Argumentation-based Dialogues for Privacy Policy Reasoning

Argumentation-based Dialogues for Privacy Policy Reasoning

Gideon Ogunniye
University of Edinburgh
Edinburgh, United Kingdom
g.ogunniye@ed.ac.uk

Nadin Kökciyan
University of Edinburgh
Edinburgh, United Kingdom
nadin.kokciyan@ed.ac.uk

ABSTRACT

The scale, heterogeneity, pervasiveness and dynamism of Internet of Things (IoT) environments introduce some privacy issues for the users and those who are affected by the environments. This is because IoT systems rely heavily on collecting data; and the major areas of concerns include the potential impact of such information flow on the privacy of users. Recently, contextual integrity theory was developed to define context-relative norms for governing information flow. Context-relative norms are characterized by a situation's general institutional and social circumstances; the involved actors and their roles; the information being collected, processed, or shared; and the expected transmission principles. One key issue is that individual users may have varying preferences regarding data collection, retention time and who the collected data can be shared with. In this paper, we provide a motivation for a dialogue between agents (human or artificial) about privacy requirements. Therefore, we introduce an argumentation-based dialogue in which participants interact by exchanging arguments about privacy requirements. Our claim is that such dialogues could help agents in understanding the users' needs in this domain.

CCS CONCEPTS

• **Security and privacy → Privacy protections**; • **Computing methodologies → Cooperation and coordination**; **Multi-agent systems**.

KEYWORDS

contextual integrity, privacy, IoT, argumentation-based dialogues

ACM Reference Format:
Gideon Ogunniye and Nadin Kökciyan. 2021. Argumentation-based Dialogues for Privacy Policy Reasoning. In *CI Symposium '21: Symposium on Contextual Integrity, September 30–October 01, 2021, Chicago, USA*. ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

The Internet of Things (IoT) envisions the pervasive interconnection and cooperation of smart things over the current and future Internet infrastructure [43]. Kökciyan and Yolum [12] highlighted some of the important characteristics of IoT that set it apart from other computational systems in terms of privacy to include: *dynamism*: ever-evolving IoT entities with no central point of entry, *large scale*: the scale of IoT makes it infeasible to realise and maintain privacy policies, and, *heterogeneity*: IoT is a collection of heterogeneous technologies that function together from different vendors, installed for different reasons, having different capabilities and possibly being managed by different principals. Also, IoT generates high-volume streams of heterogeneous yet correlated contextual information of varying quality and complexity [11].

Indeed, IoT systems rely on ubiquitous data collection or tracking to operate, but these useful features also expose the IoT world to privacy breeches that can limit its vision. These systems often obtain users' data from their surrounding environment to provide useful services such energy saving, home automation, transportation and security among others. The perpetual collection of people's data evokes some privacy implications such as the actions and behaviours of the users being tracked, sensitive information about individuals being exposed, and situations where the collected data are not only being utilised by the technology itself but also by third parties such as businesses, hackers and governments [25].

Unlike Web systems like recommender systems where privacy settings are managed through well-defined policies and standard procedures, the pervasiveness, scale, dynamism and heterogeneity of the IoT systems make it impossible to specify privacy policies for all situations [13]. In IoT, users have varying privacy preferences and expectations. According to [22, 23], individual privacy expectations are highly contextualised and shaped by individual, social, and cultural expectations and norms. In view of this, the concept of *contextual integrity* was developed to define context-relative norms for governing information flow. These norms are characterized by a situation's general institutional and social circumstances; the involved actors and their roles; the information being collected, processed, or shared; and the expected transmission principles [31]. Depending on the context of the user, some information is appropriate (resp. inappropriate) to share. For example, lawyers and doctors are expected to keep information about their clients and patients confidential. However, in a medical emergency, it would be appropriate to share a patient's information with medical staff even if explicit consents were not given for each medical staff.

Because privacy expectations vary with context, there is a need for dynamic privacy decision-making process. According to [31], the goal of context-adaptive privacy mechanisms should be to predict and anticipate the user's privacy preferences for a specific change in context. Kökciyan and Yolum [13] argue that handling of privacy has to be reasoned by the IoT devices, depending on the norms, context, as well as the trust among entities. In this paper, we motivate the need for an argumentation-based dialogue between agents (human or artificial) to reason about privacy. *Computational argumentation* is a reasoning technique that put much emphasis on the importance of exchanging information and explanations

CI Symposium '21, September 30– October 01, 2021, Chicago, USA

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/10.1145/1122445.1122456

between participants in order to resolve differences and conflicts of opinions. An argumentation-based dialogue is useful to reason about users' context to capture the dynamic nature of privacy. In IoT, information (as well as information requests) may originate from sources (including IoT devices, software agents, human agents and such) who may be more or less trusted, which will impact the weight attributed to the information (as well as the requests), and will in turn affect the decision making process for information flow.

