Analyzing Privacy Policies based on a Privacy-Aware Profile: the Facebook and LinkedIn case studies

João Caramujo and Alberto Rodrigues da Silva
Instituto Superior Técnico – Universidade de Lisboa (IST-UL) & INESC-ID
Lisboa, Portugal
{joao.caramujo, alberto.silva}@tecnico.ulisboa.pt

***Abstract*—The regular use of social networking websites and applications encompasses the collection and retention of personal and very often sensitive information about users. This information needs to remain private and each social network owns a privacy policy that describes in-depth how users' information is managed and disclosed. Problems arise when the development of new systems and applications includes an integration with social networks. The lack of clear understanding and a precise mechanism to enforce the statements described in privacy policies can compromise the development and adaptation of these statements. This paper proposes the extension and validation of a UML profile for privacy-aware systems. The goal of this approach is to provide a better understanding of the different privacy-related requirements for improving privacy policies enforcement when developing systems or applications integrated with social networks. Additionally, to illustrate the potential of this profile, the paper presents and discusses its application with two real world case studies - the Facebook and LinkedIn policies - which are well structured and represented through two respective Excel files.**

Keywords-Privacy, Requirements, UML profile, System, integration, Facebook, LinkedIn

I. INTRODUCTION

Over the last decades, both individuals and organizations have accepted the potential and use of systems and applications. Issues regarding privacy in systems have been at stake ever since Law and Health industries began to use information systems to manage their users' data [1][2]. On the other hand, the regular use of social networks motivated the integration of these platforms into the development of new systems and applications, adding a new layer on top of the systems' privacy-related requirements.

Using social networks, such as Facebook, LinkedIn or Instagram, demands users to create an account, hence, providing personal information (e.g., name, email) and, when is relevant, other sensitive information (e.g., credit card details, family relatives, address or contact list). Additionally, information based on users' activity, i.e., usage information, is also collected and retained by the service provider (e.g., geolocation or device information) or the different third parties (e.g., information based on content distributed through sharing features). As a result of the sensitive nature of this information, it has to be collected with consent of the users and remain confidential. To comply with these requirements, each social network is obliged by national and international rules and regulations (e.g., US-EU and US-Swiss Safe Harbor framework [12]) to own a privacy policy which users must accept and that describes in-depth how their information is managed and disclosed.

One of the main problems that emerge when developing a third-party system integrated with social networks is the lack of clear understanding about these platform's privacy policies and, at the same time, the absence of a precise mechanism with the proper resources to enforce the statements described in such policies. These difficulties and the effort to overcome them may jeopardize ongoing projects and also discourage future work in this area.

This paper proposes the extension and validation of a conceptual model for privacy policies [7] supported in a UML profile. This *privacy-aware profile* can be applied to describe the privacy policy used by a social network and, therefore, help the development of systems by including this information. The main features and advantages of this UML extension for customizing UML models made it suitable for the purpose of creating a privacy-aware profile in the context of this paper.

The goals of this proposed approach can be classified at different levels: firstly the purpose of this profile is to clarify the understanding of privacy policies, i.e., its objective is to provide a better and deep understanding of the different privacy-related requirements for improving privacy policies enforcement when developing systems or applications integrated with social networks. Achieving this can be of significant value for several processes in software development [3], hence the second-level goals. During the software specification activity, requirement engineers can develop more consistent and complete models using this privacy-aware profile, whereas in the software design and implementation activities, the developers are able to keep fully aware of these privacy requirements and other important details described in the privacy policies of social networks. Additionally, after the system or application is deployed, the possibility of structuring these models in a Microsoft Excel representation gives customers and users the opportunity to get a clear and easy to understand description of how their personal information is being managed by the system.

The paper is organized as follows: firstly, the related work is presented in Section II. Section III introduces the privacy-aware profile and overviews its concepts and relationships. Section IV presents and discusses such profile application with two real world case studies - the Facebook and LinkedIn privacy policies. Section V discusses the obtained results regarding the context of this paper and related work. Finally, section VI concludes the paper and provides some ideas for future work.

