A Semantic Model for Embracing Privacy as Contextual Integrity in the Internet of Things (Short Paper)

Salatiel Ezennaya-Gomez[1](✉), Claus Vielhauer[2], and Jana Dittmann[1]

[1] Otto-von-Guericke University Magdeburg, Magdeburg, Germany
{salatiel.ezennaya,jana.dittmann}@ovgu.de
[2] Brandenburg University of Applied Sciences, Brandenburg, Germany
claus.vielhauer@th-brandenburg.de

Abstract. Due to the increasing number of complaints alleging privacy violations against companies to data protection authorities, the translation of business goals to system design goals and the subsequent consequences for customers' privacy poses a challenge for many companies. For this reason, there is a need to bridge the economics of privacy and threats to privacy. To this end, our work relies on the concept of privacy as contextual integrity. This framework defines privacy as appropriate information flows subjected to social norms within particular social contexts or spheres. In this paper, we introduce a preliminary version of a semantic model which aims to relate and provide understanding on how well-established business goals may affect their customers' privacy by designing IoT devices with permission access, data acquired by sensors, among other factors. Finally, we provide a use case application showing how to use the semantic model. The model aims to be an educational tool for professionals in business informatics during the modeling and designing process of a product which may gather sensitive data or may infer sensitive information, giving an understanding of the interaction of the product and its footprint with diverse actors (humans or machines). In the future, a further complete model of the presented may also target other groups, such as law enforcement bodies, as part of their educational training in such systems.

Keywords: Privacy · Contextual integrity · Internet of Things · Semantic model · Digital exclusion

The work results presented are related in part of the general approach to the MSCA-ITN-ETN - European Training Networks Programme under Project ID: 675087 ("AMBER - enhAnced Mobile BiomEtRics") and in part to educational purposes of the model to guide forensics to the project FINANzkriminalitaeT: MethodIsche Analyse von Bedrohungsszenarien fuer moderne Karten- und App-basierte Zahlungssysteme (FINANTIA; FKZ:13N15297) funded by the Bundesministerium fuer Bildung und Forschung (BMBF).

S. Katsikas et al. (Eds.): ESORICS 2021 Workshops, LNCS 13106, pp. 413–423, 2022.
https://doi.org/10.1007/978-3-030-95484-0_24

1 Introduction

In June 2021, the number of GDPR (General Data Protection regulation) fines were six hundred ninety-two, with an amount of nearly three hundred million euros [2]. These numbers may showcase many companies and how little they embrace Privacy-by-Design as part of their business and system design processes. One side of the many-sided problem is caused by how the applications and devices, which support Big Data business models, are designed to pursue those business goals. For these reasons, it is essential to bridge the economics of privacy, ethics in system design, and privacy risks and understand the cause-effect of business goals. We believe that this objective is achievable by embracing privacy as Contextual Integrity (CI) as part of the educational agenda for professionals of business informatics.

Our work is based on a well-established philosophical framework, called CI, introduced by Nissenbaum in [14], and previous work on semantic model literature reviews for privacy risks [5,8,10]. CI defines *privacy* as "appropriate information flows according to norms specific to social spheres or contexts" as described in [7]. The framework includes abstract concepts, such as societal values and stakeholders interests, bases for privacy's ethical legitimacy. It unifies multiple known concepts of privacy, e.g., security design aspects, including the concept of context(s) or spheres, and abstract factors, such as business relations and their influence in the behavior of applications and IoT devices, as stated in [7]. If the privacy norms are not respected, the situation leads to privacy violations, such as inferring sensitive attributes from social media posts even when these attributes are not revealed, and later on, using the extracted information for psychological advertising targeting individuals [6].

