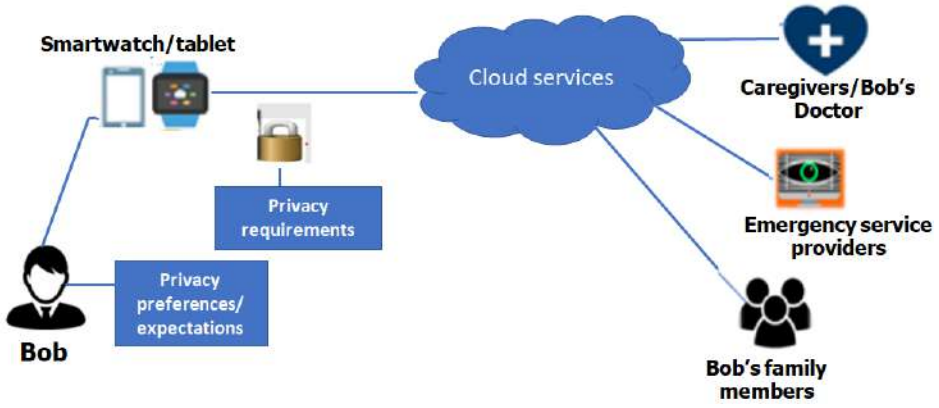

Figure 1: A typical IoT example where a user, Bob, has to interact directly or indirectly with many entities including human and automated agents.

social properties (such as trust) that might influence *Bob*'s privacy decision to share his data with certain entities (humans or devices). Furthermore, there are instances where the privacy policies governing data flow are uncertain, incomplete, or controversial (Ogunniye & Kökciyan, 2021). These policies may need to be reasoned about by the entities involved. Further explanations on the justification or legitimacy of the policies might be required. For example, the policies governing the conditions at which an *Emergency Service Provider* can request *Bob*'s medical data from his *smartwatch* without his consent need to be justified.

Contributions. In this survey, we highlight the social requirements that are important to represent the dynamism of privacy in IoT systems, which are currently not captured in state-of-the-art ontologies. Our contributions are as follows.

1. We review privacy requirements in state-of-the-art IoT ontologies that capture privacy requirements.
2. We propose a new classification system to group privacy requirements in IoT. Our classification can be extended with further requirements if needed.
3. We introduce new privacy requirements to capture the dynamism of privacy in IoT. We show the applicability of these new privacy requirements using case studies.
4. We establish future trends for capturing privacy fully in IoT by the use of ontologies, to guide researchers working on the development of AI-based privacy assistants.

The paper is organized as follows. Section 2 introduces some background information to understand privacy in the IoT domain. Section 3 highlights the methodology used in this survey paper to select publications prior to our analysis. In Section 4, we discuss the classification step in detail, where we review the privacy requirements in state-of-the-art IoT ontologies. In Section 5, we describe new privacy requirements to represent the dynamism of privacy preferences and expectations. We analyze all privacy requirements to introduce a new taxonomy of privacy requirements in IoT (Section 6). We discuss possible future directions in Section 7, and finally conclude with Section 8.

2. Background and Related Work

In this section, we provide a brief overview of the definitions of privacy and privacy requirements. We discuss how privacy requirements are represented via ontologies in the literature and also introduce some key concepts from the trust domain.

2.1 Definitions of Privacy

According to Shirey (2007), privacy is the "right of individuals to control or influence what information related to them may be collected and stored, by whom and to whom that information may be disclosed". Privacy is violated if sensitive data of an individual, such as Personal Identifiable Information (PII) is exposed to malicious or unintended recipients (Dasgupta, Gill, & Hussain, 2019). Based on this definition, existing IoT privacy ontologies (Agarwal et al., 2020; Arruda & Bulcão-Neto, 2019; Gheisari et al., 2019) have specified technical requirements to prevent privacy breaches.

Our work has been inspired by Gharib et al. (2020) who define privacy as a social concept. The authors argue that in addition to the technical aspects of privacy, the social and organizational aspects are equally important. The technical aspects of privacy focus on the technical requirements (such as access control, data minimization) required to ensure privacy, while the social and organizational aspects focus on the relationships between people and how such relationships impact their privacy. Irwin Altman's privacy regulation theory (Altman, 1975) describes privacy as a dynamic, dialectic, and non-monotonic process involving interaction between people in a given context. Waldman (2014) identifies trust relationships between individuals as one of such important social aspects of privacy.

To provide a systematic setting to understand privacy expectations in a social context, Helen Nissenbaum (2009) proposed the theory of *contextual integrity*. In this theory, adequate protection of an individual's privacy is tied to the norms of specific contexts. More specifically, Nissenbaum argued that privacy can be achieved by governing the flow of personal information to ensure that data collection and dissemination are appropriate for a given context. When it comes to IoT, enabling contextual integrity as an underlying formalism becomes more challenging due to the pervasiveness, heterogeneity, large scale, and dynamism of IoT. In other words, it may be difficult to clearly articulate the norms that govern the flow of personal information as several and complex contexts are involved. For instance, *human activity recognition* (HAR) system (Stisen et al., 2015) which is a system for interpreting human motion (e.g. gestures or behaviors that are recorded by sensors) has been deployed in a wide range of domains, including smart homes (Pham & Olivier, 2009), healthcare (Taylor et al., 2020), fitness tracking (Buttussi & Chittaro, 2008) and transportation mode detection (Mantellos, Exarhos, & Christopoulou, 2020) among others. HAR systems are deployed on a large-scale and across heterogeneous devices (different device manufacturers, models, and OS types), and since new devices can be added to and removed from a large-scale IoT environment, they are recognized as high-dynamic systems (Cicirelli et al., 2017). Large-scale IoT environments are open and dynamic systems typically extending over a wide area and including a large number of heterogeneous interacting devices. During the development of these systems, several issues have been raised, such as security (e.g., threats to confidentiality, lack of effective authentication mechanism)

(Tewari & Gupta, 2020), privacy (e.g., difficulty in keeping distributed policies up-to-date and revoke them when necessary) (Sengul, 2017), interoperability and lack of standards.

The norms governing the flow of information within these large-scale IoT-based systems may also be uncertain, incomplete, conflicting and controversial (Ogunniye & Kökciyan, 2021). These norms might need to be explained to the involved entities in a given context or be argued about. In such a context, there is a need for communication between entities (human or devices). Communication is essential to resolve differences and conflicts of opinions and arrive at an agreed conclusion, work together towards solving a problem or finding a proof, or simply inform each other of pertinent facts about the topic of discussion.

2.2 Privacy Risks in IoT and Privacy Requirements

The rapid adoption of IoT technology in various domains, including health, manufacturing, agriculture, and transportation, has numerous implications for privacy (Schaub, Könings, & Weber, 2015). IoT generates high-volume streams of heterogeneous yet correlated contextual information of varying quality and complexity (Kishore Ramakrishnan et al., 2014). For example, IoT technologies such as wearable devices (e.g., Apple iWatch, Google Glass, Google Fit, and Apple Home Kit) collect people's sensitive information, from financial status to health conditions, by observing their daily activities (Perera et al., 2015). Wearable fitness trackers are the most widely diffused and adopted IoT-based devices (Kao, Nawata, & Huang, 2019) and are capable of collecting rich contextual information about users and use it to provide personalized recommendations (Ometov et al., 2021). These devices can monitor or track some form of fitness parameters (e.g., number of steps taken in a specific time period, distances covered, average speed, calories burned, heart rates, and sleep quality) of the person who wears them (Kao et al., 2019) and provide seamless integration with online social networks (Zhou & Piramuthu, 2014). Furthermore, the outbreak of COVID-19 has tremendously impacted the evolution of wearable devices, driven by the implementation of various crowd-sourcing and contact-tracing platforms (Ometov et al., 2021). Similarly, in a smart home environment, sensors and connected devices collect user personal information, such as location and behaviour. These devices can send the information gathered to the servers that communicate with them using mobile communication channels (Kumar & Patel, 2014). In communication protocols, transmitted information may exceed the physical boundaries of smart homes and therefore is easier to eavesdrop (Geneiatakis et al., 2017).

Beyond disclosing and sharing private information; IoT devices can perform actions in the user's environment that impact and potentially disturb the user while invading their privacy (Schaub et al., 2015). For example, an insecure camera-equipped household robot could be exploited to gain access to sensitive user data. Household robots, such as CareO-Bots[1] are used to perform household tasks and provide mobility assistance (Clark, Doran, & Andel, 2017). These robots can collect and share information, move through personal spaces and territories, and interact with people socially (Rueben et al., 2018; Calo, 2011). Therefore, malicious entities can exploit security and privacy vulnerabilities in the hardware and software components of these robotic systems to gain access to the sensitive data of their users and violate their privacy (Cottrell et al., 2021; Rueben et al., 2018).

1. https://www.care-o-bot.de/en/care-o-bot-4.html

Privacy requirements specify the capabilities and functions that a system must perform to protect the personal data of end users and to empower them with the control of their data. These requirements are generally based on fundamental privacy objectives specified in the relevant privacy regulatory policy or guidance, such as GDPR (Voigt & Von dem Bussche, 2017). Importantly, privacy requirements are fundamental requirements at the start of any IoT service-design process (Macaulay, 2016). Gharib et al. (2020) highlighted some of the causes of privacy breaches, including lack of appropriate security policies, bad practices, attacks, data theft, etc. According to them, most of the existing work on privacy requirements deals with them either as generic non-functional requirements with no specific techniques on how such requirements can be met (Mouratidis & Giorgini, 2007) or as security requirements, focusing mainly on confidentiality (Kalloniatis, Kavakli, & Gritzalis, 2008). To mitigate privacy breaches in IoT applications, it is important to develop objective and measurable privacy requirements. In the literature (Gharib et al., 2020; Mozzaquatro, Jardim-Goncalves, & Agostinho, 2015), privacy requirements (such as access control, anonymity, pseudonymity, and confidentiality, among others) have been implemented in sociotechnical systems to mitigate privacy breaches.

