International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(4): 363-372
The Society of Digital Information and Wireless Communications (SDIWC), 2018 ISSN: 2305-001

Using Multiple Profiles to Protect Privacy in Web-Based Social Networks

Lila Ghemri Sabrina Shahnaj
Department of Computer Science, Texas Southern University
3100 Cleburne St, Houston, TX77479
lila.ghemri@tsu.edu

Emma Hamilton
Stanford Medicine
291 Campus Drive, Stanford, CA94305
hemma@stanford.edu

ABSTRACT

Being a member of a Web-based social network has become an integral part in the lives of millions of individuals. People make new friends, reconnect with old ones, and chronicle their life events using online social networks. However, online social networks can also become a threat to one's privacy if information finds its way to an unwanted audience. This usually happens when private information gets disclosed, either inadvertently or maliciously, to an unintended recipient. This article proposes a framework that will address the issue of unwanted disclosure by allowing a member of a social network to create multiple profiles, select whom to add to each profile, and post to a profile instead of posting to a generic view, as it is done nowadays. In the authors' opinion, this solution can assure users that their posts and interactions are restricted to their intended group and consequently cannot be disclosed beyond it.

KEYWORDS

Web-based social networks, privacy, ontology, FOAF, information disclosure, access control.

1. INTRODUCTION

There has been a proliferation of Web-based social networks (WBSNs) since the nineties of last century, such as Facebook MySpace or Twitter. Each of these sites has millions of users and is popular with a special category of people. WBSNs only require an Internet connection to work. A person who is interested in using any of these platforms is required to create an account. Subsequently, a user builds his/her social network by adding friends, acquaintances, or people he/she is interested in; this actually consists in linking their accounts with a type of relationship labeled as "friend", "follower", or "connection". When such a connection is established, the accounts' holder can usually access each other's information through an object called profile, a wall, or a timeline.

While these connections are established with the consent of both parties, some social networks do not require mutual consent. Indeed, online social networks also introduce the notion of profile visibility, that can have various settings, e.g. public, friends only, or private. These settings allow access to different types of information about a person. Numerous studies have shown that account holders do not really understand all the intricacies of profile settings [1], [2], [3] and assume more privacy than the amount that the platform actually affords to them. Besides managing profile settings, most users only have one place in which they add all their contacts, family, friends, and co-workers. This situation is at odds with real life, in which people have various and separate social spheres (such as family, professional, and friends), and brings about severe concerns about a person's privacy, as described in [4]. In WBSNs, the lack of proper control over privacy settings together with the intersection of a user's social spheres had dire consequences on people's lives, causing them to lose their job or their reputation, or even more tragic outcomes [5]. In order to avoid this kind of situation, many users have resorted to creating multiple accounts, each dedicated to a specific audience. This solution is a violation of the terms of service in most WBSNs and is not a viable solution.

This work proposes a system that provides members with a way to create multiple profiles. Each profile corresponds to a specific audience with its members, interactions, and media. Profiles are transparent to one another and members in one profile are not aware of members in another profile, making each profile work as an independent unit. A member's online interactions, postings, or comments are also made through a profile. In the authors' opinion, this separation allows a member better control over his/her privacy and more freedom in posting without fear of disclosure to an unwanted audience.

In addition to protecting a member's privacy, this approach removes the incentive to violate the platform terms of use against creating multiple accounts and increases social transparency and accountability.

Some of the ideas in this paper were presented in [6]; the current version discusses the threat of unwanted disclosure and how the authors' approach addresses it, together with implementation details. The rest of this paper is organized as follows. The next section will present the main components of WBSNs. Next, a threat model relevant to the above-illustrated problem is developed. Then, the Friend of a Friend (FOAF) machine readable ontology is presented and adopted to formally define the concepts used in the authors' system. Subsequently, the system design and implementation are introduced and conclusions finally drawn.