In the review presented by Benthall et al., in [7], the authors conclude by calling for actions on "designing systems that address the challenges of matching concrete situation with abstract spheres". They raised a set of research questions in their review on how computer science approaches CI: (RQ1) "how to be more technically precise about the nature of contexts in order to relate the definition given in CI with more concrete notions used by computer scientist?"; (RQ2) "how to apply the CI framework to IT systems which are designed to work across multiple contexts?" We aim to contribute to finding an answer to these questions by scoping the relations among every participant, from the individual(s) to businesses. Notably, in smart environment applications, where sensors and actuators interact with many users at once, e.g., in a videoconference or in a schoolroom, where it is hard to rely on individual privacy preferences and expectations [7]. For this reason, our objective is to design a semantic model capturing CI elements and privacy threats for IoT devices. The model aims to be an educational tool for professionals in business informatics during the modeling and designing process of a product (or device) which may gather sensitive data or may infer sensitive information, giving an understanding of the interaction of the product and its footprint with diverse actors (humans or machines). In the future, a further complete model of the presented may also target other groups, such as law enforcement bodies, as part of their educational training in such systems.

The document is structured as follows: In Sect. 2, the CI theory is briefly explained. Subsequently, in Sect. 3, a semantic model based on CI principles is presented, describing the methodology and introducing the model with a use case scenario. Finally, conclusions and discussion are in Sect. 4.

2 Background

This section briefly describes the CI theory. For a more detailed description and reasoning about it, we refer to Nissenbaum's work in [7,14,15].

Contextual Integrity (CI) is a benchmark theory of privacy based on law and societal norms introduced by Helen Nissenbaum in her book Privacy in context in [14]. CI defines privacy as *appropriate information flows* which are subjected to social norms within particular social contexts or spheres. Subsequently, informational privacy norms (or privacy norms) are mapped onto privacy expectation of the individuals. The norms are formed by five parameters: the *data subject*, the *sender* of the data, the *recipient* of the data, the *attribute* or *information type*, and *transmission principle*, which are the *information flow conditions* among parties such as, those that are well-known, *with data subject's consent, in confidence, required by law*, and *entitled by the recipient.*

Lastly, the author describes contextual ends, purposes, and values of society as the "essence" of the social context, legitimizing the norms mentioned earlier. Thus, when privacy norms are fulfilled, contextual integrity (i.e., privacy) is respected. Privacy norms are in line with the law as well as, with privacy expectations and social values. In legal contexts, there is a privacy violation when there is a violation of privacy laws. In CI, if defined privacy norms are not respected, the situation leads to privacy violations, such as inferring sensitive attributes from social media posts even when these attributes are not revealed, and later on, using the extracted information for psychological advertising targeting individuals [6].

In the literature, there are studies on how the users of smart home devices perceive privacy norms [4]. These studies help to understand how privacy expectations and contexts change while using those IoT devices. The results show that these expectations rely on user's trust in companies, business practices, among other factors, such as geopolitical situations.

3 A CI Semantic Model

Our goal is to design a semantic model introducing CI concepts in the IoT environment. It aims to provide another view on how related could be the elements of an agent (i.e., device or applications) to business purposes and privacy threats.

For the creation, we employed the seven steps of the 101 methodology described in [16], which are summarized into the following three steps: (1) knowledge acquisition and identification of the purpose of the ontology; (2) modeling the ontology, defining the classes and relations; (3) evaluation of the semantic model. The first step encompasses from the first to the third step of 101, which are *(step 1) determine the domain and scope of the ontology, (step 2) consider reusing existing ontologies, and (step 3) enumerate important terms in the ontology.* The second step groups *4 (Define the classes and the class hierarchy), 5 (Define the properties of classes-slots), 6 (Define the facets of the slots), and 7 (Create instances)* of the 101 methodology. Finally, the third is out of the scope of the 101 but is necessary for semantic modeling and evaluation. We achieved the first and second steps of the methodology, considering the third step as our future work. Nevertheless, we describe the model as a use case application in Subsect. 3.3.