2.3 IoT Ontologies to Represent Privacy Requirements

The semantic representation of privacy requirements is a crucial step in developing future AI-based privacy assistants. Structured information is useful for privacy assistants to automatically resolve user contexts, meet privacy requirements, and prevent privacy violations as much as possible. An ontology is a formal model to represent knowledge in a specific domain (McGuinness et al., 2004); and ontologies have proven to be a key success factor in representing privacy requirements, as they facilitate the understanding of privacy-related concepts between designers and stakeholders of sociotechnical systems (Dzung & Ohnishi, 2009; Schaub et al., 2015; Uschold & Gruninger, 1996). There are a wide variety of ontologies (Agarwal et al., 2020; Arruda & Bulcão-Neto, 2019; Gharib et al., 2020) that represent privacy requirements in IoT systems. Most of these ontologies have focused on the technical aspects of privacy requirements such as access control, data minimization, confidentiality, and accountability, among others. However, in addition to these existing requirements, modelling of further requirements is required, as we identify in this research.

2.4 Modelling Trust in IoT

Trust is an important factor that affects how people make privacy decisions. For example, people are more likely to interact with devices they trust. Several works in the literature focus on modeling trust from different perspectives. According to Urbano et al. (2013), each time an individual (hereafter named truster) needs to interact with or rely on the intention of another individual, group or thing (hereafter named trustee), a decision about trust is made. Trust is a social construct that is necessary in our daily life (Urbano et al., 2013; Pinyol & Sabater-Mir, 2011), and is a mechanism used to manage uncertainty about autonomous entities and the information they deal with (Tang, Cai, McBurney, Sklar, & Parsons, 2011). Trust plays an important role in any decentralized system in controlling user interactions and, in particular, is used to protect users from fraudulent and malicious entities (Parsons et al., 2014; Pinyol & Sabater-Mir, 2011).

We follow the work of Paglieri et al. (2014) and Urbano et al. (2013) to conceptualize the notion of trust to evaluate the trustworthiness of trustees according to two trust dimensions.

1. Direct trust occurs as a result of interacting directly with the trustee, and the truster has a reasonable level of perception of the different trust features of the trustee's trustworthiness. These dimensions can be: (i) Competence: the extent to which the trustee is deemed able to make an accurate use of the truster's data. The notion of accuracy is as defined in Section 4. (ii) Sincerity: the extent to which the trustee is considered willing to make an accurate use of the truster's data. (iii) Fairness: the extent to which the trustee is considered willing to make a fair use of the truster's data. Fairness assessment could mean the extent to which the truster thinks that the trustee will not use its data for biased or discriminatory purposes (Ogunniye et al., 2021). For example, an individual (truster) may not be willing to share its data with another individual, group, or thing (trustee) that will use the data for racial discrimination or ethnic profiling. (iv) Reliability: the extent to which the trustee is deemed reliable to keep the truster's data safe from vulnerabilities and attacks. (v) Transparency: the extent to which the truster understands what the trustee is doing with its data (c.f., the definition of transparency in Section 4). (vi) Compliance: to what extent is the trustee willing to comply with relevant privacy policies and guidelines (e.g., GDPR).

2. Reputation (indirect trust) is used to compute an aggregated rating of trustee's trustworthiness by collecting information from different individuals or groups, and a truster can rate the trustworthiness of a trustee accordingly.

Existing trust models fall short in modelling trust in the IoT domain (Kökciyan & Yolum, 2020). These models rely heavily on positive and negative experiences with entities. However, in large-scale IoT environments (Cicirelli et al., 2017), a user interacts with a large number of devices (and rarely with the same devices), making it difficult to build an experience base per entity (Kökciyan & Yolum, 2022). Using indirect trust is also not feasible since privacy is subjective and should be modeled per individual.

3. Research Methodology

We do a systematic review of the privacy requirements and methods in state-of-the-art IoT ontologies using the *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA) framework. The PRISMA framework was designed to help reviewers report why the review was done, what the authors did to complete the review and what they found as a result of the review (Page et al., 2021). The framework includes methods for identifying, selecting, assessing, and synthesizing studies. We follow the PRISMA framework to specify our information sources, search strategy, selection process, inclusion and exclusion criteria, data collection process, and qualitative synthesis. More specifically, our methodology is as follows: i) we do a systematic search to identify research papers (surveys and literature reviews) that focus on modelling privacy requirements, ii) we select the research papers that fulfill our predefined selection criteria, and iii) we analyze and present the included research papers in a systematic way and discuss our findings. Figure 2 shows our methodology consisting of three main steps: *Search*, *Analysis*, and *Classification*. The classification step will be discussed in Section 4.

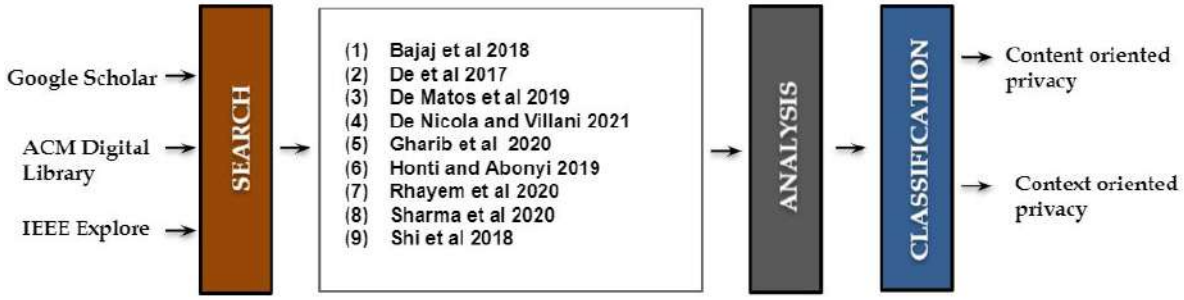

Figure 2: Research Methodology in Three Steps

3.1 Search

We review existing survey papers to extract an exhaustive list of IoT ontologies used in the literature. The search process requires a systematic narrowing of relevant survey papers given a set of input search terms and databases. Our selection is based on three main criteria: (i) the survey must be *up-to-date*, therefore, we consider surveys published from 2017 upward, (ii) the survey provides an overview of *at least five existing IoT ontologies* and some insight into privacy requirements such as data collection and retention, data integrity and user privacy expectations and preferences, among others, as well as the privacy methods adapted in the IoT ontologies, and iii) the survey must be a *peer-reviewed* publication. In this step, we first apply a keyword-based search to identify relevant papers. We then use a filtering technique to select a subset of surveys based on our selection criteria.

1. *Keyword-search:* We use three academic databases including *Google Scholar*, *ACM Digital Library* and *IEEE Explore* to review the available survey papers. Google Scholar provides a widely used platform that is used to discover the scholarly literature across an array of academic databases. IEEE Explore and ACM Digital Library helped us identify additional survey papers. We used a combination of search keywords consisting of '("IoT" OR "sensor" OR "smart device") AND "ontology" AND ("survey" OR "literature review")'. We used boolean 'AND' to link the major terms, and we used the boolean 'OR' to incorporate alternative synonyms of such terms.

2. *Filtering:* We filtered the survey papers by publication date to select recent surveys. We then checked the title and abstract information of those papers and removed those that did not discuss privacy in the IoT domain. Finally, we reviewed the remaining papers to check whether they meet all of our selection criteria. Our search strategy resulted in the nine survey papers listed in Figure 2.

3.2 Analysis

We carried out a systematic review of the selected survey papers based on the following criteria: (i) scope and contribution, (ii) analysis of the discussed ontologies in terms of their characterization, privacy requirements and methods adapted to preserve privacy, and (iii) conclusions, open questions and future trends in the state-of-research of ontologies for IoT. This analysis helps to understand the privacy requirements and methods that have been

SID	Reference	Type, Publisher	No of ontologies	Focus of Survey
S1	(Bajaj et al., 2018)	Journal, IEEE	32	Studied existing IoT ontologies by means of *core concepts* such as sensor-capabilities and context-awareness. Identified the core concepts required for developing an IoT application.
S2	(De, Zhou, & Moessner, 2017)	Book Chapter, Morgan Kaufmann	55	Presented a taxonomy and survey of the state-of-the art in Web of Things (WoT). Provided an analysis of *cross-domain ontologies of WoT elements* such as device, entity, service location and *domain-specific ontologies of WoT application areas* classified into environmental and user-oriented areas.
S3	(de Matos *et al.*, 2020)	Journal, Elsevier	10	Examined the requirements for sharing context information.
S4	(De Nicola & Villani, 2021)	Journal, MDPI	67	Investigated how and to what extent ontologies have been used to support smart city services. Identified what the current challenges for further development are.
S5	(Gharib *et al.*, 2020)	Journal, Springer	10	Carried out systematic review of privacy-related concepts and developed an ontology for privacy requirements.
S6	(Honti & Abonyi, 2019)	Journal, Wiley	34	Provided an overview of IoT semantics both technologies and models to support sensor network and IoT solution design.
S7	(Rhayem *et al.*, 2020)	Journal, Elsevier	23	Investigated and analysed the semantic-based approaches for IoT domain representation.
S8	(Sharma *et al.*, 2020)	Conf. Proc., Springer	-	Compared state-of-the-art solutions for IoT on privacy security and trust.
S9	(Shi et al., 2018)	Journal, MDPI	10	Provided a general overview of representing data semantically in IoT and make comparison between different ontology models and automatic tools.

