Semantic Web 0 (2018) 1
IOS Press

Privacy, Security and Policies: A review of Problems and Solutions with Semantic Web Technologies

Sabrina Kirrane [a,*], Serena Villata [b] and Mathieu d'Aquin [c]

[a] *Institute for Information Business, Vienna University of Economics and Business, Austria*
E-mail: sabrina.kirrane@wu.ac.at
[b] *Université Côte d'Azur, CNRS, Inria, I3S, France*
E-mail: villata@i3s.unice.fr
[c] *Data Science Institute, Insight Centre for Data Analytics, National University of Ireland Galway, Ireland*
E-mail: mathieu.daquin@nuigalway.ie

Abstract. Semantic Web technologies aim to simplify the distribution, sharing and exploitation of information and knowledge, across multiple distributed actors on the Web. As with all technologies that manipulate information, there are privacy and security implications, and data policies (e.g., licenses and regulations) that may apply to both data and software artifacts. Additionally, semantic web technologies could contribute to the more intelligent and flexible handling of privacy, security and policy issues, through supporting information integration and sense-making. In order to better understand the scope of existing work on this topic we examine 78 articles from dedicated venues, including this special issue, the PrivOn workshop series, two SPOT workshops, as well as the broader literature that connects the Semantic Web research domain with issues relating to privacy, security and/or policies. Specifically, we classify each paper according to three taxonomies (one for each of the aforementioned areas), in order to identify common trends and research gaps. We conclude by summarising the strong focus on relevant topics in Semantic Web research (e.g. information collection, information processing, policies and access control), and by highlighting the need to further explore under-represented topics (e.g., malware detection, fraud detection, and supporting policy validation by data consumers).

Keywords: Security, Privacy, Policy, Access control, Anonymity, Malware, Intellectual property

1. Introduction

Privacy, security and the proper handling of data related policies are topics that affect all technological areas, but have been under-explored in relation to Semantic Web technologies. Indeed, much research in the Semantic Web and Linked Data domain has focused on enabling the sharing of open datasets. However, as Semantic Web technologies and principles are gaining traction both in use cases that deal with sensitive data and in terms of application in industrial contexts, it is necessary to investigate the potential privacy and security issues. For example, how they might cause new or more complex threats to privacy or make the security of deployed systems harder to ensure, and how managing, tracking and enforcing policies associated with data becomes more complex.

Although the widespread use of Semantic Web technologies and Linked Data leads to new security, privacy and policy-related problems, at the same time they can also be seen as part of the solution. For example, more accurate models for detecting security issues can be built through the semantic analysis of the data. Additionally, the meaningful interpretation of personal data exchanged between individuals and various other web entities could be used to empower web

*Corresponding author. E-mail: sabrina.kirrane@wu.ac.at.

users to better control those interactions, and therefore better manage their online privacy. The machine-readable and machine-processable representation of data-related policies can also bring many advantages to companies through the automation of tasks related to policy-management.

The goal of this paper is to provide a brief overview of recent work on security, privacy and policy related challenges associated with Semantic Web technologies. The information presented herein is based on analysing the articles published in this special issue of the Semantic Web Journal, therefore acting as an editorial for it, as well as looking at the five editions of the *Society, Privacy and the Semantic Web - Policy and Technology* (PrivOn) workshop (which was collocated with the International Semantic Web Conference), two editions of the *Trust and Privacy on the Social and Semantic Web* (SPOT) workshop (which was collocated with the Extended Semantic Web Conference), and at other related sources. The objective of this literature review is to identify key trends, and especially new challenges that are being investigated from both the problem and the solution angles, as well as the gaps that the community needs to address. We therefore start by looking at existing classifications in the areas of security, privacy and policies. Following on from this we use the aforementioned classifications to frame our discussion of existing work on privacy, security and policies in the Semantic Web domain. Finally, we conclude by highlighting the current trends and, more importantly, the research gaps that present open challenges for privacy, security and policy research in the Semantic Web domain.

2. Foundation: Categorizing privacy, security and policy issues and works

Privacy, security and policy topics in data and information management are very related to each other, but also each one is very complex and multifaceted in their own right. They each represent a wide range of issues and challenges, to which a variety of solutions have been applied in other domains. While not all those issues and challenges might apply to Semantic Web technologies, it is worth looking at them broadly, inorder to understand where works by the Semantic Web community tend to place themselves, and where gaps still exist.

