Exploration of Norms and Policies in Digital Fashion Domain Using Semantic Web Technologies

Soheil Roshankish and Nicoletta Fornara

USI - Università della Svizzera italiana, Via Buffi 13, 6904 Lugano, Switzerland
{soheil.roshankish,nicoletta.fornara}@usi.ch

Abstract. Nowadays, one of the problems in policy notice of fashion companies is that they are not provided in a machine-readable format; therefore, they cannot be searched and monitored by computers. The fact that most of fashion brands transform their sales into digital format magnifies the importance of automation in policy management for the future of digital business in general and of fashion companies in particular. In this paper, we explore the use of privacy policies of companies in the digital fashion domain not only to protect customers' data but for making it feasible for companies to understand their customers' needs easier and faster. We describe how the Open Digital Rights Language (ODRL), a W3C recommendation for expressing policies using Semantic Web Technologies, can be applied in the field of digital fashion. We then discuss the required components for making it possible to use such a policy language for monitoring and enforcement services.

Keywords: digital fashion, policy, privacy, semantic web.

1 Introduction

Today, the number of companies using digital technologies for communicating with their customers is increasing expeditiously. After Covid-19 pandemic, traffic to the top 100 fashion brands' owned websites increased up to 45 percent in Europe in April 2020[1]. Meanwhile, Human Computer Interaction (HCI) studies are trying to enhance this connection in e-commerce by developing new technologies. Talking about e-commerce, the global fashion industry with the revenue of 606 billion dollars by 2020 has a major role in the economy of every country[2][1]. However, in digital fashion, there are numerous privacy concerns for companies and brands for the digital transformation of their industry[3][4].

Digital fashion communication embraces communication brands designers and clothes online [5] while using the official media and technological channels such as websites, social media, Augmented Reality applications [6], Haptic Technologies [7] and many others to reach customers [8]. In this paper, we tackle customer's privacy as one of the major challenges in digital fashion. Although all the companies are obliged

[1] https://www.shopify.com/enterprise/ecommerce-fashion-industry

to inform their clients about their policies before using their data, still we face a big gap in this area. For example, if somebody wants to shop on Zalando website, they should create an account and accept terms and conditions provided by Zalando before buying their favourite shoes. It means that they should read over 19,000 words (48 pages in Zalando UK) and consent to practices described in it[9]. That may be the reason why we are not surprised by the result of the survey done by Deloitte in USA showing that 91% of users consent their legal rights without reading them [10].

If we calculate the time to read this policy as 250 words per minute[11], which is a common reading rate for people with the high school education[12], it takes over 75 minutes to read the policy notes of Zalando. The results show that if Internet users want to read their online privacy polices word by word each time they visit a new website, it costs billions of dollars nationally for the country[11].

In the last decades, discussion about privacy policies have been one of the major subjects in e-commerce applications. In digital fashion, this issue could be crucial since companies could collect rich and accurate personal information about the customers. For example, fashion label Tommy Hilfiger introduced new technology in 2018 using smart chips in its products to collect information about how often the items would be worn by the customers[13]. Though Tommy Hilfiger insured that customers' data is encrypted and cannot be accessed without any permission, it still concerns privacy issues that must be addressed.

Since 2018, all companies must comply with the requirements of the General Data Protection Regulation (GDPR) regarding the collection and handling of customer data. For instance, brands should inform customers about how data will be collected, stored, and used, or whether it will be shared with any third parties. Even having customers' permission to use their data, they have the right to access their collected data or even delete them [14].

Although GDPR requires the costumers' consent for fashion brands to collect their data (same for the Tommy Hilfiger case), as mentioned before, most of the people do no read terms and conditions of the websites before registering their information. Therefore, there is not control whether or not companies are violating customer's privacy policies and we believe that transforming this process, thanks to the use of machine-readable formats, helps both parties understand their rights in addition to improving customers' satisfaction.

If we want to solve this problem, we need to address the various issues that cause it. First of all, companies should start expressing their privacy policies in a machine-readable format. It is undoubtedly difficult to take such a measure, and in this paper, we propose to do that by using an existing policy expression language and Semantic Web Technologies. Having done so, we need to create a software infrastructure that can handle the meaning of policies when it is specified in a format that computers can process. To achieve this, the notation used to express privacy policies must have a formal semantics that allows computers to infer conclusions from the data collected on the behaviour of the involved parties and from the policies adopted. Therefore, we will discuss the required components for making it possible to use such a policy language for monitoring and enforcement services and we will briefly present two works that attempt to solve such a problem.