2. WEB-BASED SOCIAL NETWORKS

Web-based social networks are web-based services that encourage users to join and establish a social network of friends and acquaintances. According to boyd and Ellison [7], the key elements of a WBSN are:

1. Each user is required to create an account and is provided with credentials to access it.
2. Each user has a profile which can be either public or semi-public.
3. Each user articulates a list of other users with whom a connection is established.
4. Each user has the ability to post comments, pictures, or multimedia.
5. Each user can navigate his/her and other users' network of connections, observe their activity, and react to it.

2.1 Data in Web-Based Social Network

Data in a WBSN include information related to the users, their network, and their interaction.

2.1.1. User Profile

A user profile or wall contains several types of information:

a) Information about the user himself/herself. These data include his/her account name, which could be a pseudonym, and, depending on the platform, information, such as date of birth, email, phone numbers, place of birth and residence, education, schools, work information, marital or relationship status, religion. Much of this information is personally identifiable information (PII) that could potentially be misused to impersonate the user.

b) The second type of user information relates to a user's activity on his/her social network through posting of comments about events or their daily life, sharing of some material (e.g., multimedia and links), or reaction to some information by the use of emoticons, texts, or other.

2.1.2 User Network

These data relate to the connection that an account holder has with other account holders through links such as "friend" or "follower". These connections are usually represented as a social graph (see Figure 1).

2.1.3 User Metadata Information

These data include a user browsing history, friends added/blocked, links followed, and physical locations. Most platforms keep a record of each user's interactions and this metadata is used by the platform to establish a user's

preferences and suggest new connections or advertise for products that fit the user.

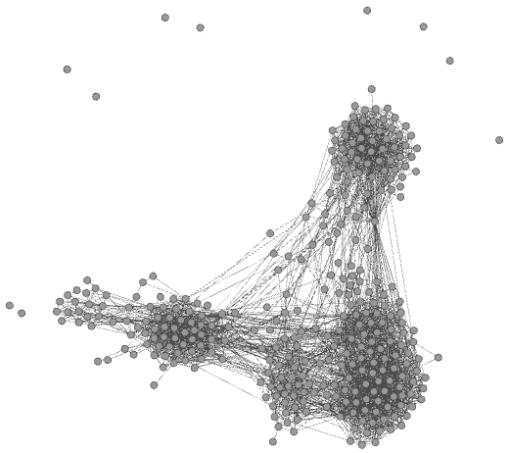

Figure 1: Social Graph [8]

3. PRIVACY THREATS IN ONLINE SOCIAL NETWORKS

3.1 Unwanted Disclosure

A member activity consists of postings or comments about a user's or others' life events. Posting an item brings about several privacy issues:

- **Unwanted Access:** Depending on the privacy settings that the user has elected, an item can be viewed by more people than the member intended. Most WBSNs implement privacy through access control. However, they put the onus on the member to understand the intricacies of privacy settings and adjust their account visibility accordingly. Several studies have been performed showing that most OSNs users are not fully aware of privacy setting and of what they really mean [9], [10].

- **Data Retention:** Most OSNs have vague policies related to how long user data are kept in their data center. For example, Twitter used to keep a member's activity data "indefinitely", until it was pressured to change its retention time policy to 30 days after deactivation [11], [12]. In some other WBSNs, such as Facebook, data posted on a user's account is kept for as long as the account holder or any of his/her connections has an active account. Even when a member deletes some content he/she has posted, it takes about one month for the deletion to "trickle down" the social network. This disparity in data retention policies makes it even more challenging for the lay user to control access to his/her activity data.

3.2 Identity Management and Multiple Accounts

Humans as social entities evolve in various spheres, such as family, friends, and co-workers. People have social norms and behaviors that they follow when they are within each of these spheres. Before the advent of WBSNs, these spheres rarely overlapped and were kept separate in a person's life. However, this is no longer true and, within a WBSN, a member may have their family, friends, and colleagues intermingling in the same account. This situation has been coined as "context collapse" by boyd [13].