Table 1: Overview of the survey papers included in the survey.

developed in the state-of-the-art of ontologies for IoT and to identify the open issues that need to be addressed. Table 1 shows an overview of the selected surveys. The table includes the serial number we give to each of the surveys, their references, the peer-reviewed venues where they were published, the number of ontologies reviewed by each of the surveys, and the focus of each of the surveys.

4. Classification of Privacy Requirements in IoT

In this section, we highlight the privacy requirements captured in existing IoT ontologies to mitigate privacy breaches, which are mainly focused on the technical aspects of privacy.

We will define new privacy requirements in Section 5, which are important to capture the social and organizational aspects of privacy.

Based on the systematic analysis of the survey papers that we carried out, we classified the privacy requirements in IoT into two broad categories, *content-oriented* and *context-oriented* privacy. Content-oriented privacy requirements focus on informational privacy, which is concerned with controlling whether and how personal data can be collected, stored, processed, and disseminated. These requirements are important to protect user data from malicious or unintended entities that could compromise the data. On the other hand, context-oriented privacy requirements focus on the privacy of a user, which involves protecting data that could be inferred as part of the user's context, such as the location and identity of the user. The context can be dynamic and indeterminate of what data can be shared about the user. For instance, it might not be acceptable to share a user's location information in an environment that exposes the user to danger. However, in some other situations, the context determines what data is to be shared about a user. In a medical context, it may be appropriate to share a patient's information with medical staff even without the explicit consent of the patient in an emergency (Nissenbaum, 2011).

4.1 Content-oriented Privacy Requirements

In the IoT domain, several content-oriented privacy requirements (Fernández et al., 2020; Hassani et al., 2018; Schwee et al., 2019) have been implemented to enforce information privacy. These requirements specify i) who can access what data, ii) constraints on what legitimate users can do with the data they have access to, who they can share the data with, how long they can retain data, and so on, and iii) the mechanisms to minimize vulnerabilities and attacks on data. For example, in the context of the Internet of Healthcare Things (IoHT), smart IoHT devices, such as smart watch, motion sensor, BP monitor, and insulin pump, are used to monitor, process, store, and transmit sensitive information (Shahid et al., 2022). In this context, content-oriented requirements are required to ensure that patient information is protected from inappropriate disclosure. However, these requirements are not enough to ensure privacy, as an adversary can identify a patient's disease based on the identity of the corresponding doctor (Boussada et al., 2019). Context requirements such as patient/doctor anonymity and unlinkability can be employed to mitigate this problem, as discussed in Section 4.2.

Alqassem and Svetinovic (2014) define some content-oriented requirements such as access control and data integrity. According to them, access control is necessary to prevent unauthorized access to data and to ensure that authorized entities can only access the data they are allowed to access. They identified the attributes of access control such as authentication and authorization. *Authentication* is central to the security of any system. It entails verifying the identity of a system user to indicate that the user is who he/she claims to be. *Authorisation* is the process of granting, denying, or limiting access to data. Since access control deals with both the identification/verification of the identities of IoT users and the prevention of unauthorized access to data, we classify it as both content-oriented and context-oriented requirements. Access control is needed to recognize and protect the identities of IoT systems/users from privacy and security breaches. Identity is the distin-

guishing character or personality of an individual or a system. Data integrity is needed to ensure the correctness of data and protect it from loss or corruption.

Agarwal et al. (2020) developed an ontology where they define some GDPR-inspired, General Data Protection Regulation (Voigt & Von dem Bussche, 2017), content-oriented privacy requirements that are related to IoT data flow (such as sharing and collection of data) as follows: (i) *Consent and choice:* The explicit consent of a data subject[2] should be sought before data is collected. The data subject should also have a choice to allow (resp. disallow) such data collection and be able to withdraw its consent at a later stage. (ii) *Data minimization:* Only the minimum amount of necessary data should be collected and processed. (iii) *Accuracy and quality:* The collected data must be accurate and up-to-date. False/incorrect data should be deleted or rectified.

Similarly, in their ontology, Arruda and Bulcao-Neto (2019) define some content-oriented privacy requirements as follows: (i) *Data sharing:* A data subject should be able to specify a set of purposes for which access to its information is granted or denied and who should be granted/denied access. (ii) *Data retention:* A data subject should be allowed to specify the maximum retention time of its data. (iii) *Data usage:* A data subject should be able to request records on how its data were used. (iv) *Temporal/time requirements:* Temporal information should be recorded/deleted as at when due. Additionally, the data subject should be able to set the time intervals in which its data are to be collected/deleted. (v) *Redress requirements:* There should be a complaint and redress mechanism in case of privacy violation.

Furthermore, Gharib et al. (2020) define some content-oriented privacy requirements as follows: (i) *Confidentiality:* This means that personal information should be kept secure from potential leaks or improper access. They break this requirement into the following principles: (i.a) *Non-disclosure:* A personal information can only be disclosed if the owner's consent is provided. It means that a data subject is in control of the disclosure of his/her data. (i.b) *Need to Know:* An actor[3] should only use information if it is strictly necessary to complete a certain task. This principle states that an actor shall only have access to the information that their job function requires, regardless of their security clearance level or other approvals. (i.c) *Purpose of Use:* This represents a purpose-binding principle, where information is only used for a specific purpose. (ii) *Notice and access:* A data subject should be notified when his/her information is being collected. The data subject should be able to access its data and delete them when they wish.

4.2 Context-oriented Privacy Requirements

In the IoT domain, several context-oriented privacy requirements (Bauer et al., 2013; Liu & Julien, 2015; Skillen et al., 2012) have been implemented to protect user privacy. In their systematic review, Gharib et al. (2020) identified some concepts and relationships for context-oriented privacy requirements as follows: (i) *Anonymity:* The identity of a data subject should not be identifiable within a set of other subjects, that is, a data subject cannot be sufficiently identified by others. This requirement might be implemented if the primary/secondary identifier of a data subject (e.g., name, social security number, address,

2. A user whose data is being collected/requested/shared
3. An actor represents an autonomous entity that performs tasks to achieve specific goals.

etc.) is removed or substituted. (ii) *Unlinkability:* This means that it should not be possible to link personal information back to its subject, that is, any information that allows such linkage should be removed. (iii) *Undetectability and Unobservability:* These are intended to hide activities (e.g., use of a resource or service) that are performed by a data subject, that is, the identity of a data subject should not be observed by others while performing an activity. For example, in an IoHT context,the data collected by IoHT devices are transmitted to the cloud service, or a remote server designed for intensive processing tasks using different communication protocols such as IEEE 802.15.6, IEEE 802.15.1 Bluetooth, and IEEE 802.11 WiFi (Shahid et al., 2022). Context-oriented requirements are required to ensure that an attacker cannot confirm whether a patient is communicating or not. Indeed, the presence of patient communication can reveal the existence of a patient's disease. (iv) *Transparency:* A data subject should be able to know who uses its information and for what purposes. The data subject should have full control over its data, know who has accessed them in the past, and, in general, know who has access to them. (v) *Accountability:* Information owners should have a mechanism available to hold information users accountable for their actions concerning information. This requirement relies on two principles: (v.a) *Non-repudiation:* The delegator cannot repudiate he/she delegated; and the delegatee cannot repudiate he/she accepted the delegation. (v.b) *Non-re-delegation:* The delegatee is requested by the delegator not to redelegate the delegatum, that is, the redelegation of a goal/permission is forbidden.

Furthermore, with the rapid development of IoT devices and smartphones with built-in Global Positioning System (GPS), location-based privacy requirements are needed to make users' location (un)detectable in certain contexts. According to Sun et al. (2017), when using location-based services (LBS), an adversary can not only link a user's identity with a location, but can also infer more private information about the user. For example, if an undercover police officer often reveals its location near a police station when using an LBS application, the location information could be used by an adversary to conjecture that the user may be a police officer. Additionally, as a large amount of data from different sources are gathered and processed, there are associated risks that may have a significant impact on informational and user privacy. For instance, an untrusted LBS having all information about users, such as their identities may use the information to track users in all kinds of ways or reveal their personal data to third parties. Risk requirements are important to mitigate these types of risk. *Risk* requirements ensure that users and their data are protected from vulnerabilities and attacks.

4.3 Analysis of the Selected Ontologies

We provide an analysis of the 36 selected ontologies from the nine survey publications that we considered in Table 1. We consider the following criteria in our comparison:

- *Ontology:* This criterion specifies the name (resp., reference) of the ontology under consideration.
- *Description of the ontology:* This criterion describes the ontology under consideration.
- *Survey Publication(s):* This criterion specifies the survey publication(s) that refers to the ontology under consideration.

- *Privacy Requirements:* This criterion specifies the privacy requirements the ontology under consideration has captured.

Table 2 shows a review of privacy requirements in existing IoT ontologies and helps to identify key privacy requirements. For example, IoT-A was published in 2013 by Bauer et al. (2013). This ontology focuses on defining concepts relevant to IoT Architecture Reference Model. The ontology appears in three of the survey papers ([S1], [S2], [S7]) we reviewed, and it implemented identity and location requirements.