2 BACKGROUND

In this paper, we propose argumentation-based dialogues between agents to reason about context in a dynamic IoT environment, and we therefore begin by describing user context. Following this, we describe the components of an argumentation-based dialogue.

2.1 User Context

Because IoT devices perform actions in users' environment that potentially expose the users to privacy risks, it is imperative to incorporate users' context into the privacy decision-making processes of the devices. A user's context in this sense, encompasses user's location, the ambience, resources and people nearby, and the activities they are engaged in and other things of interest. User context is defined as information that describes the situation of a human user either directly or indirectly [32]. This context can be dynamic and indeterminate of what data to 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, context is determinate of what data to be shared about a user.

In addition to user's context, there are other dynamic elements such as the requester context, sources of contextual information which are of varying degrees of trust, the inherent complexity in the contextual information and the contextual norms guiding the appropriateness of information sharing among others that need to be taken into consideration for privacy decision making [10, 13].

2.2 Agent Communication

An important step towards ensuring contextual integrity is to allow for communication between agents (human or artificial). These agents must communicate to resolve differences and conflicts of opinions, or simply inform each other of pertinent facts about context and the impact of the changing context on privacy decision making.

We note that several techniques have been adopted in specifying protocols for agents' communication, such as those base on *Markov decision processes* [42], *heuristics* [7, 8], *game theory* [15, 36] and *argumentation* [16, 28]. In the first three approaches, agents do not have the ability to argue with each other about the topic of discussion. Argumentation-based approaches, on the other hand, enable exchange of arguments among agents, where each agent aims to persuade other agents to accept its claims. According to [4], game-theoretic approaches usually assume complete information and unlimited computation capabilities which are sometimes not realistic. Heuristic-based approaches try to cope with the limitations of game-theoretic approaches. However, argumentation-based approaches put much emphasis on the importance of exchanging information and explanations between participants in order to mutually influence their behaviours (e.g., a participant may concede a goal having a small priority). According to Amgoud et al. [4], game-theoretic and heuristic-based approaches do not allow for the addition of information or for exchanging opinions about offers.

2.3 Argumentation

Computational argumentation is a reasoning mechanism to compute acceptable arguments based on evidence. It is a social process of reasoning to take a stand on whether to accept a disputable viewpoint by formulating propositions that are aimed at justifying (or refuting) the viewpoint. According to Walton [41], people present arguments *to try to persuade others to accept claims*. In turn, a claim is a position that one *holds* or is *committed* to.

The study of argumentation has been approached from two different perspectives [14]. The first approach is to consider argumentation as a reasoning model. This non-monotonic conception of argumentation has been studied by [6, 19, 30, 33] and many others. The second approach concerns the dialectical theory of argumentation, and in particular the role of argumentation in communication. This approach has been studied by [17, 37, 39] among others. In this paper, we consider the latter to reason about context in a dynamic IoT environment.

A dialogical (or dialectical) argumentation usually involves a set of entities or agents interacting to construct arguments for (*pro arguments*) and against (*contra arguments*) a particular claim. The dialogical process begins with the assertion of a statement (i.e., *claim* or *thesis*) by one of the participants (i.e., *proponent*) and the other participant(s) (i.e., *opponent(s)*) can accept the claim, ending the process, or can challenge the proponent's claim, requesting support for it. Evaluation in this approach examines how the strongest arguments for and against a particular proposition under consideration are aggregated and made to interact with each other and in particular, how contra arguments are used to probe each pro arguments with a view to revealing doubts about the claim in question [40]. The decision of which is better between pro and contra arguments might depend on who is observing the dialogue. An argument is a set of statements (propositions) made up of (at least) three components including a set of *premises* upon which a *conclusion* could be drawn using *inference rules*.

3 ARGUMENTATION-BASED DIALOGUES

We consider an argumentation-based dialogue system where IoT entities and users (service providers and clients etc) are represented as software agents that can perceive, reason, act and communicate with other agents. We assume that there is one agent representing each user involved in a privacy decision making process, and they will be communicating to resolve conflicts. Each agent has a *knowledge base* containing information about its environment as well as some of the other agents around it. Intuitively, a knowledge base encodes a user's context at a given time. At any point in time, an agent can request and provide information to another agent; however it is possible that an agent might decline to provide information.