In order to prevent this situation, members may create several accounts as a way to protect their privacy and manage their circles. As a result, users can choose which "friends" are allowed to access which account and information [14].

3.3 Fake Accounts

Fake accounts have two distinct origins and can cause privacy violations. The first type is identity fraud in which the account holder may be impersonating a real life person. These fake account holders intrude into the digital life of the person they impersonate, friend their real life friends, family, and acquaintances, and may cause great distress and harm to the real person they pretend to be.

The second type of fake accounts includes those created by spammers. This is made possible because of the relative ease with which one can create an account in a social network. Indeed, a person can choose any pseudonym and upload any picture as long as he/she enters a valid email. This minimal registration process allows to breach the system with little accountability [15], [16].

This paper describes an approach to protect a user's privacy by allowing him/her to create multiple profiles within a single WBSN account, and by associating members to a given profile. In

the authors' view, this approach can address two security issues: unwanted access and multiple accounts. This approach is based on the use of Semantic Web [17], particularly the FriendsOfAFriend (FOAF) ontology, to define the concepts of user, accounts, and profiles.
The issues of disclosure, security, and access are expressed using a logic-based reasoning framework that will determine what information any potential account holder may access. The result is an online social environment which satisfies privacy requirements, such as user identity management and selective disclosure.

4. THE FOAF LANGUAGE

The Semantic Web was introduced as a means to automated reasoning on the Web. The idea is to organize information on the Web as an ontology and augment it with reasoning mechanisms, so as to enable the drawing of inferences and conclusions from the Web. The ontology is defined as a network in which edges are relations between concepts.
In the Semantic Web, concepts are linked through relationships with other concepts, and can be represented as triples (concept1, relation, concept2).
For example, in order to state that Marge Simpson is a cartoon character, an entity Marge Simpson has to be created and made as an instance of a cartoon character:

```
(:CartoonCharacter  isa :#MargeSimpson)
```

To express that Marge Simpson is married to Homer Simpson, we use the triple:

```
(#MargeSimpson                    marriedTo
:#HomerSimpson).
```

This semantic representation allows inference drawing; however, the objects at this level cannot be reified nor any tangible conclusions drawn, unless they have a representation at the hypertext level and unless each entity can be uniquely identified within the paradigm. Consequently, in order for this apparatus to work, it also requires:

1. The specification of unique global names for each entity or resource, using the universal resource identifiers (URIs).
2. Access mechanisms that map a URI to its location on the Web or any other repository through the use of location and access protocols, such as hypertext transfer protocol (HTTP).

Several ontology paradigms have been designed and developed for the Semantic Web, such as Resource Description Framework (RDF) and Web Ontology Language (OWL) [18]. In this work, the authors focus on the FOAF ontology that has been designed to use with social networks.
FOAF is an ontology of the Semantic Web [19] that has been successfully used to represent social networks. Currently, many social networking web sites, such as hi5 and Buzznet, use FOAF to produce users' profiles that are compatible with the Semantic Web. Consequently, FOAF is frequently cited as an example of how the Semantic Web will evolve.
An FOAF network has three types of nodes [20]:

1. **Concepts:** A concept can be anything that needs to be represented, be it physical, such as a car or a person, or abstract, such as happiness.
2. **Relations:** Relations are either used to describe a concept like `hasColor` or `age`, or a relationship between concepts, such as `livesIn` or `worksAt`.
3. **Classes:** Classes have the same meaning as in object-oriented paradigms, in that they describe a blue print of an entity and of which concepts are instances.

FOAF concepts specialize in representing relationships amongst people on the Web and integrate three kinds of networks: Social networks, which describe human collaboration, friendship, and association; Information networks, which aim at representing and linking documents and; Representational networks, which are still somewhat less well defined and for which no current applications could be found. FOAF aims at providing a language in which users, groups and organizations, and their attributes and relationships can be expressed in a clear and concise manner. Constraints, such as membership and ownership, can also be expressed and enforced without human intervention, by using a reasoning engine. FOAF

is machine readable and is defined using RDF and OWL. FOAF vocabulary is designed to allow wide scale use, but its suitability to the various purposes that it aims to represent is still being developed and expanded.