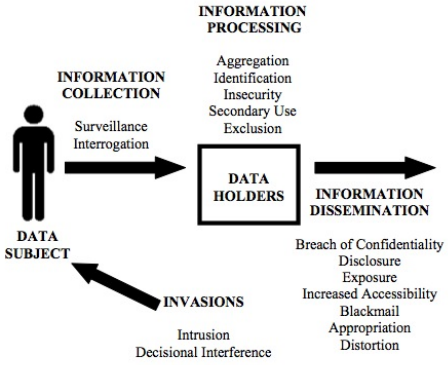

Fig. 1. A taxonomy of activities creating privacy problems, from [1]

2.1. A taxonomy of privacy

One of the most highly cited works that is used to "classify privacy" is an article entitled "A taxonomy of privacy" by Daniel Solove [1]. In said article, Solove argues (as many authors before him) that privacy is an ambiguous, polysemic and often subjective term that can therefore not be reduced to a simple concept, and especially cannot be considered purely from the point of view of the law. Instead of proposing a definition for privacy, Solove focuses on privacy threats which, he argues, can be listed and defined in a more robust manner. This taxonomy of privacy problems is depicted, in Figure 1 where information based activities that are known to create problems are divided into four main categories: information collection, information processing, information dissemination, and invasion.

2.2. Classification of Security Incidents

Security is also a broad term that can be applied to many different areas. However, considering the scope of this article, we focus here on cyber-security, which relates to security issues and challenges associated with computing devices, applications and networks. There have been several classifications of issues and problems associated with cyber-security from various organisations, including, e.g., the Software Engineering Institute [2] and the European Union Agency for Network and Information Security (ENISA) [3]. Those tend to overlap and cover similar aspects, as they focus on the incidents of problems that might occur in relation to cyber-security. Here we choose to apply the

taxonomy from the European Cybercrime Centre (EUROPOL) [4] as it focuses specifically on threats and issues that are related to technological systems. This taxonomy of incidents is reproduced in Table 1. Naturally, only a subset of those threats are expected to be relevant for Semantic Web technologies.

2.3. Tasks associated with policy management and compliance

There are several types of policies that are related to the present study. Those include privacy and security policies that strongly overlap, in their content, with the two previous classifications. We additionally consider in this category the specific tasks that are associated with the management of and compliance with policies associated with the distribution of intellectual property (IP) assets, especially software and data licenses, as well as terms of use of services and regulatory obligations. As far as we are aware, there does not exist a taxonomy of activities or issues associated with this area. We therefore take inspiration from existing literature, especially in the area of software license management, to devise a simple taxonomy of tasks associated with privacy, security, distribution and usage policies for IP assets. This taxonomy, which is presented in Table 2, is relevant for policies that relate to data or software artifacts, including services.

3. Collection: Existing works around Semantic Web security, privacy and policy

Based on the taxonomies described above, our goal is to review the privacy, security and policy research contributions associated with Semantic Web technologies. This includes both the use of Semantic technologies to support the resolution of specific privacy, security and policy issues, as well as works that tackle privacy, security and policy issues emerging from the application of semantic technologies. To do that, we create a corpus of papers and articles that directly address one or more of those aspects. We start with the works published in the Special Issue of the Semantic Web Journal on Security, Privacy and Policies (for which this article acts as editorial), namely:

- **PrivOnto: a Semantic Framework for the Analysis of Privacy Policies** [5], which presents an ontology for annotating privacy policies for the purpose of supporting users in understanding and interpreting them.
- **Reasoning with Data Flows and Policy Propagation Rules** [6], which proposes a framework for reasoning upon the propagation of data reuse and redistribution policies (especially data licences) across the workflows that manipulate them.

We also include in this analysis all the papers presented during the PrivOn workshop series, which was co-located with the International Semantic Web Conference (ISWC) from 2013 to 2017, and relevant papers from the SPOT workshop, which was co-located with the Extended Semantic Web Conference (ESWC) in 2009 and 2010. Finally, in order to obtain relevant works outside of those specific venues, we perform several Google Scholar searches, by associating keywords strongly related to Semantic Web technologies[1] with the keywords extracted from the three taxonomies described in the previous section. Since Semantic Web technologies have evolved dramatically in the last few years, we restrict this list of papers to those published in the last 10 years (on or after 2008). We also filtered out papers that appeared to be redundant with others already included (similar authors and topics). We obtained a total of 78 references[2], which were analysed in order to determine their relation to the three taxonomies in the next section. While we cannot claim that this corpus is exhaustive, we assume that it is representative of current work that relates privacy, security and policy topics with research in the Semantic Web domain.

4. Analysis: Classifying of Semantic Web security, privacy and policy works

We analyse the corpus of references collected according to the method described in the previous section by manually annotating each paper using the three taxonomies previously described. In doing so, we do not assume that any paper should only be represented by one category, or one taxonomy, as many works span across several topics with varying levels of generality. For example, the articles included in the special issue of the Semantic Web Journal are classified as depicted in *Table* 3.