3.1 Knowledge Acquisition and identification of the Purpose of the Semantic Model

Our knowledge is based on literature reviews presented in [5,8,10]. The authors identified some points in which semantic models in privacy fall short of identifying potential attributes, which can be detected/inferred from data types or different sources. As reviewed in [8], many ontologies have been proposed for semantic knowledge modeling for privacy. These ontologies range from those ensuring consent based on the legal framework (mainly focused on GDPR) to ontologies that define and relate online privacy risks, such as phishing. However, these proposals lack the issues mentioned above regarding the links between business goals and privacy violations. From the conclusions drawn in the review, we defined the following questions which the ontology aims to answer: (Q1) how are the attributes related to the purposes of the application(s) and the organization(s)? (Q2) what actions performed by agents in the IoT system may affect individual and others' attributes? Since the semantic model aims to answer questions related to privacy that need to be implemented and interpreted by human beings, we do not focus on having the best time responds while lunching a query, but rather to have consistencies in its answers.

3.2 Modeling the Ontology, Defining the Classes and Relations

In this subsection, we introduce our suggested semantic model by describing each of the top-level class nodes, their functional interrelations with other nodes in Fig. 1, and some of their subclasses or instances. Following 101 methodology recommendations, it is possible to reuse other semantic models connected through those top-level classes, e.g., *SecurityPrivacyIssues* for information security [11,12]. Figure 1 shows the core concepts of our semantic model.

Agent. An agent is an entity, i.e., *DataSubject* (active users and other individuals who are inactive users whose data are also part of the gathered dataset), *Organization, Embedded Organization, and OrganisationsDataReceivers* (other organizations which process data handed by another organization), who generates and creates other entities, such as *DigitalAgents* and *Embedded DigitalAgent* (e.g., mobile applications, trackers, third-party APIs). The agents may access several objects across the diagram, such as sensors, data generated by those sensors, and other smart devices. In addition, some of these agents may be linked to another class, called *Actors*, defined in the other data regulation semantic models, such as GConsent [17].

Assets. Assets are those essential elements for the existence of a relation between agents and essential to protecting with security mechanisms. They may be divided into two categories, *tangible assets* and *non-tangible assets.* Some subclasses are, e.g., *PhysicalSensors*, *TelemetryData*, and *ApplicationConnections.* The data are generated by data subjects and digital agents (e.g., an application), which interact with the data subjects or other digital agents. Some assets may contain instances from class *Attributes.*

Actions. They are activities that the agents can perform. Some actions or activities are mainly related to certain actors. For instance, an organization and embedded organizations could perform advertising tracking or traffic analysis using digital agents. Other actions, such as *SendReceiveStreams* or *Active Interaction* could be performed by some digital actors.

Purposes. The *Purposes* class defines the intentions for which an application is used. This class has three categories (overlapping sets) which are: *User, Business, and Application* which correspond to purposes of agents *DataSubject, Organization and Embedded Organization, and DigitalAgent and EmbeddedDigialAgent.* In addition, subclasses of purposes which contain more specific instances, among others, are *Education, Security (e.g., LockDoor), Health (e.g., DailySteps, DailyCalories), Office (e.g., ReadEmails), Banking (e.g., NFCPayment), Social Media (e.g., Tweets), and Entertainment.*

For instance, an application can be used for educational purposes, social media purposes, and security purposes, e.g., an app that teaches new languages has some security features (for unlocking the application using face and voice), including messaging with other users of the app. Therefore, the user's purposes are *education, security, and social media.* These purposes may coincide with the application purposes. Nevertheless, the set of application purposes may include more purposes, such as *IdentityFraudDetection, DeviceProfiling, Advertising.* Moreover, these application purposes may be part of a more extensive set of general business purposes which are also *Adversiting, FraudDetection, Adprofiling, DataModelsTrading, PartnerDataSharing, and SelfBusinessActivities*, among others.

Attributes. They are relevant features for the identification of individuals, their environment(s) (e.g., location, including special attributes, such as social background or race [19]), and the devices within the IoT system. These attributes can be either directly or indirectly extracted (i.e., inferred information) from a set of instances of *Assets*, e.g., data types. For example, they can be directly obtained by performing face and voice recognition while extracting a set of attributes available in live interactions or in pictures and audio stored in the device's local storage, previously permission access to storage should be granted. Also, they can be indirectly extracted from a set of assets and actions performed, e.g., audio background filtering or speaker detection performing knowledge discovery in the cloud.