This paper is organized as follows. In Section 2 the methodology adopted in this paper is described. In Section 3, the Semantic Web Technologies used in this paper are introduced. In Section 4 the ODRL policy expression language, which is W3C Recommendation since 2018, is introduced. In Section 5, we address the importance of policy monitoring and outline the necessary components that a system should have to accomplish such monitoring automatically, including some references to work proposing solutions to this problem.

2 Methodology

In this paper, we propose an approach for modelling and monitoring policies of brands and companies in the digital fashion domain not only to protect customers' data but for making it feasible for companies to understand their customer's needs easier and faster.

In Artificial Intelligence literature, there exist various languages that can be used for the specification of policies using Semantic Web Technologies [15]. One of them is the W3C Recommendation Open Digital Rights Language (ODRL 2.2)[2]. It is a policy expression language that can be used to represent permitted and prohibited actions over a certain asset, and obligations that should be meet by various stakeholders. This language can be used to express the deontic aspect of fashion policies in a machine-readable format.

In addition, in order to be able to unambiguously formalize the actions that should or should not be performed over fashion products, as for example e-commerce actions related to clothes realized with specific materials, it is required to formalize those actions and the properties for describing fashion products using Semantic Web Technologies. In particular, the definition of sharable fashion ontologies and knowledge graphs is fundamental. In literature there are some examples of ontologies used in the fashion domain[16] [17] [2] but it is not yet clear if they are expressive enough to be used for the specification of the actions regulated by policies and for taking advantage of automatic reasoning in the fashion domain.

Finally, in order to provide monitoring services for the evolution in time of deontic policies (e.g. computing the fulfilment or violation of obligations and prohibitions) a formal semantics for the ODRL policy language is required. One attempt to extend the ODRL language and to specify its formal semantics has been proposed in [18]. In this approach different ontologies (such as a domain-specific ontology, the OWL Time Ontology[3] and an Event Ontology[19]) have been used. Therefore, in order to use this model for fashion-related policies, the domain-specific ontology must be a rich and expressive fashion ontology.

[2] https://www.w3.org/TR/odrl-model/
[3] https://www.w3.org/TR/owl-time/

3 Semantic Web Technologies in Digital Fashion

Nowadays, norms and policies for regulating the use of personal data and digital assets in digital business in general and in the fashion industry in particular are only expressed in a human-readable format. This means that customers should read the policy terms of the companies before they are able to order their products online and understand all the implications of their actions. In this paper, we propose to use Semantic Web technologies to express those policies and automatically reason about their meaning. This section is a brief introduction to the Semantic Web technologies used in the next sections and explains why the Semantic Web can have a significant impact on the fashion industry today and in the near future.

3.1 Semantic Web and Semantic Web Technologies

There are growing appeals for using Semantic Web in many research areas, since Tim Berners- Lee introduced the Semantic Web (or Web of Data) in 1999. Semantic Web is an extension of current World Wide Web (WWW), in which information is given well-defined meaning that helps computers and people communicate and understand each other's needs [20] [21].

The important goal of the Semantic Web is to help advanced applications improve their search, navigation, and evaluation by making knowledge widely accessible. One of the key benefits of the Semantic Web is enabling computers to read the information in structured format. The strength of Semantic Web lies in modelling the knowledge (our privacy policies) in such a way that computers can draw conclusions from given information.

To have such flexibility we can use Semantic Web Technologies to translate the data to the formal computers' language. All the technologies presented in this paper, have been defined under the lead of the World Wide Web Consortium (W3C).

The eXtensible Markup Language (XML) and the Resource Description Framework (RDF) are the two important technologies for developing the Semantic Web. XML is a text based *Markup Language* which can be used to label structured data by using tags [22]. The meaning of each tag is determined by the mutual agreement of those who are using a specific XML language [23], but XML documents do not have formal semantics. Unfortunately, merging XML data is rather complicated and the result is not always clear.