[1] including Semantic Web, semantics, Linked Data, ontology, RDF, OWL, SPARQL

[2] https://docs.google.com/spreadsheets/d/1aWnsM4IaebADWmMgHBeWscwOp68C68lrXxAYMH8pQ9Y/edit?usp=sharing

Table 1
Classification of cybersecurity incidents from EUROPOL [4]

Class of Incident	Type of Incident	Description
Malware	Infection	Infecting one or various systems with a specific type of malware.
	Distribution	
	C&C	
	Undetermined	
Availability	DoS/DDoS	Disruption of the processing and response capacity of systems and networks in order to render them inoperative.
	Sabotage	Premeditated action to damage a system, interrupt a process, change or delete information, etc.
Gathering of information	Scanning	Active and passive gathering of information on systems or networks.
	Sniffing	Unauthorised monitoring and reading of network traffic.
	Phishing	Attempt to gather information on a user or a system through phishing methods.
Intrusion attempt	Exploitation of vulnerability	Attempt to intrude by exploiting a vulnerability in a system, component or network.
	Login attempt	Attempt to log in to services or authentication access control mechanisms.
Intrusion attempt	Exploitation of vulnerability	Actual intrusion by exploiting a vulnerability in the system, component or network.
	Compromising an account	Actual intrusion in a system, component or network by compromising a user or administrator account.
Information security	Unauthorised access	Unauthorised access to a particular set of information.
	Unauthorised modification/deletion	Unauthorised change or elimination of a particular set of information.
Fraud	Misuse or unauthorised use of resources	Use of institutional resources for purposes other than those intended.
	Illegitimate use of the name of a third party	Use of the name of an institution without permission to do so.
Abusive content	SPAM	Sending SPAM messages.
	Copyright	Distribution and sharing of copyright protected content.
	Child pornography, racism and apology of violence	Dissemination of content forbidden by law.
Other	Other	Other type of unspecified incident.

We also add another category to indicate whether the paper or article presents an issue, challenge or problem, or a solution. Unsurprisingly, considering that most works come from computing or other strongly technical disciplines, the large majority of the references relate to works presenting solutions (66 out of 78).

4.1. Works with a strong focus on Privacy

Also unsurprisingly, considering the nature of semantic web technologies and their purpose, many of the references included in our corpus relate to privacy (37 out of 78), with at least one annotation from the privacy taxonomy. A particularly frequent annotation there relates to the *Information Processing–Identification*. This category is mostly used to annotate works that relate to the general problem of anonymity and the anonymisation of personal data. These includes for example, [7] and [8] demonstrating how K-Anonymity can be applied to RDF datasets, [9] applying differential privacy to RDF data from social networks, and [10] looking into the problem of break-

Table 2
Taxonomy of tasks associated with IP distribution and usage policies.

Actor	Task	Description
Producer	Policy selection	Select or compose an appropriate policy for an artifact.
	Policy communication	Disseminate the policy to (potential) consumers.
	Monitoring	Monitor the use and distribution of the artifact for policy management.
	Policy enforcement	Put mechanisms in place to enforce compliance with the policy.
Consumer	Policy interpretation	Interpret the implications of the policy in their own context.
	Compatibility testing	Check that the policy is compatible with that of artifacts they are consuming/producing.
	Usage monitoring	Track usage of the artifact for policy compliance.
	Validation	Check that usage of the artifact is compliant with the policy.

Table 3
Sample paper classification.

Title	Privacy	Security	Policy
PrivOnto: a Semantic Framework for the Analysis of Privacy Policies [5]	Inf. collection, Inf. processing, Inf. dissemination,		Consumer, Policy Interpretation
Reasoning with Data Flows and Policy Propagation Rules [6][6]			Consumer, Usage Monitoring

ing the anonymisation of datasets through record linkage. While, [11] and [12] relate more to *Information Processing Exclusion*, which involves empowering citizens with transparency and control over personal data processing and sharing that concerns them.

Another common category addressed by works in our corpus is the one of *Information Collection*. While the two sub-categories *Surveillance* and *Interrogation* are rarely mentioned specifically, many works have used Semantic Web technologies to help users of online services to understand how and for what purpose data about them is being collected. This includes for example [13] which describes a tool to keep a record of the trackers encountered in a web user's everyday browsing, [14] looking more generally at transparency in data sharing on the web, or [15] looking specifically at restricting the collection of location data based on semantics and sensitivity.