II. Related Work

A lot of research has focused on the analysis of privacy requirements in social networks' privacy policies. Through the creation of conceptual models for supporting the definition of privacy policies [16] and, therefore, the understanding of all concepts involved revealed a gap between privacy requirements and systems requirements which may cause the disclosure of sensitive information [4]. On the other hand, the development of new formal languages for specifying privacy requirements is particularly useful since it allows one to check for conflicts within privacy policies and enables the tracing of data flows within such policies [15].

The concerns regarding privacy and personal information protection have been the trigger for the study of methodologies and strategies to design privacy-aware systems [5]. One of the approaches that came up described the creation of a privacy-aware context profile towards context-aware application development [6]. This work strongly emphasizes the importance of privacy-aware profiles in systems and applications that interact with users' personal information (i.e., the context), so that there is a need to have proper management of the context in such platforms.

Another interesting and relevant work proposes a conceptual model for privacy policies [7]. This conceptual modes describes the privacy policy domain by outlining the main concepts of a privacy policy, as well as the relationships between such concepts. On the other hand, constraints that apply to the context of the work are also identified and expressed in the model. The conceptual model is then validated with a small example of a privacy policy.

Despite having some similarities with the work presented in this paper, the previous approach applies for a different context, thus lacking a deep understanding of a privacy policy. By providing a conceptual model that specifies a privacy policy in terms of *User*, *Data* and *Action*, the subsequent specification of the privacy requirements that comprise such policies is vague and imprecise. The approach introduced in this paper proposes a UML profile that extends and validates the conceptual model but that is mainly focused on the privacy requirements of social networks. Through this extended and more concrete view of the problem, this paper aims to provide a more accurate and thorough privacy-aware profile, thus answering the challenge of specifying the privacy requirements of social networks.

III. Privacy-aware Profile

A. A UML profile approach

Being one of the most important and most used modelling languages towards the development of systems and applications, UML has been provided with the ability to be used for software systems in a domain-independent way, using controlled extension mechanisms for this purpose [8]. The UML profiling is a lightweight extension mechanism to the UML since it allows the adaptation of the UML metamodel for the creation of different domain-specific modeling languages (DSML) [13][14]. These DSMLs, defined as UML profiles, are represented through a structure diagram that defines custom stereotypes, tagged values and constraints [8]. Due to the context of this paper, in particular the need for representing privacy-related concepts in UML, the use of this extension was considered and turned out to be the most reasonable option.

B. Profile Overview

Privacy is always a sensible topic in what concerns customer relationships: companies can use for instance customers' personal information to exploit or to provide better and personalized user experience, but, on the other hand, customers rarely want to disclose information about themselves. However, customers are more willing to cooperate depending on the company's reputation and the privacy policies' completeness [9]. This particular detail highlights the importance of privacy policies and also underlines the need for developing tools that may enforce them properly.

Taking into account that the focus of this paper relies on the system's integration with social networks, we analyze two of the most popular, namely: Facebook's privacy policy [10] and LinkedIn's privacy policy [11]. Despite their differences, both cases are appropriate within this context in a way that they are extensively used worldwide.

A preliminary and thorough analysis of such privacy policies allowed us to identify new concepts and constraints which were significant within the context of this paper. With this knowledge, we provide an approach for extending the former conceptual model for privacy policies [7] into a more complete and consistent privacy-aware UML profile that can better serve the purpose of this work. The proposed UML profile is represented in Fig. 1.

1) PrivacyPolicy

PrivacyPolicy element represents the document users must accept in order to use the services provided by companies (i.e., the service providers). This document must identify what type of users' information will be managed and disclosed, but also specify how it will be performed when using the company's service(s). It is defined by a set of attributes, such as: *id* (identification of the policy), *name* (the name of the policy), *creationDate* (date in which it was created) and *revisionDate* (the date of the policy's last revision). The ***PrivacyPolicy*** element is composed by one or more ***Statement*** elements.