This limit is exceeded by RDF (Resource Description Framework), which is a formal language for describing structured information. RDF is often considered as the basic representation format for developing Semantic Web. In contrast with XML, the goal of RDF is not only displaying information in a machine-readable format but also exchanging it on the Web while preserving its original meaning.

RDF documents can be used to represent the relation among resources using labelled directed graphs. In this case, the nodes are our *resources* and the *relations* are the edge of the graph. For example, the fact that CompanyX collects customer David's personal information can be represented with the following graph:

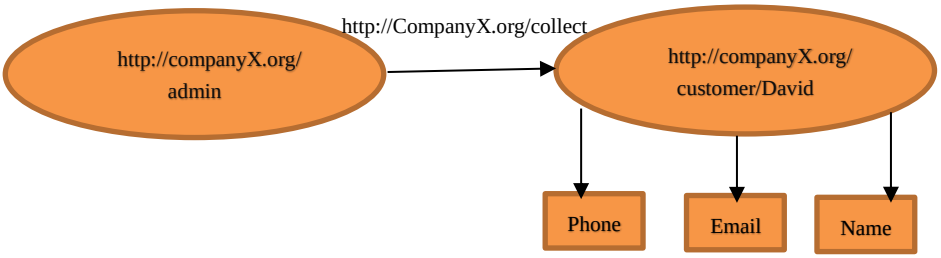

Fig. 1. An RDF graph for describing a customer data.

As it is shown in Figure 1, RDF uses naming system called Universal Resource Identifier (URI). URI is a standard syntax which helps us to simply identify the resources and exchange information on the Web and generally can be assigned to any object that has a clear identity in the privacy policy of the company .In [20], you can find further information about how to create well-formed URIs.

One of the advantages of representing data as RDF graphs is that it is very simple to combine data from multiple sources. This measure is not possible for XML documents because they are encoded in tree structure and simple union of two tree structures is not a tree anymore. In the previous example, we represented *phone*, *email*, and *name* as data values or *literals. Literals* are reserved names for RDF resources of a certain datatype and their values are usually represented as a string like "+417955555", "david@gmail.com" and "David".

When companies want to express an application independent knowledge on a given domain, it is possible to use RDF Schema. RDF Schema can be used to express schema or terminological knowledge. A well-known example of RDF Schema is *Schema.org* a vocabulary that is used by search engines and web applications to empower their user experience. RDF Schema has a formal semantics; therefore, we can use RDF reasoners for inferring implicit knowledge from the knowledge that is stated explicitly. For example, by using the clothing materials ontology[4] we can infer that a Lycra blouse is done with synthetic fibre.

Now that we know how knowledge can be represented using Semantic Web Technologies, in the next section we present some examples of well-known fashion companies that are currently using Semantic Web technologies to improve their sales and personalization approach.

3.2 Related Works Using Semantic Web Technologies in Digital Fashion

As far as we know, there is no previous research using Semantic Web Technologies (SWT) for monitoring privacy policies in digital fashion. However, SWT have been

[4] https://jbarrasa.com/2019/11/25/quickgraph9-the-fashion-knowledge-graph-inferencing-with-ontologies-in-neo4j/

applied in this domain for other purposes. In [24], they show how in the RISED (Refactoring Imperial[5] Selling Data) project they manage the collected data from customers using Semantic Web Technologies. They created the Imperial Data Ontology (IDO) and developed visualization tools to analyse all the sale data coming from different databases. One practical advantage of their method is that it can be used to answer to many queries that could help the company's sales. For example, the sales department can easily ask to the system "What are the best-selling colours within a certain period of time?".

Offering over 2,000 brands in 15 different countries, Zalando is one of the most successful Europe's leading online platform for fashion. Katariina Kari in Zalando's engineering blog [2] explains how they used SWT to improve their customers service and personalization by:

- Suggesting links to the customers for further browsing.
- Implementing business rules. For instance, if customer is browsing a particular brand, the system will not suggest the competing brand.
- Understanding the characteristics of attributes. For example, if the customer search for the vegan coats, then the leather coats will not be appeared in the result list.

More and more companies are going to use Semantic Web Technologies in the next few years. These related works show just few advantages of using Semantic Web in digital fashion domain.