Transmission Principles. This class is complex due to its interactions with other classes and subclasses. The class refers to the conditions that are created for the *transmission or gathering* of the data, e.g., protection mechanisms are applied to secure the data exchange with the user's consent, including to whom the data are sent, locations of the organization(s). Some of the subclasses of the class are *SecurityRequirements, LegalRequirements, AppliedProtectionMechanisms, DataSubjectConsent, and DataSubjectExpectations*, among others. The latter could have instances obtained from a list of user's expectations as a result of surveys in contextual privacy norms design by device manufacturers [4].

Values. As indicated by the CI theory, agents conduct their decisions and actions according to a series of ethical values and interests, which may be part of their established social norms. We understand that this class should cover social and individual's situations, for instance, current geopolitical situation of agents' region(s) where data are transferred. This class is the most abstract class of the model, and we believe that professionals in ethics and technology should define its instances. A starting point for this may be the core points established in a standard on ethics, and system design, such as the IEEE P7000 family [3]. This class is closed related to the *Transmission Principles* class since it governs the abstract principles of the transmission principles' instances.

Security and Privacy Issues. This class describes known and known-unknown security and privacy issues, which may pose security threats and privacy risks by the usage of extracted information from individuals' attributes from an active user or non-active user(s), actions performed, and relations among digital agents. The class has two non-disjoint subclasses, which are *Security Vulnerabilities* and *Privacy Threats*. They are non-disjoint classes since the former may also imply threats to privacy by exploiting a set of security vulnerabilities. Moreover, these subclasses can also be linked to more specific semantic models on privacy and security, e.g., based on ISO 27001, on legal compliant semantic models, and attack knowledge databases, such as ATT&CK of MITRE [1].

3.3 An Exemplary Use Case Application

The semantic knowledge model can be applied in the first stage of requirement analysis and definition in any software engineering design methodology found in the literature, e.g., agile or waterfall models. Within the requirement analysis step, use cases related to the technical functionalities of the product and privacy risks and law enforcement should also be described. For example, a person wears a smartwatch-fitness tracker in his workplace, connected to an app (or application) installed in the user's smartphone. Current smartwatches in the market are multi-purpose devices, i.e., a smartwatch could be used as a fitness tracker, a home assistant, among diverse usages. Hence, a list of high-level requirements for

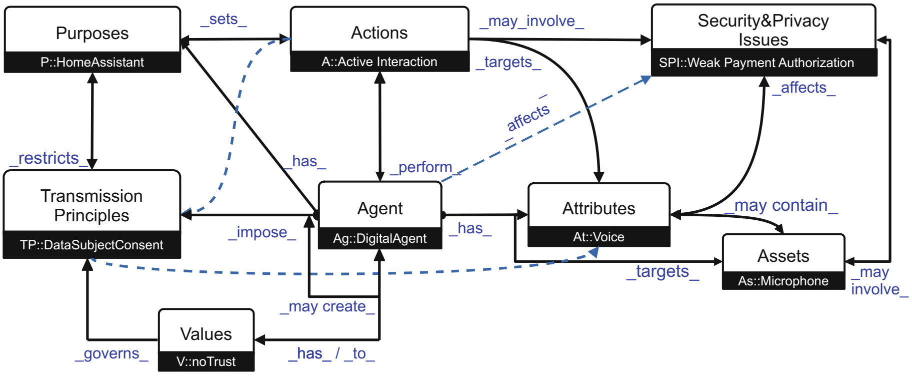

Fig. 1. The diagram showcases the relations and dependencies among classes. Below each class label, an exemplary instance is written, extracted from the use case in Subsect. 3.3. Black lines define direct relations, and blue dash lines show indirect implications between classes. (Color figure online)

the tandem smartwatch and its app could be (1)*the device must capture ECG and speech*; (2)*the smartwatch should be interoperable with an intelligent voice assistant (IVA) device and skills (third-party applications for smart home devices)*; (3)*the device can emulate a credit card for authorized contactless payments.*