Besides the aforementioned groups, several works including [5] or [16] look at privacy from a broader perspective, especially connecting privacy issues around *Information Dissemination–Increased accessibility* with the communication or interpretation of privacy policies and privacy preferences.

4.2. Works with a strong focus on Security

While rarely considered a core topic for Semantic Web research, many (46 out of 78) of the works in our corpus relate, in one way or another, to the topic of security. Most of those however focus entirely on the area of *Information Security*, with strong overlaps with the privacy and policy topics. Indeed, the large majority of the security references are classified under *Information Security–Unauthorized access* as they relate to solutions for access control either for Semantic Web related information [17–19] or that use Semantic Web technologies to support access control over other forms of data [20]. Access control frameworks defined upon Semantic Web technologies and languages have been proposed to support data producers in protecting their resources from *Unauthorized access*, allowing for *Policy enforcement* [21–24] and *Policy communication* [20, 25, 26]. These approaches rely on Semantic Web languages, i.e., RDF and SPARQL, to model their access control policies and to support the enforcement of the policies by the consumers. Additionally, the *Information Security* category includes works that investigate using existing encryption techniques to restrict access to RDF data [27–29].

Another interesting area in terms of *Information Security* where varied works can be found is in using ontologies as a basis for modeling, analysing and detect-

ing security issues. In those cases, mostly, ontologies are used as the knowledge base of an expert system, a representation schema or an annotation vocabulary for a complex, knowledge intensive security issue such as *Infection–Malware* detection/analysis [30, 31] or *Intrusion* detection [32, 33].

Interestingly other common security topics in relation to the *Gathering of Information* or *Abusive Content* (and to an extent, privacy) issues such as *SPAM* or *phishing* are rarely mentioned and are considered mostly within problem description papers in relation to Semantic Web technologies, as in [34, 35].

4.3. Works with a strong focus on Policies

With the increasing amount of (creative) content being published online, policies about IP distribution and usage are becoming more and more important, as they allow for the association of constraints relating to use and reuse. In this context, the contribution of Semantic Web technologies and languages is twofold: they may be used to support the *Producer* in associating machine-readable IP distribution and usage policies with the data that they are publishing on the Web, and they may support *Consumers* in checking whether the intended use of a certain resource published online is allowed or not. In total 33 out of 78 of the works in our corpus were associated with the policy topic, many of which were also associated either with the *Information Processing* or *Information Security–Unauthorized access* topics, indicative of the strong relationship between privacy, access control and policies research.

From the point of view of supporting and easing the activities of Producers, several approaches have been proposed in the last years. Concerning *Policy communication*, Rodriguez-Doncel *et al.* [36] proposed a dataset of over 100 licenses written in RDF extensively using ODRL.[3] They include licenses for data (like Open Data Commons), software (like Apache, MIT or BSD licenses), and general works (like Creative Commons licenses). Data producers can associate such machine-readable licenses to their resource thus indicating the conditions of reuse. This dataset is at the base of the Licentia[4] which aims at supporting *Policy selection*. More precisely, the goal of Licentia is to support producers in understanding license terms, licenses compatibility checking, and licenses graphical visualisation [37], similarly also to what is described in [38]. Additionally, ORDL has been used to model access and usage control policies [26, 39, 40], providing more evidence that there is a strong overlap between privacy, security and policies.

Other challenges deal with the Consumer point of view, where issues like compatibility testing and usage monitoring need to be addressed to assist Consumers in gaining a better understanding of the policies, thus supporting the compliant usage of protected resources. Works considering for example *Usage Monitoring* of data artifacts are therefore starting to appear (cf. [6, 41]). Those works strongly relate to the idea of making policies understandable to the consumers of data and information services, with Semantic Web technologies having a role to play in the task of *Policy Interpretation*. Works such as [5] and [16] specifically address this task in the context of privacy policies, while for IP policies, current works remain limited to usage monitoring. In addition to the challenging issue of *Usage Monitoring*, the problem of *Compatibility testing* has been addressed by combining deontic logic and Semantic Web technologies and languages [42].

5. Conclusion: Trends and open challenges Semantic Web security, privacy and policy

As can be seen from the analysis described in the previous sections, and further from the annotated corpus of collected references, research work related to Semantic Web technologies has been, at least for privacy and security, strongly focusing on a small subset of issues and challenges. Indeed, the strong prominence of references related to controlling data collection mechanisms and access control shows that, as is often the case in primarily technological disciplines, privacy and security are often reduced to those basic issues. While in security, some works have been looking at *applying* Semantic Web technologies for example to malware, SPAM or intrusion detection, very few have tackled less computational issues such as fraud detection, and even less have been looking at the specific security implications of Semantic Web technologies (with notable exceptions that remain, however, at a very high level).