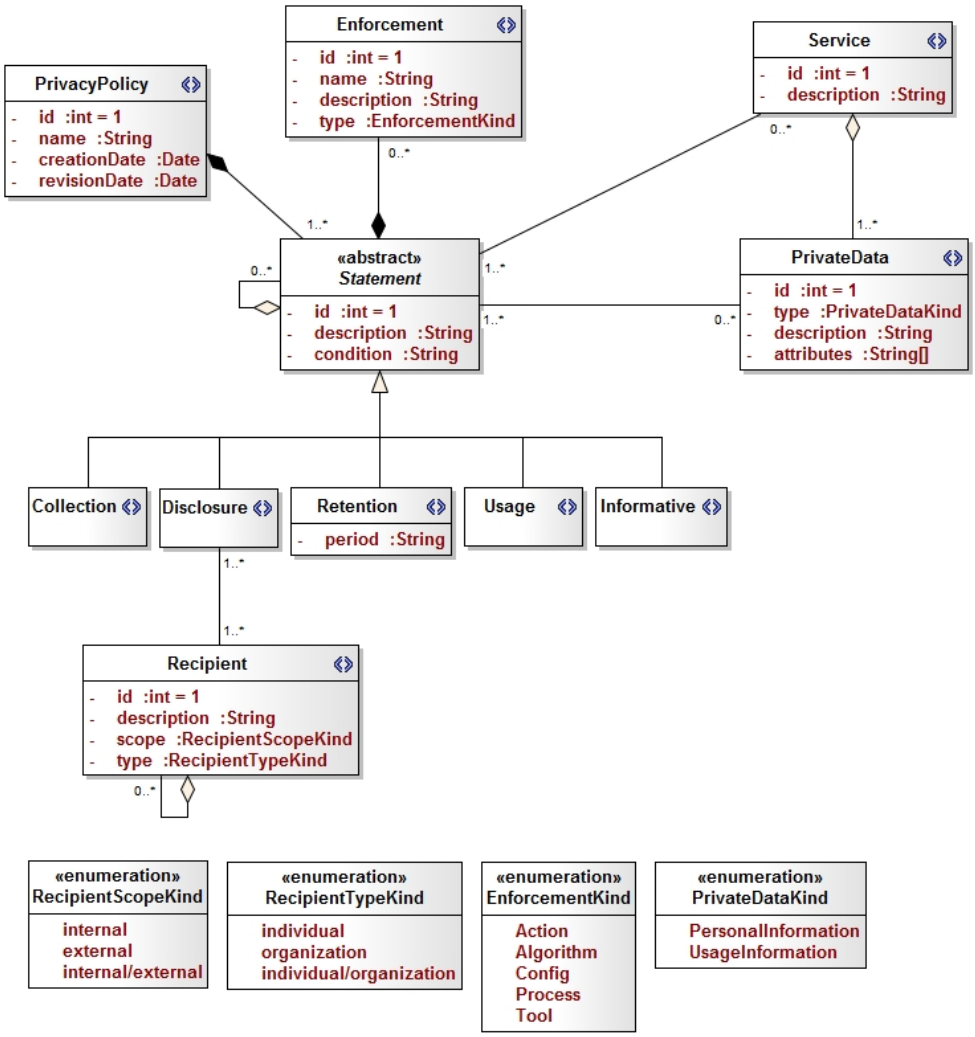

Fig. 1. Proposed privacy-aware UML profile

2) *Statement*

Statement is the core element of this privacy-aware profile. It describes the rules or actions specified in the privacy policy. One statement is defined by the following attributes: an *id* (identification of the statement), a *description* as presented in the original privacy policy and one or more *conditions* that need to be met before the rules or actions described in each one of the statements are performed. Additionally, a statement might have services (association with ***Service*** elements), as well as privacy data (association with ***PrivateData*** elements). These associations are necessary because it is useful to keep track of what services are described in the extend list of statements, whereas it is also important to know which kind of users' private data is specified in each one of the statements. At the same time, a generic ***Statement*** element can aggregate one or more specific statements. Due to the nature of the statements, one ***Statement*** element can be derived into five different specialized elements, namely: *Collection*, a statement that specifies what personal information will be collected by the service provider; *Disclosure*, a statement that defines which personal information is disclosed and to what entities); *Retention*, a statement that identifies for how long personal information will be kept; *Usage*, a statement that details the purpose of the personal information; and *Informative*, a statement that describes generic and informative statements.