In this example, the modeling starts breaking down the functional requirements for the identification of the classes. Starting from the *Agent* class, the *data subject* is the active user who wears the device; the class *organization(s)* is the company of the smartwatch and app, along with the *embeddedOrganization(s)* which offer the smartwatch services, its modalities, and other business purposes of the organization. These embedded organizations could be connected to the device via APIs or software development kits (SDKs) to develop the app and the smartwatch software. Subsequently, the primary piece of software of the device or smartwatch and the app are *digital agent(s)* which are created by the *organization(s)*, along with the trackers and third-party trackers (pieces of code that collects and send data) embedded in the used SDK or API, which are the *embeddedDigitalAgent(s)* created by *embeddedOrganization(s)*. Finally, another user could be present as a *(inactive) data subject(s)*, who may be further identified by applying specific actions on the acquired data.

On the other hand, the list of common *Purposes* for the category *user* and *business*, i.e., for the data subject and organization(s) are *Health* with instances, such as *DailySteps*, as a fitness tracker, *SmartHome* as a home assistant or IVA, and *Contactless-Payment* as a credit card emulator. Furthermore, there are more purposes for small functionalities, such as *social media*, whether sharing extracted information (e.g., hiking tracks and performance) while acting as a fitness tracker is possible. Moreover, apart from the aforementioned purposes that may have each agent, there are more purposes for the organization and the embedded organization(s), i.e., their business purposes, such as *marketing/advertising*, *IntelligentDataAnalysis*, *SocialMediaBehaviourModels*, *Contactless-Payment*, *IdentityFraudDetection*, and *DataModelsTrading* among others. Furthermore, the device has different components (physical and software) which constitute the *Assets*. For instance, for the *tangibleAssets* category, there are accelerometers, ECG sensors, BLE, microphone, NFC (e.g., used for contactless payment), for the *non-tabgibleAssets*, there are assets, such as *BiometricData*, *Metadata* and *TelemetryData* from sensors, the smartwatch, and the smartphone where the app is running.

Some of the *Actions*, that the device or any other agent may perform, are sending the collected data, e.g., *CaptureUtterance*, *Send/ReceiveStreams* of *TelemetryData* to either the app, *EmbeddedOrganization* or the IVA's cloud directly. Additionally, the app distributes data streams among *organization* and *embedded organization(s)* according to the list of purposes for both business and functionalities of the device. For instance, an organization embeds APIs that belong to financial companies or fintech in the app for conducting contactless payments. These APIs connect other applications and send information about a payment process, among other information, to their servers and fintech companies involved in the payment process. In addition, depending on the business purpose of the embedded organization, e.g., *Advertising*, the API may establish a connection to servers of another organization, called *X*, which is not involved in the payment process. This action triggers the installation of another *embedded digital agent* of the organization*X* in the user's device, as it is shown in a recent study on online payment traffic analysis in [9]. When the app has third-party trackers, i.e., one or more *embedded digital agent(s)*, at least technical/metadata data about the device where the app is installed, its functions, plus information about which app has invoked that tracker, are sent to these new embedded organization(s). Note that there are types of trackers (e.g., long-term tracker that lasts up to two years) that identify a user, which may pose a privacy threat.

From the data captured by the digital agent(s), some information is directly or indirectly extracted, which may correspond to instances of the *Attributes* class. One group of attributes may be those related to the data subject, e.g., attributes extracted from speech are *nationality*, *age*, *educational background*, *health condition*, *emotions*, and *gender* along with captured traits from other individuals. From technical information, such as access network state and connections, the location could be inferred.