4.1 FOAF Classes

FOAF is an ontology, which means that its concepts are organized into a parent-child relationship. Furthermore, FOAF defines relations that link concepts. Since this ontology aims to express social networks, it has a number of concepts and relations that allow linking people, groups, and documents together.

FOAF ontology has `owl: Thing` as the root or top class. However, the top FOAF concept is the class `foaf: Agent` which describes any entity that can take any action. People are described through the class `foaf: Person` and groups through `foaf: Group`. Another important concept is `foaf: Document`, which is used to express a user's authorship of a given document.

4.2 FOAF Properties

Each class has a defined set of properties which describes its properties, such as name, age, etc.

4.3 FOAF Relations

Relations are used to express relationships between concepts. People are connected with one another, through the relationship `foaf: knows`. Additionally, relationships between people and groups are expressed through the relationship `foaf:member`. The authorship of a document is specified using the relation `foaf:maker`.

Table 1 presents the base FOAF ontology [20]. Since FOAF is built on top of RDF, all FOAF concept and relation definitions include a header that indicates the RDF schema used.

Table1: FOAF Base Ontology

FOAF Classes	FOAF Properties	FOAF Relations
Agent/Person	account name age gender birthday mbox weblog holdsAccount	maker member knows (Person)
Group	member membershipClass	
Document/ PersonalProfile Document/ Image	topic primaryTopic	openid isPrimaryT opicOf

5. FOAF FOR SOCIAL NETWORKS

A social network is built around people, relationships between them, and their interactions. Each of these entities needs to be defined using the FOAF ontology.

5.1 Users

The base building block of an OSN is the member or user. A user is defined as an instance of a `foaf:Person`. In order to distinguish the person from his/her account, the notion of user account is also defined. A user account is an instance of a `foaf:Agent`, which is more generic than Person and allows more expressiveness.

5.2 Relationships

In the authors' paradigm, profiles need to be defined in order to define relationships between members. A profile is defined as a `foaf:group`. A relationship between two OSNs users is established by adding a user account as a member of the group representing the profile.

5.3 Members' Interactions

The primary role of a WBSN is to allow people to connect, interact, share, and exchange

information about themselves and about each other. Assuming that communications between connected members of a social group can be modeled using the concept Document, then a posting, be it text or multimedia, is described as an instance of `foaf:Document`. It originates from an Account. However, the authors find that the FOAF framework proves insufficient to fully express online interactions, since the only relations pertaining to this class are `foaf:Publications` that relates a `foaf:Person` to an `foaf:Document`.

Ghemri [6] proposed extensions to the FOAF ontology to accommodate social interactions in a WBSN. The required expansions are:

-Property: foaf:views/viewedBy
views – viewing of a document
Status: proposed
Domain: having this property implies being an Agent
Range: every value of this property is a Document

-Property: foaf:includes/includedIn
includes – including a document
Status: proposed
Domain: having this property implies being a Document
Range: every value of this property is a Document.

6. SYSTEM DESIGN

Our system includes three main components: Account creation, Social network building, and Social interactions.

6.1 Account Creation Component

The purpose of this component is to create a user account. After the user enters his/her data, the corresponding FOAF nodes get generated (Figure 3). The FOAF code consists of the creation of an entity person (Alice Smith) with the user's name and all relevant fields populated. It also automatically generates an instance of Agent that denotes the user account within the system.