3) *Recipient*

The ***Recipient*** is one or more entities to whom the privacy policy grants access to users' personal information. It is defined by an *id* (identification of the recipient), a *description* (description of the recipients as presented in the original privacy policy), a *scope* (e.g., internal, external and if the recipients are from inside and outside the social network, internal/external) and a *type* (e.g., individual, organization and if the set of entities has both individuals and organizations, individual/organization). Both attributes take their values regarding rules or actions described in each one of the statements.

4) *PrivateData*

The ***PrivateData*** element represents the type of users' information that is collected and then managed by the service provider. It can be classified into *PersonalInformation* (e.g., name and email) or *UsageInformation*, i.e., information that is gathered based on users' activity (e.g., geolocation or device information) depending on the *type* of information that is being managed. This element is also defined by an *id* (identification the ***PrivateData*** element), a *description* and a set of *attributes* (minor data elements that compose one ***PrivateData*** element).

5) *Service*

The ***Service*** element encompasses which services are offered by the service provider, i.e., what services are offered to the ones who use social networks. It has an *id* (identification of the service) and a *description* (brief description regarding the service). The association between ***Service*** elements and ***PrivateData*** elements allows one to keep a record of what personal information is being collected while using one or more services. A service is defined based on the users' point of view.

6) *Enforcement*

The ***Enforcement*** elements are the mechanisms available to enforce some of the statements described in the privacy policy. Enforcements are defined by an *id* (identification of the element), a *name* and a *description*. It is also possible to classify them according to their *type*, for instance: *Tool* (e.g., tools for downloading account information); *Action* (e.g. grant access); *Algorithm* (e.g., encryption algorithms); *Process* (e.g., access control); and *Config* (e.g., device configurations, system updates).

IV. VALIDATION

In order to validate the UML profile proposed in this paper, the profile itself needed to be applied to real world examples, i.e., it has to be applied to real privacy policies. On top of that, another objective of this approach was to provide a UML profile that could be effortless mapped into a Microsoft Excel representation, stressing the potential and the flexibility of this extended privacy-aware profile.

The following sections present two case studies - Facebook and LinkedIn -, validated by this UML profile. Due to space limitations, for each case study, we selected a relevant set of statements that cover well enough the profile's application. All tables displayed hereafter were taken from the Excel files created during the analysis of such privacy policies. In some cases, a table can aggregate information from different sheets within the file, whereas in other cases, information from the same sheet needs to be separated so that the structure and organization of this paper is not compromised.

A. *Facebook*

For the case study of Facebook, this paper only considers and identifies 5 statements, one from each type described in the profile, which are listed in Table I.

TABLE I. SET OF STATEMENTS FOR THE CASE STUDY OF FACEBOOK

id	description	type
1	We collect the content and other information you provide when you use our Services, including when you sign up for an account, create or share, and message or communicate with others. This can include the location of a photo or the date a file was created.	Collection
17	We share information we have about you within the family of companies that are part of Facebook.	Disclosure
25	We store data for as long as it is necessary to provide products and services to you and others. Information associated with your account will be kept until your account is deleted, unless we no longer need the data to provide products and services.	Retention
34	When we have location information, we use it to tailor our Services for you and others, like helping you to check-in and find local events or offers […]	Usage
47	You can also download information associated with your Facebook account through our Download Your Information tool.	Informative

TABLE II. ASSOCIATIONS BETWEEN STATEMENT, PRIVATEDATA, SERVICE AND ENFORCEMENT ELEMENTS OF FACEBOOK

Statement (id)	PrivateData (id)	Service (id)	Enforcement (id)
1	1	1	
17	1, 4		
25	All		
34	6		
47	1, 4	1	2

Due to space limitations, and since that for all chosen statements the condition to be met is the one that states "Users must accept Statement of Rights and Responsibilities (including Data Policy)", we decided not to include this attribute in the example (however, the complete analysis and application of Facebook's privacy policy is available at an external repository).

Table II describes the associations between some of the elements specified in this paper's privacy-aware UML profile (e.g., a given statement has an association with a service, i.e., a statement references directly or indirectly some service). In this situation, it represents the relationship between: a) ***Statement*** and ***PrivateData*** elements; b) ***Statement*** and ***Service*** elements; and c) ***Statement*** and ***Enforcement*** elements. In this tabular representation, associations are listed in the same row of the table with the correlation between elements being ensured by their attribute id.