Reusability: Unlike IoT sensor ontologies (Compton et al., 2012; Gyrard et al., 2014b; Shi et al., 2012; Janowicz et al., 2019) where the extensibility and reusability of existing ontologies are common, we observe that most of the IoT privacy ontologies analyzed were developed from scratch. Therefore, we did not include this criterion in the table. $DS4IoT$ (Gonzalez-Gil, Martinez, & Skarmeta, 2020) reused concepts from $STAC$ (Gyrard, Bonnet, & Boudaoud, 2014a), $IoTSECEv$ (Gonzalez-Gil, Skarmeta, & Martinez, 2019) and $IoT-Priv$ (Arruda & Bulcão-Neto, 2019). $IoTSecEv$ (Gonzalez-Gil et al., 2019) reused concepts from $IoTSec$ (Mozzaquatro et al., 2015)/ $COPri$ (Gharib et al., 2020) reused concepts from Pri (Kalloniatis et al., 2008). $IoT-OAS$ (Cirani et al., 2014) reused concepts from $CoAP$ (Pereira, Eliasson, & Delsing, 2014).

Ontology & Reference	**Description**	**Survey publication(s)**	**Requirements**
COBRA-ONT (Chen et al., 2003)	An ontology for reasoning about contextual information.	[S1], [S9]	Identity. Location. Time.
(Kim & Kim, 2015)	An ontology for reasoning about location information.	[S1]	Location.
TimeML (Pustejovsky et al., 2003)	An ontology to query specific data based on duration, events, granularity and instant.	[S1]	Time.
STAR-CITY (Lecue et al., 2014)	An ontology for semantic (road) transport analytics and reasoning for city.	[S1]	Data collection. Time.
IoT-A (Bauer et al., 2013)	An ontology to define concepts for devices, services, contexts, and information for the IoT Architecture Reference Model.	[S1],[S2], [S7]	Identity. Location.
(Chahuara et al., 2013)	An ontology for home automation.	[S2]	Identity. Time. Risk. Location.
(De et al., 2011)	An ontology for describing IoT components and data description models.	[S2]	Access control. Location. Identity.

(Continued on next page)

Table 2 (cont.)

Ontology & Reference	**Description**	**Survey publication(s)**	**Requirements**
iHSF (Ibrar et al., 2020)	An ontology for intelligent home service framework.	[S2]	Data collection. Location.
(Skillen et al., 2012)	An ontology for providing personalised, context-aware assistance services for users in mobile environments.	[S2]	Identity. Location.
ACC (Ricci et al., 2004)	An ontology for application context and the interaction between agents and the environment in Multi-Agent Systems (MASs).	[S3]	Access control.
Djess (Cabitza & Dal Seno, 2005)	An ontology for context between entities.	[S3]	Identity. Transparency.
Bluewave (Freitas et al., 2016)	Bluetooth-based technique that makes possible nearby mobile devices to share their context.	[S3]	Identity. Accuracy. Temporal.
ST-TSDB (Zeng et al., 2019)	Tool suite for data management in IoT.	[S3]	Time.
SharedLife (Kroner et al., 2009)	An ontology to share information of users between different applications and/or other users	[S3]	Identity. Access control. Time.
Magpie (Liu & Julien, 2015)	Trust-adaptive and privacy-preserving approach for context-sharing applications.	[S3]	Trust.
CoaaS (Hassani et al., 2018)	An ontology to exchange context information in the IoT environment.	[S3]	Access control.
(Schwee et al., 2020)	An ontology to prevent privacy vulnerability when sharing a dataset.	[S4]	Data sharing. Data usage. Risk.
SPECIAL (Fernandez et al., 2020)	An ontology to represent data usage policies in line with GDPR.	[S4]	Data usage. Data collection. Data sharing.
DS4IoT (Gonzalez-Gil et al., 2020)	An ontology to represent the secure data.	[S4]	Access control.
STAC (Gyrard et al., 2014)	An ontology to choose security mechanisms to secure IoT.	[S4], [S7]	Risk.
IoTSecEv (Gonzalez-Gil et al., 2019)	An ontology for IoT Context-Based Security Evaluation.	[S4]	Risk. Access control.

(Continued on next page)

Table 2 (cont.)

Ontology & Reference	Description	Survey publication(s)	Requirements
IoTSec (Mozzaquatro et al., 2015)	An ontology for cybersecurity requirements.	[S4], [S7]	Confidentiality. Data integrity. Access control.
IoT-Priv (Arruda et al., 2019)	A lightweight privacy ontology for IoT concepts (e.g., devices, sensor and service).	[S4], [S5]	Access control. Data collection, usage, retention, and sharing. Redress. Time.
(Belaazi et al., 2016)	A formal ontology to enforce privacy compliance in access control policies.	[S5]	Access control. Data collection. Data sharing. Data usage. Data retention.
(Elahi et al., 2009)	An ontology to integrate vulnerabilities into security requirements.	[S5]	Risk.
LPL (Gerl et al., 2018)	An ontology to enforce privacy in line with GDPR.	[S5]	Identity. Data collection and retention.
COPri (Gharib et al., 2020)	A comprehensive ontology for privacy requirements.	[S5]	Access control Confidentiality. Notice. Anonymity Unlinkability. Unobservability. Transparency. Accountability.
PriS (Kalloniatis et al., 2008)	An ontology to incorporate basic privacy requirements into system design process.	[S5]	Same as COPri.
Ontonym (Stevenson et al., 2009)	A set of ontologies that represent core concepts in pervasive computing.	[S6]	Temporal/Time. Identity. Location.
LIoPY (Loukil et al., 2018)	An ontology to incorporate privacy legislation into privacy policies.	[S5], [S7]	Access control.
PrOnto (Palmirani et al., 2018)	A privacy ontology that models the GDPR main conceptual core.	[S5]	Data processing.
(Dsouza et al., 2014)	A policy-driven security management approach for privacy.	[S8]	Access control.
IoT-OAS (Cirani et al., 2015)	An ontology for an external authorisation service.	[S8]	Access control.

(Continued on next page)

Table 2 (cont.)

Ontology & Reference	**Description**	**Survey publication(s)**	**Requirements**
CoAP (Pereira et al., 2015)	A framework for service-level access control.	[S8]	Access control.
(Abie & Balasingham , 2012)	A risk-based adaptive security framework for IoTs in eHealth.	[S8]	Risk.
SOUPA (Chen et al., 2004)	An ontology to represent intelligent agents with associated beliefs, desires, and intentions, time, space, events, user profiles, actions , and policies for security and privacy.	[S9]	Access control.

Table 2: Analysis of selected IoT ontologies

5. New Privacy Requirements for IoT

Our analysis suggests that the survey closest to ours is provided by Gharib et al. (2020). Their survey identified a wide range of privacy concepts and relationships in the literature. However, unlike our survey, they do not cover the new privacy requirements identified in our research. These new requirements are important to extend existing IoT ontologies with the social and organizational aspects of privacy, as we discuss here. As mentioned earlier, our idea of social requirements builds on the theory of contextual integrity (Nissenbaum, 2009) and Altman's privacy regulation theory (1975). These theories model the dynamism of privacy contexts and privacy policy. Here, social requirements are introduced to model privacy in terms of relationships and communication between IoT entities (human or devices).

We will use Example 1 to demonstrate how one could benefit from modelling our proposed new privacy requirements. Important features are underlined such as a human agent (Bob), an IoT entity (smartwatch), a data type (electronic health records), a context (emergency), or a retention policy (deactivation of an account). Note that all these features can influence the privacy decision to be made.

5.1 REQ1: Privacy Dynamics

User contexts are dynamic; hence, user privacy preferences and expectations should be modelled as *dynamic processes*.

In Example 1, there are three user contexts: *health*, *emergency*, and *crime prevention*. Bob's privacy preferences and expectations vary with these contexts. For example, in the context *crime prevention*, police may obtain Bob's location information from his smartwatch. This information will not be shared with Bob's brother based on Bob's privacy preferences. However, in the case of *emergency* where the smartwatch detects that Bob

has been immobile for about 30 minutes, the smartwatch can override Bob's privacy preference and place an automatic call to his brother to reveal his location if the brother is his emergency contact. Bob can also specify the retention time for certain personal data to be shared with other agents; however, this may not be the case in *crime prevention* context.

This example shows that identifying contexts is a complex and dynamic process. Understanding this process is essential to design context-adaptive privacy mechanisms to effectively support continuous and dynamic privacy regulation process (Schaub et al., 2015; Kökciyan & Yolum, 2020, 2022). When dealing with privacy dynamics, *timeframe* is an important concept that needs to be put into consideration. Timeframe (period of validity) is the length of time a privacy preference or a privacy obligation is valid: it could be a short or long period of time (see Section 4).

5.2 REQ2: Trust Dynamics

The decision of a data subject or data provider[4] to share particular data with a data requester/consumer[5] should be dependent on the *trust ratings* of the data requester/consumer.

To represent this requirement, the subject or data provider (hereby referred to as the truster) has the capacity to estimate the trust rating of the data requester/consumer (hereby referred to as the trustee) to take a decision on whether to share data with the data requester/consumer or not. In a context where the data subject or data provider lacks such capacity, it can rely on the trust assessment provided by a trusted third party on the data requester/consumer. Unlike traditional Web systems, such trust computation should be contextual to capture the dynamism inherent in IoT (Kökciyan & Yolum, 2020, 2022).