To see more concretely the context that motivates our research and the kind of real-world applications that could benefit from

the argumentation-based dialogues, we consider a simple privacy scenario (adapted from [13, 21]):

Bob** works for a firm. When he is at **work**, he uses his **smart mobile phone** to log his hours. Through his login data, his boss know when he comes into the building and leaves. His smart mobile phone keeps track of his data (such as **specific position, browsing history, calls/text messages log, financial data, passwords, images/audio/videos files, demographic information, saved contacts and health records etc**). His data is shared with the **phone network provider**. For **crime prevention**, the phone network provider can share Bob's data with the **Police**. Also, in the case of an **emergency**, **emergency service providers** can request for Bob's data without his consent. This data will be kept by the phone network provider **until Bob deactivates his account. Assume we have the following information:

- Bob prefers to share his location and financial data for personalised service recommendations with trustworthy agents only but he will not share such data in work context.
- If Bob's hours at work are not correctly logged in, his wages may not be paid in full.
- The quality of Bob's office login data from the QR code scanner is not very good, so they are not very trusted.

3.1 Trust Dynamics

The scenario above shows that Bob is willing to share data with different agents with varying degrees of trust. In the example, there are six agents (Bob, smart mobile phone, phone network provider, bob's boss, police and an emergency service provider). Some agents may be malicious—and data request from such agents should be discounted. According to [38], each time an agent (hereafter named truster) needs to interact with, or rely on the intention of another agent (hereby named trustee) a decision about trust is made. Trust is a social construct that is necessary in our everyday life [29, 38], and is a mechanism used for managing the uncertainty about autonomous entities and the information they deal with [35]. Trust plays an important role in any decentralized system to control the interactions among agents, and in particular, is used to protect agents from fraudulent and malicious entities [27, 29].

Tang et al. [35] point out that trust is associated with a degree of uncertainty and also affected by relationships between individuals. It is related to the actions of individuals and how those actions affect others. According to [38], trust is by nature contextual (e.g., A trusts B to do X but not Y). Paglieri et al. [26] argued that trust should not be treated as a monolithic and static concept but should be reasoned about dynamically. Castlefranchi and Falcone [5] argued against the economic and game-theoretic view of trust and presented a principled quantification of trust "degree of trust" as a basis for a rational decision to delegate or not to another agent. In this work, we propose argumentation-based dialogue to reason about different factors of trust such as *competence* (ability of the evaluated entity to perform a given task [38]), *benevolence* (the extent to which a trustee is believed to want to do good to the truster, aside from an egocentric profit motive [38]), *integrity* (commitment to the principles acceptable by the truster. Building on the existing work [13] on trust reasoning to handle privacy regulation in IoT that has specified how the trust rating of a target agent should be updated following a feedback from another agent on the target agent's actions and decisions, we propose a dialogue system to represent the dynamics of such trust updates. Argumentation is an effective reasoning mechanism to model trust dynamics and to reason about trust and belief [35]. Such reasoning will help an agent to assign degrees of trust to other interacting agents and to determine when and what to share with them.

3.2 Reasoning about Context

From the running example, we have three user contexts: work, emergency and crime prevention. Privacy preferences and expectations vary with contexts. For instance, in crime prevention context, police may obtain Bob's location information from his phone's network provider. This information will not be shared with Bob's boss based on Bob's privacy preferences. However, in a case of dispute about his office logging hours, Bob might temporarily change his privacy preference to allow his boss have access to his location information in order to support his argument about being in the office building on a particular day where QR scanner malfunctioned. Also, Bob can 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 context is a complex and dynamic process. Understanding this process is essential for designing context-adaptive privacy mechanisms to effectively support continuous and dynamic privacy regulation process [31]. Irwin Altman's privacy regulation theory [3] describes privacy as a dynamic, dialectic, and non-monotonic process. In this process, individuals have varying privacy expectations and the dynamics of privacy contexts have significant impact on these expectations. In addition, a privacy context may be *uncertain* due to unreliable information obtained from different sources, *incomplete or partial* due to certain key information undetected or unavailable. The consequences of uncertain or incomplete privacy contexts are incorrectly formed mental models and misconceptions about afforded privacy in a given situation; these increase the chance of contextual integrity violations [31]. For example, a person caught on a CCTV camera at a location might not be aware of its video footage even though the footage might reveal its identity and location information to other 3rd party applications in other remote locations.