Beyond security, the contrast between the description and study of privacy in the social sciences, portraying the issue as a complex, multifaceted and interdisciplinary notion, and its treatment in the Semantic Web literature is striking. Many of the papers re-

[3] http://w3c.github.io/poe/model/
[4] http://licentia.inria.fr/

viewed consider privacy as a single, specific (and often purely technical challenge), related most often either to identification, or to the control of either data collection or data access. Again, with some exceptions, very few works really consider the potential of Semantic Web technologies to either create or address issues such as appropriation, distortion, or broadly, information dissemination, and none has considered the challenges associated with invasion. While this is not necessarily surprising, considering the technological nature of Semantic Web research, its purpose, and the specific issues it tackles, it is disappointing to see that these technologies are not being used more creatively to address other challenges where their sense-making and inferential capability would no doubt have benefits. It is also disappointing that, as far as we could see from the references collected, those technologies are rarely being included in broader, interdisciplinary discussions about their potential privacy implications.

The policy part of our brief analysis stands out from the two others as being somehow more varied. Unsurprisingly, issues of policy communication have attracted more consideration as being more directly within the remit of the representation languages and formalisms of the Semantic Web. However, a few works have started to appear that use those representational capabilities to support interpreting, monitoring and reasoning upon policies (often related to privacy and access control, but also related to intellectual property management). Those works address issues of rights associated with information assets, and therefore overlap with research in legal informatics where Semantic Web technologies have had many contributions (which are, however, mostly out of the scope of this article). There is nevertheless much work to be done, from the few starting points we encountered, on the implications of using Semantic Web technologies to support both data producers and consumers (including private individuals) in understanding, combining and interpreting policies in a meaningful and valuable way.

References

[1] D.J. Solove, A taxonomy of privacy, *U. Pa. L. Rev.* **154** (2005), 477.

[2] J.J. Cebula, M.E. Popeck and L.R. Young, A taxonomy of operational cyber security risks version 2, Technical Report, CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2014, https://doi.org/10.13140/rg.2.2.23973.91363.

[3] L. Marinos, ENISA Threat Taxonomy: A tool for structuring threat information, ENISA, Heraklion, 2016.

[4] E. EC3, Common Taxonomy for the National Network of (CSIRTs), EUROPOL European Cybercrime Centre, 2016.

[5] A. Oltramari, D. Piraviperumal, F. Schaub, S. Wilson, S. Cherivirala, T.B. Norton, N.C. Russell, P. Story, J. Reidenberg and N. Sadeh, PrivOnto: a Semantic Framework for the Analysis of Privacy Policies, *Semantic Web Journal* **9**(2) (2018).

[6] E. Daga, A. Gangemi and E. Motta, Reasoning with Data Flows and Policy Propagation Rules, *Semantic Web Journal* **9**(2) (2018).

[7] F. Radulovic, R. García Castro and A. Gómez-Pérez, Towards the anonymisation of RDF data (2015). doi:10.18293/SEKE2015-167. https://doi.org/10.18293/SEKE2015-167.

[8] B. Heitmann, F. Hermsen and S. Decker, k–RDF-Neighbourhood Anonymity: Combining Structural and Attribute-based Anonymisation for Linked Data, in: *5th Workshop on Society, Privacy and the Semantic Web - Policy and Technology (PrivOn2017) (PrivOn)*, C. Brewster, M. Cheatham, M. d'Aquin, S. Decker and S. Kirrane, eds, CEUR Workshop Proceedings, Aachen, 2017, ISSN 1613-0073. http://ceur-ws.org/Vol-1951/#paper-03.

[9] R.R.C. Silva, B.C. Leal, F.T. Brito, V.M.P. Vidal and J.C. Machado, A Differentially Private Approach for Querying RDF Data of Social Networks, in: *Proceedings of the 21st International Database Engineering & Applications Symposium*, IDEAS 2017, ACM, New York, NY, USA, 2017, pp. 74–81. ISBN 978-1-4503-5220-8. doi:10.1145/3105831.3105838. http://doi.acm.org/10.1145/3105831.3105838.

[10] J. Miracle and M. Cheatham, Semantic Web Enabled Record Linkage Attacks on Anonymized Data, in: *4th Workshop on Society, Privacy and the Semantic Web - Policy and Technology (PrivOn2016) (PrivOn)*, C. Brewster, M. Cheatham, M. d'Aquin, S. Decker and S. Kirrane, eds, CEUR Workshop Proceedings, Aachen, 2016, ISSN 1613-0073. http://ceur-ws.org/Vol-1750/#paper-03.