The *TansmissionPrinciples* includes the so-called agreement conditions, which refers to the *LegalRequirements, DataSubjectConsent*, along with data subject's expectations fulfilled by surveys, which may be, e.g., *AppliedAdditionalObfuscation* on specific attributes that are found in a particular asset. Specifically, this particular transmission principle may be governed by an instance of the abstract class *Values*, such as *geopolitical situation* under which the transmission and process of information take place. Also, there could be instances from *Values* related to agents, e.g., *data subject* has *No Trust* on *Embedded Organisation.*

The semantic model can relate business purposes to individuals' privacy, answering $Q1$ and $Q2$ from the Subsect. 3.1 as follows. For example, for the

Contactless-Payment purpose, it is needed access to a set of tangible and non-tangible assets. These assets are, but not restricted to, *NFC sensor*, *payment data*, *telemetrydata* and *metadata*. These assets are also used for purposes, such as *IdentityFraudDetection* (for detecting payment fraud), *DataModelsTrading* (for selling models to merchants or other companies). From these datasets, attributes and subsequent user information can be inferred. From the *telemetrydata, payment data, and metadata*, the attributes of *location* of the user, and *language* used in the device can be obtained. Moreover, from these attributes, it is possible to know the educational background or nationality, as well as from purchased items, including the categorization of the merchant's marketplace, it is possible to infer attributes, such as *gender* or *sexual orientation*. Nevertheless, these attributes may imply a set of instances of the *Security and Privacy Issues* class. The aforementioned inferred attributes, along with specific actions performed by the organizations involved, may imply known privacy issues, such as knowing the user's residence district is possible to infer information about the ethnic group or economic status. This particular example is due to the digital agent of *Send/ReceiveStreams* of *payment data*, and to use the asset for *OnlineBehaviouralDataModelsTrading* as business purpose. Furthermore, known security vulnerabilities of physical assets, e.g.,*NFC sensor*, may pose privacy threats as well.

4 Discussion and Conclusions

In the presented paper, we have introduced a semantic model based on privacy as contextual integrity. One limitation of our semantic model is the lack of validation by privacy engineers. This point is expected to be solved in our future work. The other limitation is the creation of relationships among classes. For some exemplary cases of privacy issues, describing the relationships becomes a difficult task due to the complexity and dependencies between classes and instances. In addition, the model does not yet cover cases such as, identifying bystanders who have not given consent and are accidentally recorded and what mitigations should be employed to reduce privacy risks; however, they are not ruled out for the next stages of model development.

During the literature review and creation of the model, we encountered some privacy challenges in the field. One is the inferred information (extracted information of other individuals) not provided explicitly by a single user. However, it could be extracted from the user's data by knowledge discovery methods, which is mathematically described in [6] as a situated information flow theory. We believe that this challenge could be described in the semantic model by using instances of the classes *Asset, Actions, Attributes*, and *Security&PrivacyIssues* based on studies on knowledge discovery. The second is the description of the consequences of the privacy preferences of a social group, which may affect an individual's privacy preferences. This problem is called Digital Exclusion, and it is discussed in [18]. Unfortunately, this particular problem is not described in the semantic model yet. Such problems seem to be closer to an ethical and philosophic issue than a technical issue. Nevertheless, the use of technology affects these issues. For these reasons, the inclusion of socio-technological models as part of the design cycle of a technological product becomes essential to achieve systems that respect social norms and the integrity of individuals.

Bridging the gap between Nissenbaum's theory, in which privacy is understood as contextual integrity (CI), and IoT system design, we provide a preliminary version of a semantic model to understand what aspects may affect an individual's privacy using IoT devices. The model aims to be an educational tool for professionals in business informatics during the modeling and designing process of a product which may gather sensitive data or may infer sensitive information, giving an understanding of the interaction of the product and its footprint with diverse actors (humans or machines). Moreover, the model can be helpful for organizations that conduct a privacy impact assessment, research ethics in pervasive data, and developers to get information on where and what could impact individuals' privacy by relations among attributes, sensors, and actors. We believe that this model may also contribute to the initiative of the Software Bill of Material of the National Telecommunications and Information Administration of the US (NTIA) for enhancing transparency in software by including the influence of third-party software over users' privacy and privacy statements, along with security vulnerabilities [13].

In the future, a further complete model of the presented may also target other groups, such as law enforcement bodies, as part of their educational training in such systems. The presented paper is a theoretical proposal and is considered for future implementation and validation as future work.