The example above shows that Bob is willing to share data with different agents with varying degrees of trust. Some agents may be malicious or incompetent, and data requests from such agents should be discounted. For example, Bob may feel comfortable sharing his health record with his doctor (who he trusts to handle such data), but not his financial data (which may not be appropriate in the healthcare context).

5.3 REQ3: Privacy Dialogue

A *privacy dialogue* is defined as the communication between a data subject/provider and a data requester/consumer to resolve conflicts about privacy preferences and expectations.

Privacy dialogues between entities are effective to harmonise conflicting views and come up with the best views towards achieving the goals under consideration (Kökciyan et al., 2017; Baarslag et al., 2017; Kekulluoglu et al., 2018). Conflicts can arise from the privacy preferences of various parties. For instance, a third-party entity might request Bob's medical data to provide personalized medical service to him, but Bob might decline such request. In addition, there are many situations where an individual needs to collect some other individuals' preferences over privacy settings in order to decide what would be optimal for an individual and a group of individuals. The limited knowledge about the available options could also result in conflicting situations. For example, an individual may be willing to give up its medical data in return for personalised recommendations, while another individual may consider medical data as a commodity that should not be shared.

4. An agent (human or device) that possess a particular data being collected/requested/shared
5. An agent (human or device) that is requesting to access a particular data

5.4 REQ4: Privacy Explanation

We define a *privacy explanation* as an explanation from a data requester/consumer to a data subject or a data provider on *what*, *why* and *how* the data of a data subject are being collected and *who* the data are being shared with.

Like a privacy dialogue, an exchange of explanations about privacy preferences and expectations is essential to resolve conflicts of opinions. Explanations are important to improve users' understanding of privacy preferences and expectations to help them make informed decisions. Following Miller's definition of explainability (Miller, 2019), Mosca and Such (2021) define an explanation as a cognitive process, the abductive inference process that determines the causal attribution of a given event, and a social process, that is, the process of transferring knowledge between the explainer and the explainee. In the field of Explainable AI, explanations are used to make AI results more understandable to humans (Adadi & Berrada, 2018; Kiritchenko, Nejadgholi, & Fraser, 2021). In the literature, the concept of explainability has been defined in different ways. Abdul et al. (2018) relate the concept of explainability to transparency, interpretability, trust, fairness, and accountability, among others. Halpern and Pearl (2005) define a good explanation as a reason for a *why* question that provides information that goes beyond the knowledge of the individual asking the question.

6. A Taxonomy of IoT Privacy Requirements

After reviewing the existing privacy requirements and introducing the new ones, we now share a taxonomy of IoT privacy requirements. To obtain a basic understanding of the relationship between IoT privacy requirements, Figure 3 represents our proposed taxonomy. We classify IoT privacy requirements into two broad categories (context-oriented and content-oriented privacy requirements) and provide the subcategories as shown in Figure 3. Access control requirements and risk requirements are classified as both context-oriented and content-oriented requirements. Notice and access requirements are sub-requirements of data collection, data retention, data sharing, and data usage requirements. Likewise, direct trust requirements and reputation requirements are sub-requirements of trust requirements, where accountability, transparency, fairness, competence, and reliability requirements are sub-requirements of both direct trust and reputation requirements. The requirements in the existing IoT ontologies are in white-shaded rectangles, whereas the ones we proposed are in blue-shaded ones.

The proposed taxonomy provides a basis for organizing privacy requirements and would provide valuable input into the development of new privacy ontologies. For example, to develop an ontology for data collection, sub-requirements such as consent and choice, confidentiality, data minimization, notice and access, non-disclosure and need-to-know need to be taken into consideration. While our taxonomy serves a basis for organizing privacy requirements, we note that the taxonomy is not exhaustive and can be extended further.

7. Open Issues and Future Trends

We identify four future directions to represent IoT privacy requirements. As discussed earlier, the existing approaches in developing IoT privacy ontologies do not account for i)

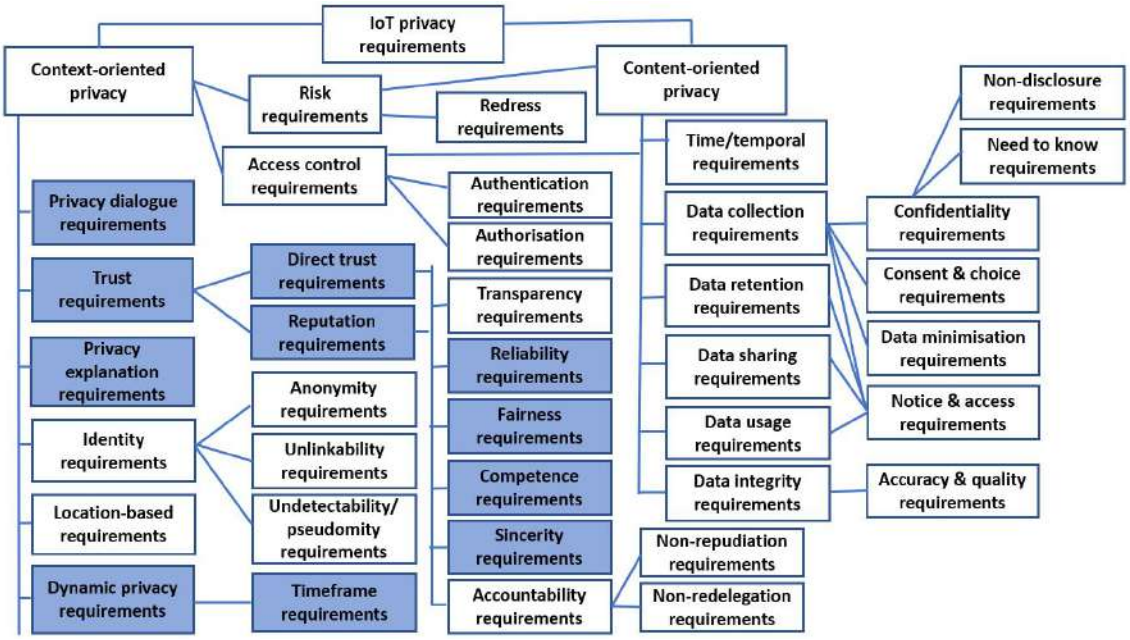

Figure 3: A Taxonomy of IoT Privacy Requirements.

privacy as a dynamically continuous process, ii) the diversity of privacy preferences and expectations and conflict resolution mechanisms to resolve conflicting privacy preferences and norms, iii) privacy as a dialectic and non-monotonic process, and iv) sociological aspects of privacy such as trust dynamics.

7.1 Privacy as a Dynamically Continuous Process

According to the privacy regulation theory of Altman (1975), the privacy expectations and privacy regulation behaviours are subject to dynamic adaptation processes. For example, in a smart home environment, a static privacy policy, applied throughout, would be either too invasive or too restrictive for the occupants due to their conflicting and ever-changing privacy preferences and the dynamic nature of their contexts. In this case, an automated system may continue to open doors for wrong people if the changing contexts of the occupants and their dynamic privacy preferences are not taken into consideration. To mitigate this privacy breach, a user's context can be mapped to appropriate privacy preferences and expectations. For example, what data about the user should be accessed at a given time. Once the context changes, privacy preferences and expectations should be updated.

In addition to changing users' contexts, there are other dynamic elements such as the functionalities and privacy policies of IoT devices that are constantly updated, the changing data requesters' or data consumers' contexts, and other contextual information, requiring dynamic updates of users' privacy preferences and expectations. To capture this dynamic process of privacy, we identify two key concepts (see Section 5.1). *Privacy dynamics* (dependent on context) and *timeframe* (the period of time that a privacy preference or obligation

is valid) requirements are important for the future design of context-adaptive privacy mechanisms for IoT systems.

7.2 Resolving Conflicting Privacy Preferences and Norms

Social norms play an important role in defining what individuals consider normal and acceptable (Williams, Nurse, & Creese, 2016). These norms differ between cultures, and as such, privacy perceptions have been shown to vary across the world (Daehnhardt, Taylor, & Jing, 2015; Williams et al., 2016). In their study of Twitter settings, Daehnhardt et al. (2015) revealed that the citizens of Japan were more private than those of Brazil or Spain. Individuals from 'Multi-active' societies are observed to be more likely to project their opinions than those from 'Reactive' cultures.

As conflicts may arise in individual and group privacy preferences and expectations due to differences in their individual, social, and cultural expectations and norms (Schaub et al., 2015), privacy policies should encode requirements for conflict resolution. These requirements are essential to elicit an optimal privacy policy for an individual user or a group of users in a given context. An optimal privacy policy is one that optimally protects the privacy preferences of an individual user and a group of users in a given context. Such requirements can also be learned automatically by developing privacy assistants that could adapt to their user behaviour in various contexts.

We note that various techniques have been developed to resolve conflicting privacy preferences in IoT: i) agent-based privacy negotiation models where an agent autonomously negotiates privacy agreements for users based on the learned preferences of actual users (Baarslag et al., 2017; Mohammad & Nakadai, 2019; Sanchez, Torre, & Knijnenburg, 2020), ii) privacy-utility trade-off mechanisms that consider profit and privacy trade-off (Krause & Horvitz, 2010; Fernandez, Jaimunk, & Thuraisingham, 2019; Mohammad & Nakadai, 2018) and agent-based privacy reasoning models (Kökciyan & Yolum, 2020, 2022). An avenue for the future is to integrate these techniques into IoT privacy ontologies for standardization.