Finally, Table III encloses the remaining information that is necessary to complete the analysis of this set of statements and, subsequently, the validation of the proposed profile based on the Excel representation.

Given all the information described before, it is simple to classify one statement according to this UML profile and therefore providing a better understanding and formalization of the different privacy-related requirements that are described in the privacy policy.

TABLE III. RELEVANT INFORMATION ABOUT THE REMAINING ELEMENTS OF FACEBOOK

Recipient				
id	**description**	**scope**	**type**	**disclosure statements (id)**
1	Facebook family companies	internal	organization	17, 22

PrivateData			
id	**type**	**description**	**attributes**
1	Personal Information	Facebook Account	first name, surname, email, mobile number […]
2	Personal Information	Payment Information	credit or debit card number, shipping and contact details
3	Personal Information	Friends and Contacts	name, email, other contact information
4	Usage Information	Public Activity or Profile	posts, photos, status updates, public profile
5	Usage Information	Device Specifications	operating system, hardware version, device settings […]
6	Usage Information	Device Locations	specific geographic locations
7	Usage Information	Connection Information	name of your mobile operator or ISP, browser type, IP address […]
8	Usage Information	Third-parties Activity	information gathered while visiting third-party websites and apps

Service		
id	**PrivateData (id)**	**description**
1	1, 4, 5, 6, 7	Facebook Account (includes all services possible to someone with a Facebook account - from the user point of view)

Enforcement			
id	**name**	**type**	**description**
2	Download Your Information Tool	Tool	Users are able to download information associated with their Facebook account

To illustrate the previous conclusion, we sum up the classification of one of the identified statements, in particular the statement with id 1 (S1). S1 is a *Collection* statement, since it describes what user information will be collected by the service provider (in this case, Facebook) and how. By scanning the information showed in Table II it shows an association between S1 and the ***PrivateData*** element with id 1 (P1), i.e., S1 specifies the information that is collected and that is described in terms of its attributes in PD1. The examination of PD1 (listed in Fig. 2) identifies it as the "Facebook Account" (therefore classified as "Personal Information") and containing attributes like name and email. On the other hand, Table II also identifies a relationship between S1 and a ***Service*** element with id 1 (SV1). SV1 is described as "Facebook Account", a service which includes all possible actions for a user to do with an account (e.g., posting, sharing or commenting). At the same time, it is also worth noticing that being a broad service, SV1 manages more than one ***PrivateData*** element. From Table II and also from Table III it is showed how this Excel representation handles the case of the 0..* multiplicity: a cell without a value means that, in Table II, one statement does not describe directly or indirectly any service or enforcement resource (zero instances).

To provide another representation for this example, Fig. 2 represents an object diagram for S1 that clearly shows the instances of classes and associations from the UML profile discussed in section III.

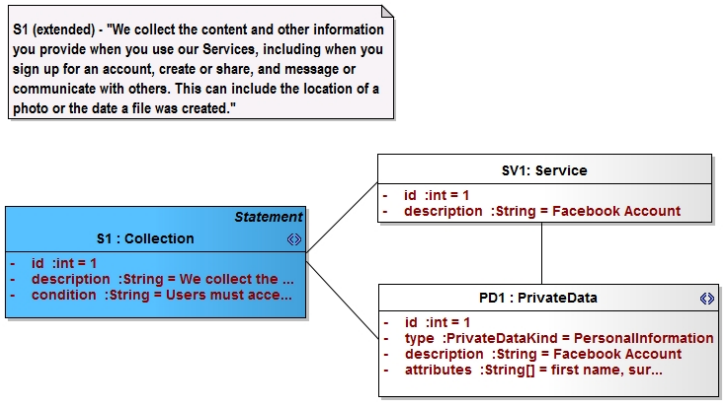

Fig. 2. Object diagram for statement S1 (partial view)

B. *LinkedIn*

As for the case study of Facebook, and in order to compare both privacy policies, the approach followed by this paper regarding the case study of LinkedIn had to be the same. For that reason, we compiled a list of 5 different statements that is presented in Table IV.