[11] M. d'Aquin, S. Elahi and E. Motta, Semantic Monitoring of Personal Web Activity to Support the Management of Trust and Privacy, in: *Proceedings of the Second Workshop on Trust and Privacy on the Social and Semantic Web (SPOT2010)*, CEUR-WS.org, 2010. http://CEUR-WS.org/Vol-576/paper2.pdf.

[12] P.A. Bonatti, S. Kirrane, A. Polleres and R. Wenning, Transparent Personal Data Processing: The Road Ahead, in: *Computer Safety, Reliability, and Security - SAFECOMP 2017 Workshops, ASSURE, DECSoS, SASSUR, TELERISE, and TIPS, Trento, Italy, September 12, 2017, Proceedings*, 2017, pp. 337–349. doi:10.1007/978-3-319-66284-8_28. https://doi.org/10.1007/978-3-319-66284-8_28.

[13] N. Guha, Spy watch: a tool for transparency in web tracking, in: *Proceedings of the Privon 2013 workshop on Society, Privacy and the Semantic Web-Policy and Technology*, CEUR-WS.org, 2013, pp. 60–66.

[14] M. d'Aquin and K. Thomas, Semantic Web Technologies for Social Translucence and Privacy Mirrors on the Web., in: *Proceedings of the Privon 2013 workshop on Society, Privacy and the Semantic Web-Policy and Technology*, CEUR-WS.org, 2013, pp. 60–66.

[15] B. Agir, J.-P. Calbimonte and K. Aberer, Semantic and sensitivity aware location privacy protection for the internet of things, in: *Proceedings of the Privon 2014 workshop on Society, Privacy and the Semantic Web-Policy and Technology*, CEUR-WS.org, 2014, pp. 58–63.

[16] D. Ceolin, L. Aroyo and J. Duinker, Modeling Social Web Privacy to Detect Perception Gaps, in: *Proceedings of the Privon 2015 workshop on Society, Privacy and the Semantic Web-Policy and Technology*, 2015, https://sites.google.com/site/privon2015/program.

[17] A. Padia, T. Finin and A. Joshi, Attribute-based Fine Grained Access Control for Triple Stores, in: *Proceedings of the Privon 2015 workshop on Society, Privacy and the Semantic Web-Policy and Technology*, 2015, https://sites.google.com/site/privon2015/program.

[18] N. Fornara and F. Marfia, Modeling and Enforcing Access Control Obligations for SPARQL-DL Queries, in: *Proceedings of the 12th International Conference on Semantic Systems*, SEMANTiCS 2016, ACM, New York, NY, USA, 2016, pp. 145–152. ISBN 978-1-4503-4752-5. doi:10.1145/2993318.2993337. http://doi.acm.org/10.1145/2993318.2993337.

[19] S. Kirrane, A. Mileo and S. Decker, Applying DAC principles to the RDF graph data model, in: *IFIP International Information Security Conference*, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013, pp. 69–82. ISBN 978-3-642-39218-4. doi:10.1007/978-3-642-39218-4_6. https://doi.org/10.1007/978-3-642-39218-4_6.

[20] O. Sacco and A. Passant, A Privacy Preference Ontology (PPO) for Linked Data, in: *WWW2011 Workshop on Linked Data on the Web, Hyderabad, India, March 29, 2011*, C. Bizer, T. Heath, T. Berners-Lee and M. Hausenblas, eds, CEUR Workshop Proceedings, Vol. 813, CEUR-WS.org, 2011. http://ceur-ws.org/Vol-813/ldow2011-paper01.pdf.

[21] A. Gabillon and L. Letouzey, A View Based Access Control Model for SPARQL, in: *Fourth International Conference on Network and System Security, NSS 2010, Melbourne, Victoria, Australia, September 1-3, 2010*, Y. Xiang, P. Samarati, J. Hu, W. Zhou and A. Sadeghi, eds, IEEE Computer Society, 2010, pp. 105–112. ISBN 978-1-4244-8484-3. http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=5634608.

[22] L. Costabello, S. Villata and F. Gandon, Context-Aware Access Control for RDF Graph Stores, in: *ECAI 2012 - 20th European Conference on Artificial Intelligence. Including Prestigious Applications of Artificial Intelligence (PAIS-2012) System Demonstrations Track, Montpellier, France, August 27-31 , 2012*, L.D. Raedt, C. Bessière, D. Dubois, P. Doherty, P. Frasconi, F. Heintz and P.J.F. Lucas, eds, Frontiers in Artificial Intelligence and Applications, Vol. 242, IOS Press, 2012, pp. 282–287. ISBN 978-1-61499-097-0. http://www.booksonline.iospress.nl/Content/View.aspx?piid=31572.