7.3 Privacy as a Dialectic and Non-monotonic Process

Through a dialectical process of privacy regulation, individuals (playing different roles such as data subject, data processor, data consumer, etc.) can communicate and explain their privacy preferences to one another and seek to resolve the conflicts that may arise through any form of dialogue such as inquiry, negotiation, persuasion, or deliberation. There are different ways in which this type of dialogue can be implemented. One way is through an interactive user interface for an interaction with a user moderated by a software agent. From Example 1, an app for Bob's smartwatch with an interactive user interface to dialogue with other agents (human or artificial) can be installed on Bob's smartphone. Such a dialectical process is also useful for communication between end-users and vendors of IoT devices to enhance privacy agreements and privacy-utility trade-offs. In this case, non-monotonic reasoning (McCarthy, 1980; Reiter, 1987) is useful to capture and represent defeasible reasoning between these entities (i.e., a type of reasoning in which reasoners draw tentative conclusions, enabling reasoners to retract their conclusion(s) based on further evidence).

A popular AI approach for dialectical and non-monotonic reasoning is argumentation-based dialogues. Argumentation is a social process of reasoning to take a stand on whether to accept a disputable viewpoint or not by formulating propositions that are aimed at justifying (or refuting) the viewpoint. Argumentation provides a paradigm for reasoning in the presence of conflicts and uncertainties (Modgil et al., 2013). Argumentation frameworks have been used in various applications within multi-agent systems to enhance agents' communication (Amgoud, Maudet, & Parsons, 2002; Reed & Walton, 2005), collaborative intelligence analysis (Toniolo et al., 2015), trust reasoning (Ogunniye et al., 2017, 2018), ontological knowledge base querying (Croitoru et al., 2015), modeling dialogues (Amgoud et al., 2000; McBurney & Parsons, 2009), and decision making (Sklar et al., 2016) among others. Furthermore, argumentation frameworks have been used in legal theory and legal psychology (Bex et al., 2010).

We identify *privacy dialogue* and *privacy explanation* as important requirements to ensure communication between IoT entities about privacy policies and to resolve conflicts. Integrating argumentation-based dialogues into privacy policy reasoning to ensure communication between IoT entities is an avenue of future work.

7.4 Sociological Aspects of Privacy

In his article, Waldman (2014) argued that privacy contexts are defined by trust relationships between individuals. The author argues that privacy heavily depends on trust; and trust relationships are determined by the presence of experience, strong overlapping networks, and identity sharing among others.

We observe that modelling trust dynamics in the IoT domain is important for privacy policy reasoning. In a social interaction, people (perhaps subconsciously) decide to share their sensitive data with other entities (humans or devices), depending on the trust placed in the entities. For example, in a typical e-business scenario, trust in information sources has a strong influence on an agent's decision to buy or to sell a specific kind of stock. Indeed, to take such a decision, an agent may consult several types of information source (banks, companies, consultants, and so on) and may draw conclusions about the stock based on the degree of trust that it ascribes to the consulted sources. This problem of trust-based decision making has been studied by Lorini and Demolombe (2009) where trust is defined as the power, abilities, and disposition of an information source to provide information that is in line with the goals of the information receiver. According to Han and Liu (2012), IoT-based e-business process would enhance the e-business market by up to $2.5 billion in 2020. IoT systems are deployed to shape the business process in various industries such as transportation, manufacturing, healthcare, and agriculture (Bi et al., 2014; Ruan et al., 2020; Shoukry et al., 2021). However, in a typical IoT environment, data requests may originate from several sources with varying degrees of trustworthiness, for example, due to maliciousness, incompetence, etc. We note that existing IoT privacy ontologies have not captured this important aspect of privacy policies.

8. Conclusion

This survey presents a detailed analysis and classification of privacy requirements in the existing IoT ontologies. We first conducted a systematic review of nine recent surveys of

IoT ontologies that capture privacy requirements. Such a review will guide AI researchers who would like to represent privacy requirements semantically while automating the privacy decision-making process in the IoT domain. Our survey emphasizes the need for the reusability of IoT privacy ontologies, while clarifying the research gaps in the field of knowledge representation and reasoning. To achieve this, we share a list of new privacy requirements that should be captured in the ontologies to be developed. Additionally, these requirements need to be addressed to develop future AI-based privacy assistants to help humans, who clearly need help in their decision-making and to minimize privacy breaches in the IoT domain. Finally, we provide a broad classification of existing and new privacy requirements. This taxonomy is important to organize privacy requirements and will provide a shared understanding of privacy requirements among stakeholders in the IoT domain. Our next steps include the development of a new ontology to capture the social requirements identified in this survey. We will implement a conversational agent model (i.e., a privacy assistant) that uses ontologies to reason about data to make sharing decisions while incorporating the privacy preferences of the users and their feedback.

Acknowledgments

This research was funded by the UKRI Strategic Priorities Fund via the REPHRAIN research centre. The authors thank the members of the TULiPS lab for their feedback.

References

Abdul, A., Vermeulen, J., Wang, D., Lim, B. Y., & Kankanhalli, M. (2018). Trends and trajectories for explainable, accountable and intelligible systems: An hci research agenda. In *Proceedings of the 2018 CHI conference on human factors in computing systems*, pp. 1–18.

Adadi, A., & Berrada, M. (2018). Peeking inside the black-box: a survey on explainable artificial intelligence (xai). *IEEE access*, *6*, 52138–52160.

Agarwal, R., Elsaleh, T., & Tragos, E. (2020). Gdpr-inspired iot ontology enabling semantic interoperability, federation of deployments and privacy-preserving applications. arXiv preprint arXiv:2012.10314.

Alqassem, I., & Svetinovic, D. (2014). A taxonomy of security and privacy requirements for the internet of things (iot). In *2014 IEEE International Conference on Industrial Engineering and Engineering Management*, pp. 1244–1248. IEEE.

Altman, I. (1975). The environment and social behavior: privacy, personal space, territory, and crowding.. *Monterey, CA: Brooks/Cole Publishing*, *1*.

Amgoud, L., Maudet, N., & Parsons, S. (2000). Modelling dialogues using argumentation. In *MultiAgent Systems, 2000. Proceedings. Fourth International Conference on*, pp. 31–38. IEEE.

Amgoud, L., Maudet, N., & Parsons, S. (2002). An argumentation-based semantics for agent communication languages. In *ECAI*, Vol. 2, pp. 38–42.

Arruda, M. F., & Bulcão-Neto, R. F. (2019). Toward a lightweight ontology for privacy protection in iot. In *Proceedings of the 34th ACM/SIGAPP symposium on applied computing*, pp. 880–888.

Baarslag, T., Alan, A. T., Gomer, R., Alam, M., Perera, C., Gerding, E. H., & Schraefel, m. (2017). An automated negotiation agent for permission management. In *Proceedings of the 16th Conference on Autonomous Agents and MultiAgent Systems*, pp. 380–390.

Bajaj, G., Agarwal, R., Singh, P., Georgantas, N., & Issarny, V. (2018). 4w1h in iot semantics. *IEEE Access*, *6*, 65488–65506.

Bauer, M., Bui, N., De Loof, J., Magerkurth, C., Nettsträter, A., Stefa, J., & Walewski, J. W. (2013). Iot reference model. In *Enabling Things to Talk*, pp. 113–162. Springer, Berlin, Heidelberg.

Bex, F. J., Van Koppen, P. J., Prakken, H., & Verheij, B. (2010). A hybrid formal theory of arguments, stories and criminal evidence. *Artificial Intelligence and Law*, *18*(2), 123–152.

Bi, Z., Da Xu, L., & Wang, C. (2014). Internet of things for enterprise systems of modern manufacturing. *IEEE Transactions on industrial informatics*, *10*(2), 1537–1546.

Boussada, R., Hamdane, B., Elhdhili, M. E., & Saidane, L. A. (2019). Privacy-preserving aware data transmission for iot-based e-health. *Computer Networks*, *162*, 106866.

Buttussi, F., & Chittaro, L. (2008). Mopet: A context-aware and user-adaptive wearable system for fitness training. *Artificial Intelligence in Medicine*, *42*(2), 153–163.

Cabitza, F., & Dal Seno, B. (2005). Djess-a knowledge-sharing middleware to deploy distributed inference systems.. In *WEC (2)*, pp. 66–69. Citeseer.

Calo, M. R. (2011). 12 robots and privacy. *Robot ethics: The ethical and social implications of robotics*, *33*, 187.

Cicirelli, F., Guerrieri, A., Spezzano, G., Vinci, A., Briante, O., Iera, A., & Ruggeri, G. (2017). Edge computing and social internet of things for large-scale smart environments development. *IEEE Internet of Things Journal*, *5*(4), 2557–2571.

Cirani, S., Picone, M., Gonizzi, P., Veltri, L., & Ferrari, G. (2014). Iot-oas: An oauth-based authorization service architecture for secure services in iot scenarios. *IEEE sensors journal*, *15*(2), 1224–1234.

Clark, G. W., Doran, M. V., & Andel, T. R. (2017). Cybersecurity issues in robotics. In *2017 IEEE conference on cognitive and computational aspects of situation management (CogSIMA)*, pp. 1–5. IEEE.

Colnago, J., Feng, Y., Palanivel, T., Pearman, S., Ung, M., Acquisti, A., Cranor, L. F., & Sadeh, N. (2020). Informing the design of a personalized privacy assistant for the internet of things. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, p. 1–13.