References

1. A definition of the mitre att&ck framework. https://attack.mitre.org/matrices/enterprise/. Accessed 12 July 2021
2. GDPR Fines Tracker & Statistics (2021), https://www.privacyaffairs.com/gdpr-fines/. Accessed 12 July 2021
3. Model process for addressing ethical concerns during system design (2021). https://ethicsinaction.ieee.org/p7000/. Accessed 16 Sept 2021
4. Abdi, N., Zhan, X., Ramokapane, K.M., Such, J.: Privacy norms for smart home personal assistants. In: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (2021)
5. Badillo-Urquiola, K., Page, X., Wisniewski, P.: Literature review: Examining Contextual Integrity Within Human-Computer Interaction. SSRN 3309331 (2018)
6. Benthall, S.: Situated information flow theory. In: Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security. HotSoS 2019, Association for Computing Machinery, New York (2019)
7. Benthall, S., Gürses, S., Nissenbaum, H.: Contextual integrity through the lens of computer science. found. Trends® Priv. Secur. **2**(1), 1–69 (2017)
8. Ezennaya-Gomez, S.: Rethinking and privacy-knowledge and modeling-about and uncovering accepted and data collection and business and practices as privacy and risks. Technical Report FIN-03-2020, Otto-von-Guericke University Magdeburg, Germany (2020)

9. Ezennaya-Gomez, S., Kiltz, S., Kraetzer, C., Dittmann, J.: A semi-automated http traffic analysis for online payments for empowering security, forensics and privacy analysis. In: The 16th International Conference on Availability, Reliability and Security. ARES 2021, Association for Computing Machinery, New York (2021). https://doi.org/10.1145/3465481.3470114
10. Gharib, M., Giorgini, P., Mylopoulos, J.: Towards an ontology for privacy requirements via a systematic literature review. In: Conceptual Modeling, pp. 193–208. Springer International Publishing, Berlin (2017). https://doi.org/10.1007/978-3-642-34002-4
11. Halpin, H.: Semantic insecurity: security and the semantic web. In: PrivOn 2017 - Workshop Society, Privacy and the Semantic Web - Policy and Technology. vol. 1951, pp. 1–10. Vienna, Austria, October 2017
12. Herzog, A., Shahmehri, N., Duma, C.: An ontology of information security. Int. J. Inform. Secur. Privacy **1**(4), 1–23 (2007)
13. National Telecommunication Information Association, U.S.D.o.C.: Software bill of material (2021), https://www.ntia.gov/SBOM. Accessed 12 July 2021
14. Nissenbaum, H.: A contextual approach to privacy online. In: Digital Enlightenment Yearbook 2012, vol. 140, pp. 219–234 (2012)
15. Nissenbaum, H.: Respecting context to protect privacy: why meaning matters. Sci. Eng. Ethics **24**(3), 831–852 (2015). https://doi.org/10.1007/s11948-015-9674-9
16. Noy, N.F., McGuinness, D.L.: Ontology Development 101: A Guide to Creating Your First Ontology: Knowledge Systems Laboratory. Stanford University. Tech. rep, Stanford University (2001)
17. Pandit, H.J., Debruyne, C., O'Sullivan, D., Lewis, D.: GConsent - a consent ontology based on the GDPR. In: Hitzler, P., Fernández, M., Janowicz, K., Zaveri, A., Gray, A.J.G., Lopez, V., Haller, A., Hammar, K. (eds.) ESWC 2019. LNCS, vol. 11503, pp. 270–282. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-21348-0_18
18. Rehak, R.: What does data protection actually protect? Why data protectionists must stop talking about individual privacy (2018). https://media.ccc.de/v/35c3-9733-was_schutzt_eigentlich_der_datenschutz. Accessed 12 July 2021
19. A requirement analysis for privacy preserving biometrics in view of universal human rights and data protection regulation. In: 2018 26th European Signal Processing Conference (EUSIPCO), pp. 548–552 (2018)