[23] J. Rachapalli, V. Khadilkar, M. Kantarcioglu and B.M. Thuraisingham, Towards fine grained RDF access control, in: *19th ACM Symposium on Access Control Models and Technologies, SACMAT '14, London, ON, Canada - June 25 - 27, 2014*, S.L. Osborn, M.V. Tripunitara and I. Molloy, eds, ACM, 2014, pp. 165–176. ISBN 978-1-4503-2939-2. doi:10.1145/2613087. http://doi.acm.org/10.1145/2613087.

[24] S. Kirrane, A. Abdelrahman, A. Mileo and S. Decker, Secure Manipulation of Linked Data, in: *The Semantic Web - ISWC 2013*, Lecture Notes in Computer Science, Vol. 8218, Springer Berlin Heidelberg, 2013, pp. 248–263. http://dx.doi.org/10.1007/978-3-642-41335-3_16.

[25] G. Flouris, I. Fundulaki, M. Michou and G. Antoniou, Controlling Access to RDF Graphs, in: *Future Internet - FIS 2010 - Third Future Internet Symposium, Berlin, Germany, September 20-22, 2010. Proceedings*, A. Berre, A. Gómez-Pérez, K. Tutschku and D. Fensel, eds, Lecture Notes in Computer Science, Vol. 6369, Springer, 2010, pp. 107–117. ISBN 978-3-642-15876-6. doi:10.1007/978-3-642-15877-3. https://doi.org/10.1007/978-3-642-15877-3.

[26] S. Steyskal and S. Kirrane, If you can't enforce it, contract it: Enforceability in Policy-Driven (Linked) Data Markets, in: *Joint Proceedings of the Posters and Demos Track of 11th International Conference on Semantic Systems - SEMANTiCS 2015 and 1st Workshop on Data Science: Methods, Technology and Applications (DSci15) 11th International Conference on Semantic Systems - SEMANTiCS 2015, Vienna, Austria, September 15-17, 2015.*, 2015, pp. 63–66. http://ceur-ws.org/Vol-1481/paper21.pdf.

[27] A. Kasten, A. Scherp, F. Armknecht and M. Krause, Towards Search on Encrypted Graph Data, in: *Proceedings of the 2013th International Conference on Society, Privacy and the Semantic Web - Policy and Technology - Volume 1121*, PrivOn'13, CEUR-WS.org, Aachen, Germany, Germany, 2013, pp. 46–57. http://dl.acm.org/citation.cfm?id=2874535.2874540.

[28] S. Gerbracht, Possibilities to encrypt an RDF-Graph, in: *Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on*, IEEE, 2008, pp. 1–6.

[29] J.D. Fernández, S. Kirrane, A. Polleres and S. Steyskal, Self-Enforcing Access Control for Encrypted RDF, in: *The Semantic Web - 14th International Conference, ESWC 2017, Portorož, Slovenia, May 28 - June 1, 2017, Proceedings, Part I*, E. Blomqvist, D. Maynard, A. Gangemi, R. Hoekstra, P. Hitzler and O. Hartig, eds, Lecture Notes in Computer Science, Vol. 10249, 2017, pp. 607–622. ISBN 978-3-319-58067-8. doi:10.1007/978-3-319-58068-5. https://doi.org/10.1007/978-3-319-58068-5.

[30] T. Tafazzoli and S.H. Sadjadi, Malware fuzzy ontology for semantic web, *International Journal of Computer Science and Network Security* **8**(7) (2008), 153–161.

[31] R. Carvalho, M. Goldsmith and S. Creese, Malware investigation using semantic technologies (2016), https://iesd2016.wordpress.com/program/.

[32] W. Li and S. Tian, An ontology-based intrusion alerts correlation system, *Expert Systems with Applications* **37**(10) (2010), 7138–7146, ISSN 0957-4174. doi:https://doi.org/10.1016/j.eswa.2010.03.068. http://www.sciencedirect.com/science/article/pii/S095741741000271X.

[33] Y.-T.F. Chan, C.A. Shoniregun, G.A. Akmayeva and A. Al-Dahoud, Applying semantic web and user behavior analysis to enforce the intrusion detection system, in: *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*, IEEE, 2009, pp. 1–5, https://doi.org/10.1109/ICITST.2009.5402616.

[34] A. Hasnain, M. Al-Bakri, L. Costabello, Z. Cong, I. Davis and T. Heath, Spamming in linked data, in: *Proceedings of the Third Workshop on Consuming Linked Data (COLD)*, CEUR-WS.org, 2012, pp. 39–50.