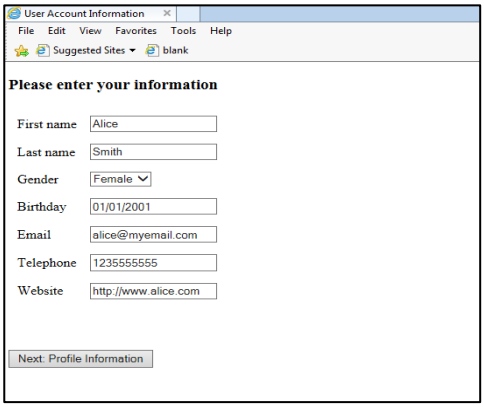

Figure 2. Account Creation

```
<rdf:RDF
xmlns:rdf="http://www.w3.org/1
999/02/22-rdf-syntax-ns#"
xmlns:rdfs="http://www.w3.org/
2000/01/rdf-schema#"
xmlns:foaf="http://xmlns.com/f
oaf/0.1/">
<foaf:Person
rdf:nodeID="#AliceSmith">
<foaf:name>Alice
Smith</foaf:name>
<foaf:firstName>Alice</foaf:fi
rstName>
<foaf:lastName>Smith</foaf:las
tName>
<foaf:gender>Female</foaf:gend
er>
<foaf:birthday>01/01/2001</foa
f:birthday>
<foaf:mbox>alice@myemail.com</
foaf:mbox>
<foaf:phone
rdf:resource="tel:123-555-
5555"/>
<foaf:account rdf:resource=
"http://www.alice.com" />
</foaf:Person>
<foaf:Agent
rdf:nodeID="AliceSmithAccount"
>
<foaf:name>Alice Smith
Account</foaf:name>
<foaf:homepage rdf:resource=
"http://www.alice.com" />
<foaf:made rdf:resource=
"http://www.alice.com/SmithPro
fessionalProfile" />
<foaf:maker rdf:nodeID=
"#AliceSmith" />
</foaf:Agent>
</rdf:RDF>
```

Figure 3. Account Generation FOAF

6.2 Social Network Building

The second aspect consists in adding profiles and members to these profiles so as to build the user's social network (Figure. 4).

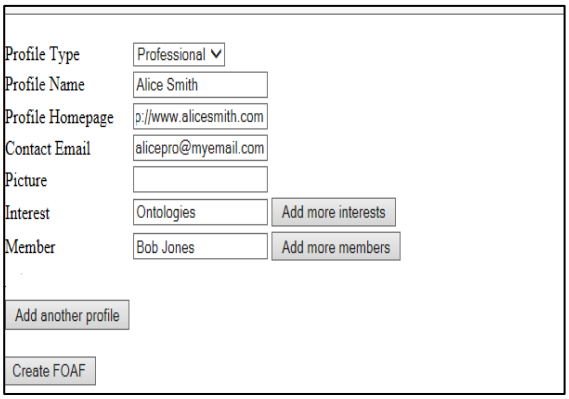

Figure 4. Alice Smith Professional Profile

The corresponding generated FOAF code creates two concepts: Group and ProfileDocument. The Group concept includes information about the Group maker and Group members. The second FOAF concept which is created is the ProfileDocuments, which includes information about the documents posted/included on the profile.

7. PREVENTING PRIVACY ATTACKS

The implementation generates RDF and FOAF constructs that can be reasoned about using an engine which supports inference about facts and can thus automatically enforce selective disclosure.
The above system and organization was implemented using JavaScript and tested on a scenario that can lead to unwanted disclosure, that is:
Alice wants to post pictures of her last party; she wants to post them on her close friends' profiles, which do not include Mallory or Eve, but includes Bob.