4 The Open Digital Rights Language

All the fashion brands using the Internet as platform to offer their products to their customers must fulfil the General Data Production Regulation (GDPR) since it was introduced in May 2018. There exist some tools such as Microsoft Trust Centre[14] and TrustArc [25] which can be used manually by companies to help in assessing the GDPR regulations. However, as the number of companies in the digital fashion world grows, the automated compliance checking approach can ease these processes [24].
First, we need a formal language for specifying our policies. In this section, we describe the ODRL information model and its core classes. Moreover, we show how it is possible to use the ODRL language for formalizing some examples of privacy policies used in the digital fashion domain.

4.1 The ODRL Information Model

In general, Digital Rights Management (DRM) systems are responsible for describing, layering, analyzing, trading, and monitoring of the rights over digital or physical assets on the Web of Data [26]. Right Expression Languages (REL) is a fundamental part of DRM system, which is machine-readable language, used to express the rights.

[5] Imperial Fashion is one of well-known fast-fashion in Italy

There are several REL standards such as XrML [27], MPEG 21 [28] and other initiatives, but the most common REL standard is the Open Digital Rights Language (ODRL) [29].

The ODRL Information Model[6] defines a set of core classes and properties for expressing a *Policy*[7]. A *Policy* must contain at least one *Rule* object, that is, one object belonging to one of the *Rule* subclasses that are *Permission*, *Prohibition*, or *Duty*. For example, one policy can describe the permission to use customers' contact details and another one can represent the prohibition of sharing customers' sensitive data.

A *Policy* object must belong to one of the following three policy types: *Set*, *Offer*, or *Agreement*. The *Set* policy is the default type in which any combination of *Rules* can be represented. The *Offer* subclass represents *Rules* that are being offered from an assigner and normally targets a wider audience. The *Agreement* subclass represents *Rules* that are granted from an assigner to an assignee. Normally in digital fashion when we use terms assigner and assignee, we consider the fashion companies as an assigner who choose the terms of policies and customers as assignee. When there exists an agreement, it means we must have at least one assigner and one assignee. Most of the privacy policies terms are of type *Agreement*. For example, the *Agreement* between a customer and a company about which customer data should be collected by company.

Every *Policy* has a unique identifier. A *Policy* regulates the *Actions* performed on an *Asset*, which is any physical or digital resource or collection of resources. Examples of *Asset* are the email or the telephone number of a customer. The *Actions* are labels that can be specified using *Constraints*, which are Boolean or logical expressions. *Actions* can be for example "*use*", "*share*", '*transfer*", or "*play*". On *Action* can be permitted on a given asset whereas another one can be prohibited. In addition, we can consider some constraints for each *Action*. For example, customers can give permission to the company to collect their contact details, but company can contact the customers only via email. A Policy involves some *Parties*, which are a person, a collection of people, an organisation, or an agent. For instance, fashion companies are the parties that provide services for other parties like customers.

A *Rule*, which can be a *Permission*, a *Prohibition* or a *Duty*, can be constrained by a condition, if the condition holds the *Rule* becomes in force. In particular: a *Permission* is used for allowing an *Action*, when all refinements satisfied, to be exercised on an *Asset*. A *Prohibition* disallows an action, with all refinements satisfied, to be exercised on an *Asset* even if all constraints are satisfied. Finally, a *Duty* represents the obligation to exercise an action, with all refinements satisfied. For example, in some fashion websites, customers can be obliged to pay (as a *Duty*) small amount of money if they want to access VIP services. In the next session, we will analyse some existing policies used in the digital fashion and formalize them using the ODRL language in order to express them in a machine-readable format.

[6] The ODRL Information Model is available at https://www.w3.org/TR/odrl-model/#infoModel
[7] We use capital letter for referring to ODRL classes.

4.2 Examples of ODRL policies for the fashion domain

In this Section we will formalize an existing privacy policy, which is taken from Zalando's web site (Zalando Privacy Notice,2020.) by using ODRL. We want to clarify that Zalando does not use our approach and to the best of our knowledge, neither Zalando nor any fashion company use automated methods for their policy compliance checking processes.