Once again, the total set of statements only has one common condition which needs to be met: "Users must agree to LinkedIn's User Agreement and Privacy Policy". To avoid redundancy we removed this attribute from the statements like we did with Facebook. The remaining information that is relevant to analyze the statements is described in Table V and Table VI.

For the LinkedIn case study we overview the classification of Disclosure statement. By providing a different example, we intend to enrich the study of both cases and also demonstrate how flexible and far-reaching the privacy-aware profile is on the analysis of privacy policies.

TABLE IV. SET OF STATEMENTS FOR THE CASE STUDY OF LINKEDIN

id	description	type
1	To create an account on LinkedIn, you must provide us with at least your name, email address and/or mobile number, and a password and agree to our User Agreement and this Privacy Policy.	Collection
26	We may also disclose your personal information to a third party as part of a sale of the assets of LinkedIn Corporation, a subsidiary, or division, or as the result of a change in control of the company or one of its affiliates, or in preparation for any of these events.	Disclosure
39	We retain the personal information you provide while your account is in existence or as needed to provide you services. We may retain your personal information even after you have closed your account if retention is reasonably necessary to comply with our legal obligations.	Retention
46	We use personal information from our Services, including Member profiles, Groups content, and Company Pages, to inform and refine our search service.	Usage
59	We adhere to the Digital Advertising Alliance's self-regulatory principles for online behavioral advertising.	Informative

Considering the statement with an id of 26 (S26), it is classified as a *Disclosure* statement because it specifies which personal information is disclosed and to what entities. By browsing through Table V, it is possibly to identify an association between S1 and ***PrivateData*** elements with an id of 1 and 2 respectively (P1 and P2). Both P1 and P2 are classified as "Personal Information" being P1 labeled as "LinkedIn Account" and having as attributes the name or mobile number, whereas P2 is identified as "Additional Profile (public)" and therefore containing profile that are public like, for example, the job title or professional experience. Since we are analyzing a statement of type "Disclosure" it is necessary to characterize the entity to whom the information is disclosed. Through Table VI, the entity, i.e., the ***Recipient*** element, has an id of 7, is described as a generic "Third-party", external to LinkedIn but, at the same time, it can be an organization or an individual. On the other hand, by exploring the last column of the table, one can infer that this entity receives information that is also described in statements 32 and 34. As we did for the case study of Facebook, this section also presents an object diagram for the statement (S26) discussed in the example.

TABLE V. ASSOCIATIONS BETWEEN STATEMENT, PRIVATEDATA, SERVICE AND ENFORCEMENT ELEMENTS OF LINKEDIN

Statement (id)	PrivateData (id)	Service (id)	Enforcement (id)
1	1	1	
26	1, 2		
39	All	1	
46	2		
59			

This different representation is represented in Fig. 3. Both case studies are missing any reference to the ***PrivacyPolicy*** element. The irrelevance in the case studies context, as well as the space limitations, determined this course of action.

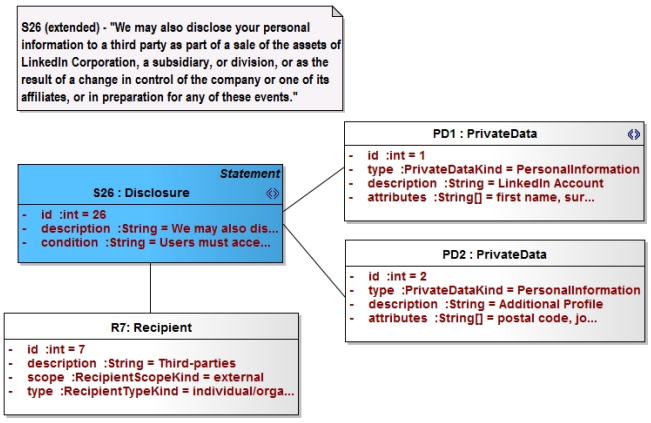

Fig. 3. Object diagram for statement S26 (partial view)

C. *Other social networks*

Although the purpose of this paper only encompassed two real world case studies, during our research we skimmed through other privacy policies from different social networks and we noticed how similar they were both in content as well in structure of the document itself. In some way this conclusion strengthens the UML profile and, on the other hand, also increases the prospect of extending its domain of validity.