7.1 Representation and Inference

Let W be the set of all people registered with the WBSN.
-o is an account holder, $o \in W$
-d is a document posted by o in profile P
$maker(o, P) \wedge publications(P, d)$
-r is a member of W and is a requester for viewing the document d
There are three kinds of requesters:

- A requester $u \in U$; u is authenticated by the account owner o through the triple (o, *knows*, u), but u is not a member of profile P.
- A requester m, who is a member of the profile P in which the document d was posted, $P \subseteq U : member(m, P)$
- An anonymous requester a who is a member of $A \subseteq W$, $A \cap U = \varnothing$, which means that $\neg(o, knows, u)$

Let R be the set of possible requesters of document d. $R = \{m, u, a\}$ with member entities such as o for account holder, m for profile member, u for authenticated user, and a for anonymous.
Profiles act as filters that only let people who are members of A profile see the information posted on them.
The assumption is that all data posted by account owner o is contained in an identity profile document P_{Id}, which can be represented as a set of RDF triples
(o, *publication*, d).
In addition, for each piece of data to be posted, the owner o needs to specify in which profile it has to be included.
In FOAF, this is done through the RDF triple
(P *includes* d).
Since both triples are required, a posting on a profile of an account owner o is defined as:
$(o, publications, d) \wedge (P, includes, d)$ (1)

Profile P' represents P_{Id} profile filtered by data requester $r \in W$. Data posted and contained in the profile are a subset of triples in P_{Id}, such as:
$P' \subseteq P_{Id}$ that requester r is allowed to see.

A filter function f realizes a mapping from a set of triples to values {0, 1} depending on the identity of the requester. 1 means r is allowed to see the information, while 0 means that r is not allowed.
To each requester $r \in W$, a filter function defined as (2) is associated:

$f: I \times \{(o, publications, d)\} \rightarrow \{0, 1\}$ (2)

Function f yields 1 for each triple in profile P_{Id} and identity owner *o*, as shown in (3), meaning the account holder can view all his/her postings.

$$f(o, (o, publications, d)) = f_o(o, publications, d)=1 \quad (3)$$

For *r* a member of *W*, the function should return 0 when:

- the requester *r* is not a member of profile *P'*, or
- the document *d* is not included in the profile *P'*, or
- the profile *P'* is not authenticated to belong to owner *o*.

Based on these constraints, the function f_m will determine if *r* can see the posting.

$$f_r(o, views, d)= \begin{cases} 1 \; if \; r \in P' \; \& \; P_{Id} \; includes \; d \\ 0 \qquad\qquad otherwise \end{cases} \quad (4)$$

If any of these constraints is false, the conjunction will return 0 and *r* will not be allowed to see the posting.

In order to generalize the approach to any possible requester and insure that no unwanted disclosure happens, a function *A(r)* is introduced to describe access privileges based on the type of requesters.

$$A(r) = \begin{cases} m & if \; m \in P' \subseteq U \\ u & if \; u \in U \wedge u \notin P' \\ a & if \; a \notin U \end{cases} \quad (5)$$

Using equations (4) and (5), we can define $R_{P'}$, the set of all requesters *r* that can see documents d posted on profile *P as* :

$$R_P = \{(P, includes, d)| f_{A(r)}(o, publications, d))=1\} \quad (6)$$

This set uniquely determines who can see a document *d* posted on a profile *P'* and filters out all requesters who do not satisfy the constraints.

8. RELATED WORK

The literature contains numerous studies and systems that aim at protecting a user's privacy in WBSN. A comprehensive survey can be found in [21] work. The designers of the DECENT system [22] proposed a decentralized architecture in which participants in an OSN are organized into a hash table and a cryptographic mechanism is used to protect a participant's confidentiality and privacy. Paul *&.al* [23] proposed a color coded scheme to set privacy options and make clear to users what kind of access they are providing to their audience. Busnel, Serrano-Alvarado, and Lamarre on the other hand, described a system in which privacy is set in terms of strength and frequency of interaction between members, rather than a static classification [24]. The same approach was also followed by Ardagna, De Capitani di Vimercati, Foresti, Paraboschi, and Samarati [25].

A privacy aware social network is proposed in [26] which offers the user ways to communicate their privacy concerns across the platform and combines provenance and accountability to safeguard a user's information. Another approach to protect a user's privacy consists in the user assigning a social value to each of his/her friends and in the system subdividing them into "safe" and "unsafe" [27]. SybilGuard is a system that protects social networks from Sybil attacks [28].