[35] P. Nasirifard, M. Hausenblas and S. Decker, Privacy concerns of FOAF-based linked data, in: *Trust and Privacy on the Social and Semantic Web Workshop (SPOT 09) at ESWC09, Heraklion, Greece*, 2009.

[36] V. Rodríguez-Doncel, S. Villata and A. Gómez-Pérez, A dataset of RDF licenses, in: *Legal Knowledge and Information Systems - JURIX 2014: The Twenty-Seventh Annual Conference, Jagiellonian University, Krakow, Poland, 10-12 December 2014*, R. Hoekstra, ed., Frontiers in Artificial Intelligence and Applications, Vol. 271, IOS Press, 2014, pp. 187–188. ISBN 978-1-61499-467-1. doi:10.3233/978-1-61499-468-8-187. https://doi.org/10.3233/978-1-61499-468-8-187.

[37] C. Cardellino, S. Villata, F. Gandon, G. Governatori, H. Lam and A. Rotolo, Licentia: a Tool for Supporting Users in Data Licensing on the Web of Data, in: *Proceedings of the ISWC 2014 Posters & Demonstrations Track a track within the 13th International Semantic Web Conference, ISWC 2014, Riva del Garda, Italy, October 21, 2014.*, M. Horridge, M. Rospocher and J. van Ossenbruggen, eds, CEUR Workshop Proceedings, Vol. 1272, CEUR-WS.org, 2014, pp. 277–280. http://ceur-ws.org/Vol-1272/paper_54.pdf.

[38] E. Daga, M. d'Aquin, E. Motta and A. Gangemi, A bottom-up approach for licences classification and selection, in: *Revised Selected Papers of the ESWC 2015 Satellite Events on The Semantic Web: ESWC 2015 Satellite*, Springer, 2015, pp. 257–267, https://doi.org/10.1007/978-3-319-25639-9_41.

[39] S. Steyskal and A. Polleres, Defining expressive access policies for linked data using the ODRL ontology 2.0, in: *Proceedings of the 10th International Conference on Semantic Systems, SEMANTICS 2014, Leipzig, Germany, September 4-5, 2014*, H. Sack, A. Filipowska, J. Lehmann and S. Hellmann, eds, ACM, 2014, pp. 20–23. ISBN 978-1-4503-2927-9. doi:10.1145/2660517.2660530. http://doi.acm.org/10.1145/2660517.2660530.

[40] K. Fatema, E. Hadziselimovic, H.J. Pandit, C. Debruyne, D. Lewis and D. O'Sullivan, Compliance through Informed Consent: Semantic Based Consent Permission and Data Management Model, in: *5th Workshop on Society, Privacy and the Semantic Web - Policy and Technology (PrivOn2017) (PrivOn)*, C. Brewster, M. Cheatham, M. d'Aquin, S. Decker and S. Kirrane, eds, CEUR Workshop Proceedings, Aachen, 2017, ISSN 1613-0073. http://ceur-ws.org/Vol-1951/#paper-05.

[41] E. Daga, M. d'Aquin, A. Gangemi and E. Motta, Propagation of policies in rich data flows, in: *Proceedings of the 8th International Conference on Knowledge Capture*, ACM, 2015, p. 5, https://doi.org/10.1145/2815833.2815839.

[42] G. Governatori, A. Rotolo, S. Villata and F. Gandon, One License to Compose Them All - A Deontic Logic Approach to Data Licensing on the Web of Data, in: *The Semantic Web - ISWC 2013 - 12th International Semantic Web Conference, Sydney, NSW, Australia, October 21-25, 2013, Proceedings, Part I*, H. Alani, L. Kagal, A. Fokoue, P.T. Groth, C. Biemann, J.X. Parreira, L. Aroyo, N.F. Noy, C. Welty and K. Janowicz, eds, Lecture Notes in Computer Science, Vol. 8218, Springer, 2013, pp. 151–166. ISBN 978-3-642-41334-6. doi:10.1007/978-3-642-41335-3. https://doi.org/10.1007/978-3-642-41335-3.

[43] C. Brewster, M. Cheatham, M. d'Aquin, S. Decker and S. Kirrane (eds), Proceedings of the 5th Workshop on Society, Privacy and the Semantic Web - Policy and Technology (PrivOn2017) (PrivOn), in: *5th Workshop on Society, Privacy and the Semantic Web - Policy and Technology (PrivOn2017) (PrivOn)*, CEUR Workshop Proceedings, Aachen, 2017, ISSN 1613-0073. http://ceur-ws.org/Vol-1951/.