TABLE VI. RELEVANT INFORMATION ABOUT THE REMAINING ELEMENTS OF LINKEDIN

Recipient				
id	**description**	**scope**	**type**	**disclosure statements (id)**
7	Third-parties	external	individual/organization	26, 32, 34

PrivateData			
id	**type**	**description**	**attributes**
1	Personal Information	LinkedIn Account	name, email, mobile number, password
2	Personal Information	Additional Profile	postal code, job title, company, descriptions of skills, professional experience […]
3	Personal Information	Purchases Information	credit card details
4	Personal Information	Friends and Contacts	name, email, other contact information
5	Personal Information	Email	content of email messages, other information
6	Usage Information	Device Information	IP address, computer OS details, type of web browser, name of your ISP […]
7	Usage Information	Third-parties Activity	information gathered while visiting third-party websites and apps

Service		
id	**PrivateData (id)**	**description**
1	1, 2, 6	LinkedIn Account (includes all services possible to someone with a LinkedIn account - from the user point of view)

V. DISCUSSION

The extended privacy-aware profile proposed in this paper defined a new set of concepts and constraints. These modifications were of a considerable necessity in a way that we lacked a profile which was complete and detailed enough for analyzing privacy policies from social networks and capturing all major privacy requirements. On the other hand, the Excel representation was of great value because it is a proper and simple mechanism for organizing - based on the defined profile - the statements described in the privacy policies.

The decision of choosing Facebook and LinkedIn as case studies relied on the fact that these social networks are globally used and well-known, even though both social networks have considerable differences in their goals and *target audience*. The discussion of these two case studies, hence validating the profile, allowed one to better understand the different privacy-related requirements for improving privacy policies enforcement. Thus, it is already possible to prove the importance of this profile regarding the development of third-party systems. Developers and designers can get familiar with the services and privacy data that are handled on such social networks. Besides these advantages, one can recognize some patterns - whether regarding natural language itself or information collection and management - that can foster the development of techniques for automatic extraction.

Through the analysis described in this paper it is possible to identify some similarities between the two privacy policies - despite the different writing style - and that were expected *a priori*, such as the ***PrivateData*** elements (e.g., Account Information and Purchase/Payment Details) which are essential for both social networks' operations, as well as ***Recipient*** and ***Service*** elements. Both social networks have a set of partners that support their business hence the common recipients and, at the same time, social networks also share some similar services (e.g., account features and advertising). However, there are some differences regarding the ***Enforcement*** elements due to the fact that each social network tend to use or provide distinct tools or technologies for themselves or their users. On the other hand, it is noteworthy that the analysis of both case studies allowed us to examine thoroughly and carefully the privacy policies provided by these companies, thus we are also able to compare them in terms of format. Despite the aforementioned writing style, LinkedIn's privacy policy is more exhaustive and descriptive when compared to Facebook's document. Nevertheless, the writing and structuring concerns emphasize that companies are starting to see the importance of such policies not just legally but also in a technical and business perspectives.

VI. CONCLUSION

This paper proposes and discusses an extended privacy-aware profile towards the integration of social networks in the development of third-party systems. In order to lay out a clear understanding of the different privacy-related requirements described in privacy policies and, therefore, improving the enforcement of such privacy-related requirements and giving the possibility of having simple and quick methods of checking for conflicts and inconsistencies regarding the privacy policies involved when developing systems integrated with social networks, there was a need to carry out adjustments to previous profiles or models [6][7], so that the revised profile could be of greater value. These modifications are highlighted in the UML profile and described on the validation of the proposed profile against real world social networks - Facebook and LinkedIn - which made it possible to illustrate its potential and discuss its application. Future work will focus on the extension of the RSLingo approach [17] in order to have a complete and renewed perspective on specifying and documenting privacy-related requirements. This course of action encompasses a need for carrying out the necessary adjustments to RSL-IL [18], a formal language for specifying requirements, allowing its conversion into a formal DSML based on the privacy-aware profile introduced in this paper that can provide formal specifications of privacy-related requirements. At the same time, the application of the profile with real world case studies introduced in a plainer manner other extensions of this work, such as an information extraction approach that strives for automatic classification of statements and extraction of textual fragments from privacy policies written in natural language text, as well as automatic classification of privacy policies (against a set of privacy-aware patterns) allowing us to, in the future, classify the privacy policies from popular websites and assign them a qualitative value (e.g., a grade ranging from 1 to 5) regarding some privacy criteria.