Fig. 2. Zalando data collection policy when a customer contacts them

Data collection procedure varies in Zalando based on wide range of communication between customers and company. Figure 2. Shows the policy of the collection of data while a customer contacts Zalando. As it is shown many personal data can be collected depends on how the company is contacted. Such a permission can be represented in ODRL as illustrated in Figure 3. To make the formalization of the policy simple, we will formalize only some of the personal information mentioned in the policy reported in Figure 2 (i.e. phone number and email). More details on the syntax of ODRL policies can be find on ODRL website[8].

```
{   "@context": "http://www.w3.org/ns/odrl.jsonld",
    "@type": "Set",
    "uid": "http://example.com/policy:1001",
    "permission": [{
        "target": "http://example.com/asset:1008.phone",
        "target": "http://example.com/asset:1009.email",
        "action": "archive"    }] }
```

Fig. 3. Representation of the permission to archive customer's contact details such as email and phone number in ODRL

Figure 4 shows an example of agreement between CompanyX and user David to use the hometown of the customer. Such an information could significantly improve the sale of the company by getting information about bestselling article in each city [22]. Figure 5 represents a policy that includes two rules one permission and one prohibition on the same resource, "phone number". Customer David give the permission to the

[8] https://www.w3.org/TR/odrl-model/.

company to collect his phone information but on the other hand the company is prohibited to share such data to the third parties. In addition, if any conflicts happen between *Prohibition* and *Permission*, the *conflict* property term indicates that which one will take precedence. In this example the *conflict* property is set to *perm* which means that the *Permission* has priority over the *Prohibition*.

```
{ "@context": "http://www.w3.org/ns/odrl.jsonld",
"@type": "Agreement",
"uid": "http://example.com/policy:1002",
"profile": "http://example.com/odrl:profile:01",
"permission": [{
"target":  "http://example.com/asset:9898.hometown",
"assigner": "http://example.com/party:org:CompanyX",
"assignee": "http://example.com/party:person:CustomerDavid",
"action": "use"   }]  }}
```

Fig. 4. Representation of Figure 2 in ODRL for customer David and CompanyX for the use of David's hometown information. This example highlights an ODRL limitation: it not possible to specify template of policies applicable to a set of agents.

```
{    "@context": "http://www.w3.org/ns/odrl.jsonld",
   "@type": "Agreement",
   "uid": "http://example.com/policy:10003",
   "profile": "http://example.com/odrl:profile:08",
   "conflict": "perm",
   "permission": [{
      "target": "http://example.com/phone",
      "action": "collect",
      "assigner": "http://example.com/party:org:CompanyX",
      "assignee": "http://example.com/party:person:CustomerDavid", }],
   "prohibition": [{
      "target": "http://example.com/phone",
      "action": "share",
      "assigner": "http://example.com/party:org:CompanyX",
      "assignee": "http://example.com/party:person:CustomerDavid",    }]
```

Fig. 5. Formalization of one permission and one prohibition in a policy agreement between CompanyX and Customer David. It shows that CompanyX is allowed to collect David's phone number, but it is prohibited to share this information with third-party companies.

5 Monitoring Norms and Policies

In the preceding sections, we outlined the efforts taken to represent and structure the privacy policy of the companies for the sake of ultimately being access and processed by computers. Moreover, in this section we study the role of automated policy monitoring. Firstly, we seek to address the importance of monitoring policies and secondly, we discuss the need of some components for automated monitoring.

Here we describe few useful services that can be provided on a set of machine-readable policies:

- Monitoring the compliance of policies in which a person is involved as debtor. This functionality plays a critical role especially in fashion companies due to their need to collect sensitive customers' data and to their need to monitor their employees' behavior towards customers' privacy inside their organization.
- Giving the flexibility and confidence to customers by providing monitoring platform that they can use to see whether their privacy policies are violated or not. For instance, a customer can attach to one picture the prohibition to published it on a public platform for advertisement and would like to monitor if the actions performed on the picture are compliant with this prohibition [4].
- Searching accurately the resources and the possible actions that can be performed on them. For instance, we assume that the company offered some services to collect some personal data about customer's interest to explore more effective personalization [30].

In order to monitor policies automatically we need the following components:

1. A machine-readable data structure of the actions performed or planned by companies or customers.
2. A mechanism for monitoring the status of policies to check whether there are active or not. For example, as mentioned in the previous section, some policies can contain constrains and as soon as they become satisfied the policies status will be changed.
3. A mechanism for controlling if a given action (realized on given resource by a certain agent) is compliant with the set of active policies.
4. A mechanism for automatically computing if the active policies such as obligations or prohibitions are violated or fulfilled.