Facebook in particular has been the topic of several studies that have tested its privacy settings and also the security risks of its social network graph [29]. As to the use of Semantic Web and its ontologies in managing user privacy in WBSNs, several privacy languages have been developed, particularly the Platform for Privacy Preferences or P3P1 [30] that provides a mechanism for informing users about privacy policies of Web site before they release their information. However, the P3P1 does not ensure that sites act according to their policies.

ProProtect3 is a system that protects user data within the WebIDs framework. A WebID uniquely identifies a Web entity, such as a person, company, organization, or other agent, using a URI. ProProtect3 particularly focuses on unwanted retrieval, malicious manipulation, and improper use, and integrates its method with the WebID authentication sequence using an inference reasoner [31]. Although this research follows the same general approach of using Semantic Web ontologies and logical inferencing, the authors believe that their work is different. In the authors' approach, unwanted disclosures are

handled through multiple profiles of a single user. PropProtect3, on the other hand, focuses on protecting a single profile from unwanted retrieval using WebID.

9. CONCLUSION

In this work, the authors argued that allowing a Web-based social network account holder to create multiple profiles will address two main security threats in these systems: the creation of multiple accounts for a single user, that stems from a user's desire to protect his/her privacy, and unwanted disclosure. The authors proposed the use of semantic ontologies, in particular the FOAF ontology, to allow a social network account holder to create multiple profiles. The user selects which members to add to a specific profile and which posts to publish in each profile. The researchers presented a system that builds the FOAF representation corresponding to a user's account and a user's profile and showed that this framework, coupled with an ontology reasoner, can provide document access control by filtering out documents, a.k.a postings that a given requester can see. Controlling access at the outset will eliminate the need for cumbersome and confusing privacy settings that current WBSNs have and allow users a safe environment for their social interactions.

ACKNOWLEDGEMENTS:

This work was supported by the DHS Center of Excellence for Command, Control and Interoperability for Advanced Data Analysis. The authors wish to thank the anonymous reviewers and Ms. Franchell Davidson for very valuable comments on improving this paper.

REFERENCES

1. Acquisti, A., Gross, R.: Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In: Proc. of Workshop on Privacy Enhancing Technologies, Cambridge, England (2006).
2. Dwyer, C., Hiltz, S. R., Passerini, K.: Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. In: Proc. Thirteenth Americas Conference on Information Systems, Keystone, CO. (2007).
3. Johnson, M., Egelman, S., Bellovin, S.M.: Facebook and Privacy: it's complicated. In: Proc. Eighth Symposium on Usable Privacy and Security, Washington DC. (2012).
4. Beye, M., Jeckmans, A., Erkin, Z., Hartel, P., Lagendijk, R., Tang, Q.: Privacy in Online Social Networks. (2010).
5. Correa, T., Willard Hinsley, A., Gil de Zúñiga, H.: Who interacts on the Web? : The intersection of users' personality and social media use. Computers in Human Behavior, 26, 247--253. (2010).
6. Ghemri, L.: A user centered approach to managing privacy in online social networks. In: Proc. Informing Science & IT Education Conference (InSITE). Miami. (2015).
7. boyd, d. m., Ellison, N. B.: Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 13(1), 210--230. (2007).
8. Diarra, M.: Online Social Networks Analysis (Unpublished master's thesis). Texas Southern University, Houston, TX. (2014)
9. Gross, R., Acquisti, A.: Information Revelation and Privacy in Online Social Networks. In: Proc. ACM Workshop on Privacy in the Electronic Society. Alexandria. (2005).
10. Madejski, M., Johnson, M., Bellovin, S. M. A.: Study of Privacy Setting Errors in an Online Social Network. In: Proc. 4th IEEE International Workshop on Security and Social Networking, Budapest, Hungary. (2014).
11. Pangburn, D. J.: Twitter data retention policy targeted by WikiLeaks in #NOLOGS campaign. http://www.deathandtaxesmag.com/171966/wikileaks-targets-twitter-data-retention-policy-in-nologs-campaign/ (2012).
12. Twitter Terms of Service https://twitter.com/tos?lang=en#privacy.
13. boyd, d.: *Taken Out of Context: American Teen Sociality in Networked Publics***.** PhD Dissertation. University of California-Berkeley, School of Information (2008).
14. Uski, S., Lampinen, A.: Social norms and self-presentation on social network sites: Profile work in action: New media & society 18(3) 447--464 (2016).
15. Gosnell, J.: The 'Fakebook': The Rise of Bogus Users in Facebook Infographic. http://www.trendhunter.com/trends/fakebook-the-rise-of-bogus-users-in-facebook. (2012).
16. Mier, J.: Fake Identities in Social Media. http://mastersofmedia.hum.uva.nl/2012/11/14/fake-identities-in-social-media/ (2012).
17. Fensel, D., Hendler, J., Lieberman, H.: Spinning the Semantic Web. MIT Press. Cambridge, MA (2003).
18. OWL. (https://www.w3.org/OWL/). (2016).
19. FOAF. Vocabulary Specification .Paddington, http://xmlns.com/foaf/spec/ (2014).
20. Brickley, D., Miller, L.: FOAF Vocabulary Specification 0.99 - Paddington Edition. Retrieved http://xmlns.com/foaf/spec/. (2014).