ACKNOWLEDGMENTS

This work was partially supported by national funds through FCT – Fundação para a Ciência e a Tecnologia, under the projects CMUP-EPB/TIC/0053/2013, UID/CEC/50021/2013 and DataStorm Research Line of Excellency funding (EXCL/EEI-ESS/0257/2012).

REFERENCES

[1] J. Jenkins, “What can information technology do for law?”, in Harvard Journal of Law & Technology, 21(2), 2008.

[2] T. C. Rindfleisch, “Confidentiality, information technology and health care”, in Privacy, Information Technology and Healthcare, Communications of the ACM, 40(8), August 1997.

[3] I. Sommerville, “Software processes”, in Software Engineering, 9th ed. Pearson, 2010, ch.2, pp. 45-46.

[4] P. Kumari, “Requirement analysis for privacy in social networks”, in 8th International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods, 2010.

[5] P. Guarda and N. Zannone, “Towards the development of privacy-aware systems”, in Inform. Softw. Technol., 51(2), February 2009.

[6] G. M. Kapitsaki and I. S. Venieris "PCP: Privacy-aware context profile towards context-aware application development", in Proceedings of the 10th International Conference on Information Integration and Web-based Applications & Services (iiWAS), 2008.

[7] A. Coen-Porisini et al., “A conceptual model for privacy policies”, in Proceedings of the 11th IASTED International Conference on Software Engineering and Applications, 2007.

[8] Object Management Group (OMG). UML 2.4.1 Superstructure Specification [Online]. Available: http://www.omg.org/spec/UML/2.4.1 [Accessed: 15-03-2015]

[9] E. B. Andrade, V. Kaltcheva, and B. Weitz ,"Self-disclosure on the web: the impact of privacy policy, reward, and company reputation", in NA - Advances in Consumer Research, 29, 2002.

[10] Facebook. Data Policy [Online]. Available: https://www.facebook.com/policy.php [Accessed: 04-03-2015]

[11] LinkedIn. Privacy Policy [Online]. Available: https://www.linkedin.com/legal/privacy-policy?trk=hb_ft_priv [Accessed: 04-03-2015]

[12] Export.gov. U.S.-EU & U.S.-Swiss Safe Harbor Frameworks [Online]. Available: http://www.export.gov/safeharbor/index.asp [Accessed: 15-03-2015]

[13] B. Selic, "A systematic approach to domain-specific language design using UML", in Proceedings of the 10th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing, 2007.

[14] G. Giachetti, B. Marín and O. Pastor, “Using U.M.L. as a Domain-Specific Modeling Language: A Proposal for Automatic Generation of UML Profiles”, in Lecture Notes in Computer Science, 5565, 2009.

[15] T.D. Breaux, H. Hibshi and A. Rao, “Eddy, A Formal Language for Specifying and Analyzing Data Flow Specifications for Conflicting Privacy Requirements”, in Requirements Engineering, 19 (3), 2014.

[16] A. Coen-Porisini, P. Colombo and S. Sabri, “Privacy Aware Systems: From Models to Patterns”, in Software Engineering for Secure Systems: Industrial and Research Perspectives, 2010.

[17] D. Ferreira and A. R. Silva, ”RSLingo: An Information Extraction Approach toward Formal Requirements Specifications”, 2nd Int. Workshop on Model-Driven Requirements Engineering (MoDRE 2012), IEEE CS, 2012.

[18] D. Ferreira and A. R. Silva, “RSL-IL: An Interlingua for Formally Documenting Requirements”, 3rd IEEE International Workshop on Model-Driven Requirements Engineering (MoDRE 2013), IEEE CS, 2013.