In literature there are two interesting proposals of extending ODRL with an operational semantics for monitoring norms and policies automatically. In [16] the model of policies proposed in ODRL has been extended in order to make it possible to express its operational semantics. The authors put in evidence some properties of the policies that are relevant for their life-cycle, in particular their deadline and their activation condition.

In another interesting paper [31] M. De Vos et al. proposes an ODRL profile that can capture the semantics of both business policies and regularity requirement. They use Answer Set Programming for the policy compliance checking with possibility of reporting the problem in case that compliance is not achieved.

6 Conclusion

In this paper we investigated how we can use ODRL and Semantic Web technologies for expressing privacy policies of the fashion brands in the Web of Data. We stressed on the transformation of policies from natural language to the machine-readable format using RDF. We used ODRL as a policy language for expressing the action that should or should not performed on the resources. Finally, we have highlighted the literature for monitoring the policies automatically. Our investigations into this area are still ongoing and, in our future, works we plan to investigate the use of the OWL Web Ontology Language for expressing actions performed by the agent and infer their implications by using OWL reasoning.

7 Acknowledgement

The research reported in this paper has been funded by the SNSF (Swiss National Science Foundation) grant no. 200021 175759/1.

The final authenticated version is available online at `https://doi.org/10.1007/978-3-030-78227-6_28 .`

References

[1] C. Gonzalo, A., Harreis, H., Altable, H., & Villepelet, "The fashion industry's digital transformation: Now or never | McKinsey," 2020. https://www.mckinsey.com/industries/retail/our-insights/fashions-digital-transformation-now-or-never (accessed Feb. 12, 2021).

[2] K. Kari, "The Art of Ontology," *2018*. https://engineering.zalando.com/posts/2018/03/semantic-web-technologies.html (accessed Feb. 12, 2021).

[3] K. Rowshankish, A. Trittipo, and S. London, "Data privacy: What every manager needs to know," *McKinsey Insights*, no. July, 2018.

[4] A. Oltramari *et al.*, "PrivOnto: A semantic framework for the analysis of privacy policies," *Semant. Web*, vol. 9, no. 2, pp. 185–203, 2018, doi: 10.3233/SW-170283.

[5] T. S. Garraza, "Fashion in the digital environment - Ediciones Universidad de Navarra," 2015. https://www.eunsa.es/libro/moda-en-el-entorno-digital_102440/ (accessed Feb. 12, 2021).

[6] Y. A. Sekhavat, "Privacy preserving cloth try-on using mobile augmented reality," *IEEE Trans. Multimed.*, vol. 19, no. 5, pp. 1041–1049, 2017, doi: 10.1109/TMM.2016.2639380.

[7] M. Ornati and L. Cantoni, "FashionTouch in E-commerce: An Exploratory

Study of Surface Haptic Interaction Experiences," in *HCI in Business, Government and Organizations*, 2020, pp. 493–503.

[8] N. Kalbaska and L. Cantoni, "Digital fashion competences: Market practices and needs," *Lect. Notes Electr. Eng.*, vol. 525, no. March, pp. 125–135, 2019, doi: 10.1007/978-3-319-98038-6_10.

[9] "Zalando Privacy Notice." https://mosaic01.ztat.net/cnt/privacy-page/pdf/Zalando_Privacy_Notice_(English).pdf.

[10] "2017 Global Mobile Consumer Survey :," 2017.

[11] A. M. Mcdonald, "Lorrie Faith Cranor, The Cost of Reading Privacy Policies," *Isjlp*, vol. 4, pp. 1–22, 2008, [Online]. Available: http://www.ftc.gov/os/2000/o5/testimonyprivacy.htm.%0Ahttps://heinonline.org/HOL/License.

[12] R. P. Carver, "Is Reading Rate Constant or Flexible?," *Read. Res. Q.*, vol. 18, no. 2, p. 190, 1983, doi: 10.2307/747517.

[13] "Tommy Hilfiger introduces Tommy Jeans XPLORE smart clothes." https://www.businessinsider.com/tommy-hilfiger-smart-clothes-rewards-2018-7?r=US&IR=T (accessed Feb. 12, 2021).