21. Islam, M. B., Iannella, R., Watson, J., Geva, S.: Privacy Architectures in Social Networks state-of-the-art survey. International Journal of Information Privacy Security and Integrity, 2(2), 102--137. (2015).
22. Jahid, S., Nilizadeh, S., Mittal, P., Borisov, N., Kapadia, A.: DECENT: A Decentralized Architecture for Enforcing Privacy in Online Social Networks. In: Proc. 4th IEEE International Workshop on Security and Social Networking, Budapest, Hungary. (2014).
23. Paul, T., Stopczynski, M., Puscher, D., Volkamer, M., Strufe, T.: C4PS - Colors for Privacy Settings. In: Proc. Conference on World Wide Web, Lyon. (2012).
24. Busnel, Y., Serrano-Alvarado, P., Lamarre, P.: Trust your Social Network According to Satisfaction, Reputation and Privacy. In Proc. Third International Workshop on Reliability, Availability, and Security, Zurich. (2010).
25. Ardagna, C. A., De Capitani di Vimercati, S., Foresti, S., Paraboschi, S., Samarati, P.: Supporting Privacy Preferences in Credential-Based Interactions. In: Proc. WPES'10Chicago, Illinois, USA (2010).
26. Aïmeur, E., Gambs, S., Ho, A.: Towards a Privacy-Enhanced Social Networking Site. In: Proc. 5th International Conference on Availability, Reliability, and Security, Krakow (2010).
27. Becker, J., Chen, H.: Measuring Privacy Risk in Online Social Networks. In: Proc. 2009 IEEE Workshop on WEB 2.0 Security and Privacy, Oakland (2009).
28. Yu, H., Kaminsky, M., Gibbons, P. B., Flaxman, A. SybilGuard: Defending Against Sybil Attacks via Social Networks. In: Proc. ACM SIG in Data Communication, Pisa. (2006).
29. Stein, T., Chen, E., Mangal, K.: Facebook Immune System. In: Proc. 4th ACM EuroSys Workshop on Social Network Systems, Salzburg. (2011).
30. W3C: The Platform for Privacy Preferences 1.0. http://www.w3.org/TR/P3P (2002)
31. Wild, S., Wiedemann, F., Heil, S., Chudnovskyy, O., Gaedke, M.: ProProtect3: An Approach for Protecting User Profile Data from Disclosure, Tampering, and Improper Use in the Context of WebID. Transactions on Large-Scale Data- and Knowledge-Centered Systems XIX. 87--127. Heidelberg: Springer. (2015).