To reason about contexts in IoT, effective techniques are required to represent the dynamics of privacy contexts and to minimise the inconsistencies and uncertainties in order to obtain optimal privacy decisions. Argumentation is an effective mechanism to reason about uncertain, incomplete, partial and inconsistent information [24]. Argumentation-based dialogues between agents will not only allow agents to specify their privacy preferences in a given context, but also allow them to exchange arguments about the preferences and to evaluate the exchanged arguments using an appropriate argumentation semantics to compute acceptable arguments.

3.3 Handling Conflicts

An important problem in the scenario above is the handling of conflicts. By conflicts, we mean several conflicting privacy preferences by different agents. For instance, an agent might request for Bob's financial data to make personalised recommendations to him, but

Bob might decline such request. Also, there are many situations when an agent needs to collect some other agents' preferences over privacy settings in order to decide what would be optimal for an individual agent and a group of agents.

Conflicts may arise in the preferences of agents due to their limited knowledge about the available options or because an individual agent assigns different utilities to possible options. For example, an agent may be willing to give up its financial data in return for personalised recommendations, while, another agent may consider financial data as a commodity that should not be shared. There is also a problem of *privacy paradox*, a phenomenon where people say that they value privacy highly, yet in their behavior relinquish their personal data for a relatively small rewards [34].

Argumentation-based dialogues between agents are effective to harmonise conflicting views and come up with the best views towards achieving the goals under consideration. Essentially, in such dialogues, an agent specifies its privacy preferences in a certain context and provide arguments to support them. The arguments can be accepted, refuted, or questioned by another agent. Dialogues with other agents are useful to agree on a set of privacy constraints. Once a dialogue between agents is terminated, agents will have access to a set of arguments and a set of attacks that represent conflicts among arguments. In argumentation theory, various semantics are used in order to decide on acceptable (justified) arguments.

3.4 Exchanging Explanations

We propose argumentation-based dialogues between agents to facilitate exchange of explanations over privacy preferences and expectations. Explanations are important to enhance users' understanding of privacy settings in order to help them make informed decisions. Following Miller's definition of explainability [18], Mosca and Such [20] defines an explanation as a cognitive process, the process of abductive inference determining the causal attribution for a given event and a social process, i.e. 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 [2]. In the literature, the concept of explainability has been defined in different ways. Abdul et al [1] relate the concept of explainability to transparency, interpretability, trust, fairness and accountability among others. Halpern and Pearl [9] define a good explanation as a reason to a *why* question that provides information that goes beyond the knowledge of the individual asking the question.

3.5 An Example Dialogue between Agents

A dialogue between two or more agents consists of a sequence of *moves*, where each move references both a statement and the agent that made the statement. A statement can be a request for an information, a provided information or a privacy decision to grant (resp. decline) an information request. More formally, a dialogue involves n agents $Ag_1, \ldots, Ag_n$ where $(n \geq 2)$. Within a dialogue D, a move is denoted as M_x^t where $x, t \in \mathbb{N}$, denoting that a move with identifier x is made at a timepoint t. Then, a *dialogue* D can be defined as $D = [[M_1^1, \ldots, M_x^1], \ldots, [M_1^t, \ldots, M_x^t]]$.

In Table 1, we illustrate a dialogue between two agents *Bob* (Ag_1) and his *phone network provider* (Ag_2) based on the running example.

Moves/Agents	Arguments
M_1^1 by Ag_2	Hi, *AppA* is requesting access to your card details
M_2^1 by Ag_1	Sure, access granted
M_3^1 by Ag_1	My phone is hacked!
M_4^1 by Ag_1	*AppB* has access to my card details
M_5^1 by Ag_2	*AppA* shared your card details with *AppB*
M_6^1 by Ag_1	I have deleted *AppA* and *AppB*
M_7^1 by Ag_1	Do not share my card details with any other app
M_1^2 by Ag_2	Hi, *AppC* is requesting access to your card details
M_2^2 by Ag_1	Access denied
M_3^2 by Ag_2	*AppC* is a secured and trustworthy app
M_4^2 by Ag_1	Okay, access granted

Table 1: An example dialogue between two agents

The example demonstrates how the exchange of messages between agents can enhance privacy decision making process. In addition, the example shows how trust evolves in a dialogue and how the dynamics of privacy contexts can be represented. While the work in [13] has considered how the trust of an agent can be updated *following* a feedback on the decisions of the agent, we observe that *within a dialogue*, trust in an agent can change and such change in trust should affect privacy decision making when dealing with the agent. Our approach put emphasis on the fact that trust updates occur during a dialogue, which have an immediate effect on the decision being made. In long-lasting agents (human or artificial) discussions, conflicts may arise in the opinions of the participating agents. Such conflicts will be represented and resolved through argumentation-based reasoning by participating agents. In addition, contextual integrity [22] defines context-related norms of information flow. These norms will be represented as explanations/arguments to the participating agents of an argumentation-based dialogue.