[14] "General Data Protection Regulation, GDPR Overview." https://www.microsoft.com/en-us/trust-center/privacy/gdpr-overview (accessed Feb. 12, 2021).

[15] S. Kirrane, S. Villata, and M. D'Aquin, "Privacy, security and policies: A review of problems and solutions with semantic web technologies," *Semant. Web*, vol. 9, no. 2, pp. 153–161, 2018, doi: 10.3233/SW-180289.

[16] K. Bollacker, N. Díaz-Rodríguez, and X. Li, "Beyond Clothing Ontologies: Modeling Fashion with Subjective Influence Networks," *Mach. Learn. meets Fash. KDD Work.*, no. August, pp. 1–7, 2016, [Online]. Available: https://kddfashion2016.mybluemix.net/kddfashion_finalSubmissions/Beyond Clothing Ontologies Modeling Fashion with Subjective Influence Networks.pdf.

[17] "Clothing Product Information Ontology Language Reference." http://www.ebusiness-unibw.org/ontologies/cpi/ns (accessed Feb. 12, 2021).

[18] N. Fornara and M. Colombetti, "Using Semantic Web Technologies and Production Rules for Reasoning on Obligations , Permissions , and Prohibitions," 2019, doi: 10.3233/AIC-190617.

[19] N. Fornara, "Specifying and monitoring obligations in open multiagent systems using semantic web technology," in *Studies in Computational Intelligence*, 2011, vol. 344, pp. 25–45, doi: 10.1007/978-3-642-18308-9_2.

[20] S. R. profile imageSebastian R. Pascal Hitzler, Markus Krtzsch profile imageMarkus Krtzsch, *Foundations of Semantic Web TechnologiesAugust 2009*. 2009.

[21] by Tim Berners-lee, J. Hendler, and O. Lassila, "The Semantic Web A new form of Web content that is meaningful to computers will unleash a revolution of new possibilities." Accessed: Feb. 12, 2021. [Online]. Available: http://www.

[22] R. Snyder, "A Practical Introduction to the XML , Extensible Markup

Language , By Way of Some Useful Examples," *Preceeding 2004 ASCUE Conf.*, pp. 239–247, 2004.

[23] R. Alnaqeib, F. H. Alshammari, M. A. Zaidan, A. A. Zaidan, B. B. Zaidan, and Z. M. Hazza, "An Overview: Extensible Markup Language Technology," no. June, 2010, [Online]. Available: http://arxiv.org/abs/1006.4565.

[24] S. Peroni and F. Vitali, "Interfacing fast-fashion design industries with Semantic Web technologies: The case of Imperial Fashion," *J. Web Semant.*, vol. 44, pp. 37–53, 2017, doi: 10.1016/j.websem.2017.06.001.

[25] "Home – TrustArc The Leader in Privacy Management Software." https://trustarc.com/ (accessed Feb. 12, 2021).

[26] R. Iannella, "The open digital rights language: XML for digital rights management," *Inf. Secur. Tech. Rep.*, vol. 9, no. 3, pp. 47–55, Jul. 2004, doi: 10.1016/S1363-4127(04)00031-7.

[27] "XrML Elements | Microsoft Docs." https://docs.microsoft.com/en-us/previous-versions/windows/desktop/adrms_sdk/xrml-elements (accessed Feb. 12, 2021).

[28] I. Burnett, R. Van de Walle, K. Hill Rightscom, U. J. Bormans, and F. Pereira, "MPEG-21: goals and achievements," 2003. Accessed: Feb. 12, 2021. [Online]. Available: https://ro.uow.edu.au/infopapers/46.

[29] S. Guth, "Rights Expression Languages," *Lect. Notes Comput. Sci.*, no. 2770, pp. 101–112, 2003, doi: 10.4018/9781605662626.ch001.

[30] T. H. Nobile and N. Kalbaska, "An exploration of personalization in digital communication. insights in fashion," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Jul. 2020, vol. 12204 LNCS, pp. 456–473, doi: 10.1007/978-3-030-50341-3_35.

[31] M. De Vos, S. Kirrane, J. Padget, and K. Satoh, "ODRL policy modelling and compliance checking," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2019, vol. 11784 LNCS, pp. 36–51, doi: 10.1007/978-3-030-31095-0_3.