Compton, M., Barnaghi, P., Bermudez, L., Garcia-Castro, R., Corcho, O., Cox, S., Graybeal, J., Hauswirth, M., Henson, C., Herzog, A., et al. (2012). The ssn ontology of the w3c semantic sensor network incubator group. *Journal of Web Semantics*, *17*, 25–32.

Cottrell, K., Bose, D. B., Shahriar, H., & Rahman, A. (2021). An empirical study of vulnerabilities in robotics. In *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, pp. 735–744. IEEE.

Croitoru, M., Thomopoulos, R., & Vesic, S. (2015). Introducing preference-based argumentation to inconsistent ontological knowledge bases. In *International Conference on Principles and Practice of Multi-Agent Systems*, pp. 594–602. Springer.

Daehnhardt, E., Taylor, N. K., & Jing, Y. (2015). Usage and consequences of privacy settings in microblogs. In *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, pp. 667–674. IEEE.

Dasgupta, A., Gill, A. Q., & Hussain, F. (2019). Privacy of iot-enabled smart home systems. In *Internet of Things (IoT) for automated and smart applications*, p. 9. IntechOpen.

De, S., Zhou, Y., & Moessner, K. (2017). Ontologies and context modeling for the web of things. *Managing the Web of Things*, *1*, 3–36.

De Nicola, A., & Villani, M. L. (2021). Smart city ontologies and their applications: A systematic literature review. *Sustainability*, *13*(10), 5578.

Dzung, D. V., & Ohnishi, A. (2009). Ontology-based reasoning in requirements elicitation. In *2009 seventh iEEE international conference on software engineering and formal methods*, pp. 263–272. IEEE.

Fernández, J. D., Sabou, M., Kirrane, S., Kiesling, E., Ekaputra, F. J., Azzam, A., & Wenning, R. (2020). User consent modeling for ensuring transparency and compliance in smart cities. *Personal and Ubiquitous Computing*, *24*, 465–486.

Fernandez, M., Jaimunk, J., & Thuraisingham, B. (2019). Privacy-preserving architecture for cloud-iot platforms. In *2019 IEEE International Conference on Web Services (ICWS)*, pp. 11–19. IEEE.

Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., & Baldini, G. (2017). Security and privacy issues for an iot based smart home. In *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 1292–1297. IEEE.

Gharib, M., Giorgini, P., & Mylopoulos, J. (2020). An ontology for privacy requirements via a systematic literature review. *Journal on Data Semantics*, *9*(4), 123–149.

Gheisari, M., Wang, G., Khan, W. Z., & Fernández-Campusano, C. (2019). A context-aware privacy-preserving method for iot-based smart city using software defined networking. *Computers & Security*, *87*, 101470.

Gonzalez-Gil, P., Martinez, J. A., & Skarmeta, A. F. (2020). Lightweight data-security ontology for iot. *Sensors*, *20*(3), 801.

Gonzalez-Gil, P., Skarmeta, A. F., & Martinez, J. A. (2019). Towards an ontology for iot context-based security evaluation. In *2019 Global IoT Summit (GIoTS)*, pp. 1–6. IEEE.

Gyrard, A., Bonnet, C., & Boudaoud, K. (2014a). An ontology-based approach for helping to secure the ETSI machine-to-machine architecture. In *2014 IEEE International*

Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom), pp. 109–116. IEEE.

Gyrard, A., Datta, S. K., Bonnet, C., & Boudaoud, K. (2014b). Standardizing generic cross-domain applications in internet of things. In *2014 IEEE Globecom Workshops (GC Wkshps)*, pp. 589–594. IEEE.

Halpern, J. Y., & Pearl, J. (2005). Causes and explanations: A structural-model approach. part ii: Explanations. *The British journal for the philosophy of science*, *56*(4), 889–911.

Han, J., & Li, Z. (2012). Constructing logistics e-commerce platform based on internet of things. *Value Engineering*, *31*(29), 183–185.

Hassani, A., Medvedev, A., Haghighi, P. D., Ling, S., Indrawan-Santiago, M., Zaslavsky, A., & Jayaraman, P. P. (2018). Context-as-a-service platform: exchange and share context in an iot ecosystem. In *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 385–390. IEEE.

Honti, G. M., & Abonyi, J. (2019). A review of semantic sensor technologies in internet of things architectures. *Complexity*, *2019*.

Janowicz, K., Haller, A., Cox, S. J., Le Phuoc, D., & Lefrancois, M. (2019). Sosa: A lightweight ontology for sensors, observations, samples, and actuators. *Journal of Web Semantics*, *56*, 1–10.

Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2008). Addressing privacy requirements in system design: the pris method. *Requirements Engineering*, *13*(3), 241–255.

Kao, Y.-S., Nawata, K., & Huang, C.-Y. (2019). An exploration and confirmation of the factors influencing adoption of iot-based wearable fitness trackers. *International journal of environmental research and public health*, *16*(18), 3227.

Kekulluoglu, D., Kökciyan, N., & Yolum, P. (2018). Preserving privacy as social responsibility in online social networks. *ACM Transactions on Internet Technology (TOIT)*, *18*(4), 42:1–42:22.

Kim, S. I., & Kim, H. S. (2015). Ontology based location reasoning method using smart phone data. In *2015 International Conference on Information Networking (ICOIN)*, pp. 509–514. IEEE.

Kiritchenko, S., Nejadgholi, I., & Fraser, K. C. (2021). Confronting abusive language online: A survey from the ethical and human rights perspective. *Journal of Artificial Intelligence Research*, *71*, 431–478.

Kishore Ramakrishnan, A., Preuveneers, D., & Berbers, Y. (2014). Enabling self-learning in dynamic and open iot environments. *Procedia Computer Science*, *32*, 207–214.

Kökciyan, N., Yaglikci, N., & Yolum, P. (2017). An argumentation approach for resolving privacy disputes in online social networks. *ACM Transactions on Internet Technology (TOIT)*, *17*(3), 27:1–27:22.

Kökciyan, N., & Yolum, P. (2020). Turp: Managing trust for regulating privacy in internet of things. *IEEE Internet Computing*, *24*(6), 9–16.

Kökciyan, N., & Yolum, P. (2022). Taking situation-based privacy decisions: Privacy assistants working with humans. In Raedt, L. D. (Ed.), *Proceedings of the Thirty-First International Joint Conference on Artificial Intelligence, IJCAI-22*, pp. 703–709. International Joint Conferences on Artificial Intelligence Organization. Main Track.

Krause, A., & Horvitz, E. (2010). A utility-theoretic approach to privacy in online services. *Journal of Artificial Intelligence Research (JAIR)*, *39*(1), 633–662.

Kumar, J. S., & Patel, D. R. (2014). A survey on internet of things: Security and privacy issues. *International Journal of Computer Applications*, *90*(11), 20–26.

Liu, C., & Julien, C. (2015). Pervasive context sharing in magpie: adaptive trust-based privacy protection. In *International Conference on Mobile Computing, Applications, and Services*, pp. 122–139. Springer.

Lorini, E., & Demolombe, R. (2009). From trust in information sources to trust in communication systems: an analysis in modal logic. In *Knowledge Representation for Agents and Multi-Agent Systems*, pp. 81–98. Springer.

Macaulay, T. (2016). Confidentiality and integrity and privacy requirements in the iot. *RIoT Control*, *1*, 125–139.

Mantellos, G., Exarhos, T. P., & Christopoulou, E. (2020). Human activity and transportation mode recognition using smartphone sensors. In *2020 5th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, pp. 1–7. IEEE.

McBurney, P., & Parsons, S. (2009). Dialogue games for agent argumentation. In *Argumentation in artificial intelligence*, pp. 261–280. Springer.

McCarthy, J. (1980). Circumscription—a form of non-monotonic reasoning. *Artificial intelligence*, *13*(1-2), 27–39.

McGuinness, D. L., Van Harmelen, F., et al. (2004). Owl web ontology language overview. *W3C recommendation*, *10*(10), 2004.

Miller, T. (2019). Explanation in artificial intelligence: Insights from the social sciences. *Artificial intelligence*, *267*, 1–38.

Modgil, S., Toni, F., Bex, F., Bratko, I., Chesñevar, C. I., Dvořák, W., Falappa, M. A., Fan, X., Gaggl, S. A., García, A. J., et al. (2013). The added value of argumentation. In *Agreement Technologies*, pp. 357–403. Springer.

Mohammad, Y., & Nakadai, S. (2018). Utility elicitation during negotiation with practical elicitation strategies. In *2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 3100–3107. IEEE.

Mohammad, Y., & Nakadai, S. (2019). Optimal value of information based elicitation during negotiation. In *Proceedings of the 18th International Conference on Autonomous Agents and MultiAgent Systems*, pp. 242–250.

Mosca, F., & Such, J. (2021). Elvira: an explainable agent for value and utility-driven multiuser privacy. In *International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, p. 916–924.

Mouratidis, H., & Giorgini, P. (2007). Secure tropos: a security-oriented extension of the tropos methodology. *International Journal of Software Engineering and Knowledge Engineering*, *17*(02), 285–309.

Mozzaquatro, B. A., Jardim-Goncalves, R., & Agostinho, C. (2015). Towards a reference ontology for security in the internet of things. In *2015 IEEE International Workshop on Measurements & Networking (M&N)*, pp. 1–6. IEEE.

Naeini, P. E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L. F., & Sadeh, N. (2017). Privacy expectations and preferences in an iot world. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, pp. 399–412.