4 CONCLUSIONS

In this paper, we emphasized how argumentative dialogues can be used for privacy policy reasoning in IoT. We have also described a research path we are currently pursuing to create a complete argumentation-based dialogue system for privacy policy reasoning and understand its properties. Argumentation-based dialogues is a promising mechanism to represent the context-related norms of information flow in contextual integrity, the dynamics of privacy contexts and to reason about uncertain, incomplete and conflicting privacy preferences. Moreover, we are planning to use argument graphs to communicate privacy decisions to the users while providing visual explanations.

ACKNOWLEDGMENTS

This research was funded by the UKRI Strategic Priorities Fund via the REPHRAIN research centre.

REFERENCES

[1] Ashraf Abdul, Jo Vermeulen, Danding Wang, Brian Y Lim, and Mohan Kankanhalli. 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*. 1–18.

[2] Amina Adadi and Mohammed Berrada. 2018. Peeking inside the black-box: a survey on explainable artificial intelligence (XAI). *IEEE access* 6 (2018), 52138–52160.

[3] Irwin Altman. 1975. The environment and social behavior: privacy, personal space, territory, and crowding. (1975).

[4] Leila Amgoud, Sihem Belabbes, and Henri Prade. 2005. Towards a formal framework for the search of a consensus between autonomous agents. In *Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems*. 537–543.

[5] Cristiano Castelfranchi and Rino Falcone. 2005. Socio-cognitive theory of trust. *J. Pitt. London: Wiley* (2005).

[6] Phan Minh Dung. 1995. On the acceptability of arguments and its fundamental role in nonmonotonic reasoning, logic programming and n-person games. *Artificial intelligence* 77, 2 (1995), 321–357.

[7] Peyman Faratin, Carles Sierra, and Nick R Jennings. 1998. Negotiation decision functions for autonomous agents. *Robotics and Autonomous Systems* 24, 3-4 (1998), 159–182.

[8] Shaheen S Fatima, Michael Wooldridge, and Nicholas R Jennings. 2002. Multi-issue negotiation under time constraints. In *Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1*. 143–150.

[9] Joseph Y Halpern and Judea Pearl. 2005. Causes and explanations: A structural-model approach. Part II: Explanations. *The British journal for the philosophy of science* 56, 4 (2005), 889–911.

[10] Pramod Jagtap, Anupam Joshi, Tim Finin, and Laura Zavala. 2011. Preserving privacy in context-aware systems. In *2011 IEEE Fifth International Conference on Semantic Computing*. IEEE, 149–153.

[11] Arun kishore Ramakrishnan, Davy Preuveneers, and Yolande Berbers. 2014. Enabling self-learning in dynamic and open IoT environments. *Procedia Computer Science* 32 (2014), 207–214.

[12] Nadin Kökciyan and Pinar Yolum. 2017. Context-Based Reasoning on Privacy in Internet of Things.. In *IJCAI*. 4738–4744.

[13] Nadin Kökciyan and Pınar Yolum. 2020. TURP: Managing Trust for Regulating Privacy in Internet of Things. *IEEE Internet Computing* 24, 6 (2020), 9–16.

[14] Andrew Koster, Jordi Sabater-Mir, and Marco Schorlemmer. 2013. Argumentation and trust. In *Agreement Technologies*. Springer, 441–451.

[15] Sarit Kraus and Ronald C Arkin. 2001. *Strategic negotiation in multiagent environments*. MIT press.

[16] Peter McBurney and Simon Parsons. 2002. Games that agents play: A formal framework for dialogues between autonomous agents. *Journal of logic, language and information* 11, 3 (2002), 315–334.

[17] Peter McBurney and Simon Parsons. 2007. Retraction and revocation in agent deliberation dialogs. *Argumentation* 21, 3 (2007), 269–289.

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

[19] Sanjay Modgil and Martin Caminada. 2009. Proof theories and algorithms for abstract argumentation frameworks. In *Argumentation in artificial intelligence*. Springer, 105–129.