Nissenbaum, H. (2009). *Privacy in context*. Stanford University Press.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32–48.

Ogunniye, G., & Kökciyan, N. (2021). Argumentation-based dialogues for privacy policy reasoning. In *The 3rd Annual Symposium on Applications of Contextual Integrity (2021)*. [Online; accessed 25-Nov-2021] url = https://edin.ac/3D8LuwC.

Ogunniye, G., Legastelois, B., Rovatsos, M., Dowthwaite, L., Portillo, V., Vallejos, E. P., Zhao, J., & Jirotka, M. (2021). Understanding user perceptions of trustworthiness in e-recruitment systems. *IEEE Internet Computing*, *25*(6), 23–32.

Ogunniye, G., Toniolo, A., & Oren, N. (2017). A dynamic model of trust in dialogues. In *International Workshop on Theorie and Applications of Formal Argumentation*, pp. 211–226. Springer.

Ogunniye, G., Toniolo, A., & Oren, N. (2018). Meta-argumentation frameworks for multi-party dialogues. In *PRIMA 2018: The 21st International Conference on Principles and Practice of Multi-Agent Systems*, p. 79. Springer.

Ometov, A., Shubina, V., Klus, L., Skibińska, J., Saafi, S., Pascacio, P., Flueratoru, L., Gaibor, D. Q., Chukhno, N., Chukhno, O., et al. (2021). A survey on wearable technology: History, state-of-the-art and current challenges. *Computer Networks*, *193*, 108074.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., et al. (2021). The prisma 2020 statement: an updated guideline for reporting systematic reviews. *Systematic reviews*, *10*(1), 1–11.

Paglieri, F., Castelfranchi, C., da Costa Pereira, C., Falcone, R., Tettamanzi, A., & Villata, S. (2014). Trusting the messenger because of the message: feedback dynamics from information quality to source evaluation. *Computational and Mathematical Organization Theory*, *20*(2), 176–194.

Parsons, S., Atkinson, K., Li, Z., McBurney, P., Sklar, E., Singh, M., Haigh, K., Levitt, K., & Rowe, J. (2014). Argument schemes for reasoning about trust. *Argument & Computation*, *5*(2-3), 160–190.

Pereira, P. P., Eliasson, J., & Delsing, J. (2014). An authentication and access control framework for coap-based internet of things. In *IECON 2014-40th Annual Conference of the IEEE Industrial Electronics Society*, pp. 5293–5299. IEEE.

Perera, C., Ranjan, R., Wang, L., Khan, S. U., & Zomaya, A. Y. (2015). Big data privacy in the internet of things era. *IT Professional*, *17*(3), 32–39.

Pham, C., & Olivier, P. (2009). Slice&dice: Recognizing food preparation activities using embedded accelerometers. In *European Conference on Ambient Intelligence*, pp. 34–43. Springer.

Pinyol, I., & Sabater-Mir, J. (2011). Computational trust and reputation models for open multi-agent systems: a review. *Artificial Intelligence Review*, *40*(1), 1–25.

Reed, C., & Walton, D. (2005). Towards a formal and implemented model of argumentation schemes in agent communication. *Autonomous Agents and Multi-Agent Systems*, *11*(2), 173–188.

Reiter, R. (1987). Nonmonotonic reasoning. *Annual Review of Computer Science*, *2*(1), 147–186.

Rodríguez-Rodríguez, I., Rodríguez, J.-V., Elizondo-Moreno, A., & Heras-González, P. (2020). An autonomous alarm system for personal safety assurance of intimate partner violence survivors based on passive continuous monitoring through biosensors. *Symmetry*, *12*(3), 460.

Ruan, J., Hu, X., Huo, X., Shi, Y., Chan, F. T., Wang, X., Manogaran, G., Mastorakis, G., Mavromoustakis, C. X., & Zhao, X. (2020). An iot-based e-business model of intelligent vegetable greenhouses and its key operations management issues. *Neural Computing and Applications*, *32*(19), 15341–15356.

Rueben, M., Aroyo, A. M., Lutz, C., Schmölz, J., Van Cleynenbreugel, P., Corti, A., Agrawal, S., & Smart, W. D. (2018). Themes and research directions in privacy-sensitive robotics. In *2018 IEEE workshop on advanced robotics and its social impacts (ARSO)*, pp. 77–84. IEEE.

Sanchez, O. R., Torre, I., & Knijnenburg, B. P. (2020). Semantic-based privacy settings negotiation and management. *Future Generation Computer Systems*, *111*, 879–898.

Schaub, F., Könings, B., & Weber, M. (2015). Context-adaptive privacy: Leveraging context awareness to support privacy decision making. *IEEE Pervasive Computing*, *14*(1), 34–43.

Schwee, J. H., Sangogboye, F. C., Johansen, A., & Kjærgaard, M. B. (2019). Ontology-based modeling of privacy vulnerabilities for data sharing. In *IFIP International Summer School on Privacy and Identity Management*, pp. 109–125. Springer.

Sengul, C. (2017). Privacy, consent and authorization in iot. In *2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN)*, pp. 319–321. IEEE.

Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data protection and privacy of the internet of healthcare things (iohts). *Applied Sciences*, *12*(4), 1927.

Shi, F., Li, Q., Zhu, T., & Ning, H. (2018). A survey of data semantization in internet of things. *Sensors*, *18*(1), 313.

Shi, Y., Li, G., Zhou, X., & Zhang, X. (2012). Sensor ontology building in semantic sensor web. In *Internet of things*, pp. 277–284. Springer.

Shirey, R. W. (2007). Internet security glossary, version 2. *RFC*, *4949*, 1–365.

Shoukry, A., Khader, J., & Gani, S. (2021). Improving business process and functionality using iot based e3-value business model. *Electronic Markets*, *31*(1), 17–26.

Sicari, S., Rizzardi, A., Grieco, L., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146 – 164.

Skillen, K.-L., Chen, L., Nugent, C. D., Donnelly, M. P., & Solheim, I. (2012). A user profile ontology based approach for assisting people with dementia in mobile environments. In *2012 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pp. 6390–6393. IEEE.

Sklar, E. I., Parsons, S., Li, Z., Salvit, J., Perumal, S., Wall, H., & Mangels, J. (2016). Evaluation of a trust-modulated argumentation-based interactive decision-making tool. *Autonomous Agents and Multi-Agent Systems*, *30*(1), 136–173.

Stisen, A., Blunck, H., Bhattacharya, S., Prentow, T. S., Kjærgaard, M. B., Dey, A., Sonne, T., & Jensen, M. M. (2015). Smart devices are different: Assessing and mitigatingmobile sensing heterogeneities for activity recognition. In *Proceedings of the 13th ACM conference on embedded networked sensor systems*, pp. 127–140.

Sun, G., Chang, V., Ramachandran, M., Sun, Z., Li, G., Yu, H., & Liao, D. (2017). Efficient location privacy algorithm for internet of things (iot) services and applications. *Journal of Network and Computer Applications*, *89*, 3–13.

Tanczer, L. M., López-Neira, I., & Parkin, S. (2021). 'i feel like we're really behind the game': perspectives of the united kingdom's intimate partner violence support sector on the rise of technology-facilitated abuse. *Journal of gender-based violence*, *5*(3), 431–450.

Tang, Y., Cai, K., McBurney, P., Sklar, E., & Parsons, S. (2011). Using argumentation to reason about trust and belief. *Journal of Logic and Computation*, *22*(5), 979–1018.

Taylor, W., Shah, S. A., Dashtipour, K., Zahid, A., Abbasi, Q. H., & Imran, M. A. (2020). An intelligent non-invasive real-time human activity recognition system for next-generation healthcare. *Sensors*, *20*(9), 2653.

Tewari, A., & Gupta, B. B. (2020). Security, privacy and trust of different layers in internet-of-things (iots) framework. *Future generation computer systems*, *108*, 909–920.

Tolmie, P., Crabtree, A., Rodden, T., Greenhalgh, C., & Benford, S. (2007). Making the home network at home: Digital housekeeping. In *ECSCW 2007*, pp. 331–350. Springer.

Toniolo, A., Norman, T. J., Etuk, A., Cerutti, F., Ouyang, R. W., Srivastava, M., Oren, N., Dropps, T., Allen, J. A., & Sullivan, P. (2015). Supporting reasoning with different types of evidence in intelligence analysis. In *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*, pp. 781–789. International Foundation for Autonomous Agents and Multiagent Systems.

Urbano, J., Rocha, A. P., & Oliveira, E. (2013). A socio-cognitive perspective of trust. In *Agreement Technologies*, pp. 419–429. Springer.

Uschold, M., & Gruninger, M. (1996). Ontologies: Principles, methods and applications. *The knowledge engineering review*, *11*(2), 93–136.

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (un) informed consent: Studying gdpr consent notices in the field. In *Proceedings of the 2019 Acm Sigsac Conference on Computer and Communications Security*, pp. 973–990.

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide* (1st edition)., Vol. 10. Springer Publishing Company, Incorporated.

Waldman, A. E. (2014). Privacy as trust: Sharing personal information in a networked world. *U. Miami L. Rev.*, *69*, 559.

Williams, M., Nurse, J. R., & Creese, S. (2016). The perfect storm: The privacy paradox and the internet-of-things. In *2016 11th International Conference on Availability, Reliability and Security (ARES)*, pp. 644–652. IEEE.

Zhou, W., & Piramuthu, S. (2014). Security/privacy of wearable fitness tracking iot devices. In *2014 9th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1–5. IEEE.