[20] Francesca Mosca and Jose Such. 2021. ELVIRA: an Explainable Agent for Value and Utility-driven Multiuser Privacy. In *International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*.

[21] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy expectations and preferences in an IoT world. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*. 399–412.

[22] Helen Nissenbaum. 2009. Privacy in Context: Technology, Policy and the Integrity of.

[23] Helen Nissenbaum. 2020. *Privacy in context*. Stanford University Press.

[24] Gideon Ogunniye, Alice Toniolo, and Nir Oren. 2017. A dynamic model of trust in dialogues. In *International Workshop on Theorie and Applications of Formal Argumentation*. Springer, 211–226.

[25] Ali Padyab and Anna Ståhlbröst. 2018. Exploring the dimensions of individual privacy concerns in relation to the Internet of Things use situations. *Digital Policy, Regulation and Governance* (2018).

[26] Fabio Paglieri, Cristiano Castelfranchi, Célia da Costa Pereira, Rino Falcone, Andrea Tettamanzi, and Serena Villata. 2014. Trusting the messenger because of the message: feedback dynamics from information quality to source evaluation. *Computational and Mathematical Organization Theory* 20, 2 (2014), 176–194.

[27] Simon Parsons, Katie Atkinson, Zimi Li, Peter McBurney, Elizabeth Sklar, Munindar Singh, Karen Haigh, Karl Levitt, and Jeff Rowe. 2014. Argument schemes for reasoning about trust. *Argument & Computation* 5, 2-3 (2014), 160–190.

[28] Simon Parsons and Peter McBurney. 2003. Argumentation-based dialogues for agent co-ordination. *Group Decision and Negotiation* 12, 5 (2003), 415–439.

[29] Isaac Pinyol and Jordi Sabater-Mir. 2011. Computational trust and reputation models for open multi-agent systems: a review. *Artificial Intelligence Review* 40, 1 (2011), 1–25.

[30] John L Pollock. 2010. Defeasible reasoning and degrees of justification. *Argument and Computation* 1, 1 (2010), 7–22.

[31] Florian Schaub, Bastian Könings, and Michael Weber. 2015. Context-adaptive privacy: Leveraging context awareness to support privacy decision making. *IEEE Pervasive Computing* 14, 1 (2015), 34–43.

[32] Kamran Sheikh, Maarten Wegdam, and Marten van Sinderen. 2008. Quality-of-context and its use for protecting privacy in context aware systems. *J. Softw.* 3, 3 (2008), 83–93.

[33] Guillermo R Simari and Ronald P Loui. 1992. A mathematical treatment of defeasible reasoning and its implementation. *Artificial intelligence* 53, 2-3 (1992), 125–157.

[34] Daniel J Solove. 2021. The myth of the privacy paradox. *Geo. Wash. L. Rev.* 89 (2021), 1.

[35] Yuqing Tang, Kai Cai, Peter McBurney, Elizabeth Sklar, and Simon Parsons. 2011. Using argumentation to reason about trust and belief. *Journal of Logic and Computation* (2011), exr038.

[36] Tatiana Tatarenko. 2019. Stochastic learning in multi-agent optimization: Communication and payoff-based approaches. *Automatica* 99 (2019), 1–12.

[37] Pancho Tolchinsky, Sanjay Modgil, Katie Atkinson, Peter McBurney, and Ulises Cortés. 2012. Deliberation dialogues for reasoning about safety critical actions. *Autonomous Agents and Multi-Agent Systems* 25, 2 (2012), 209–259.

[38] Joana Urbano, Ana Paula Rocha, and Eugénio Oliveira. 2013. A socio-cognitive perspective of trust. In *Agreement Technologies*. Springer, 419–429.

[39] Douglas Walton. 1995. *Commitment in dialogue: Basic concepts of interpersonal reasoning*. SUNY press.

[40] Douglas Walton. 2009. Argumentation theory: A very short introduction. In *Argumentation in artificial intelligence*. Springer, 1–22.

[41] Douglas N. Walton. 1996. *Argumentation Schemes for Presumptive Reasoning*. L. Erlbaum Associates.

[42] Ping Xuan, Victor Lesser, and Shlomo Zilberstein. 2001. Communication decisions in multi-agent cooperation: Model and experiments. In *Proceedings of the fifth international conference on Autonomous agents*. 616–623.

[43] Jan Henrik Ziegeldorf, Oscar Garcia Morchon, and Klaus Wehrle. 2014. Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks* 7, 12 (2014), 2728–2742.