Proceedings of Informing Science & IT Education Conference (InSITE) 2015

Cite as: Ghemri, L. (2015). A user centered approach to managing privacy in online social networks. *Proceedings of Informing Science & IT Education Conference (InSITE) 2015,* 187-199. Retrieved from http://Proceedings.InformingScience.org/InSITE2015/InSITE15p187-199Ghemri1637.pdf

A User Centered Approach to Managing Privacy in Online Social Networks

Lila Ghemri
Department of Computer Science,
Texas Southern University, Houston, TX, USA

ghemri_lx@tsu.edu

Abstract

Since their initial introduction in the early 90's, the popularity of web based online social networking sites has been growing exponentially, encompassing millions of users. As these social networks continue to grow and become more popular, users' different social circles (friends, family, and colleagues) are very likely to collide, as they all coexist under the same infrastructure. Considering the different levels of relationships between a user and their social circles, concerns about privacy arise. How does a user conceal private data? Who has access to it? And what is the most effective way in managing it? Many different approaches have been taken by online social network providers to give users more control over their data, but these methods have not always been affective, resulting in the misuse of the data or unintentional disclosure. We propose a new framework that aims at reducing risks of privacy violation by giving the user better and more intuitive ways to manage their social circles and control who accesses what type of data.

Keywords: Online Social Networks, Privacy, Profile, FOAF

Introduction

Using **w**eb **b**ased **o**nline **s**ocial **n**etworks (WOSN)s is fast becoming a fact of life for an ever increasing number of people. These social networks have initially been designed with a specific audience in mind, young college students for Facebook (Facebook, 2009), young and tech savvy professionals for LinkedIn (LinkedIn, 2003) and so on. However as their popularity grows, these "exclusively" social sites are also entering work arena with people "friending" their colleagues, coworkers and managers. This situation is quite new and unique in a person's life, in that multiple social groups and types of relationships that a person experiences during their life coexist in a single environment and may sometimes collide. One important aspect of preventing this social collision for a WOSN user is the control of what, and how much to expose about themselves and to whom. This aspect was dubbed "social transparency" by DiMicco and Millen (DiMicco & Millen, 2007).

Various strategies have been devised by online social network companies to allow a user this control. These mechanisms have mostly consisted of dividing a user's connections into groups, friends, friends of friends, followers, etc... However, few users are fully aware of these mechanisms and how to best use them to protect their

Editor: Eli Cohen

privacy and control access to the information they post. Instead, they sometimes resort to creating multiple accounts for themselves, each destined for a specific audience or type of acquaintances.

In a study of the accountability systems of web based online social networks and the types of violations that are perpetrated by a network member, it was shown that one of the most frequent and common violation, is the creation of multiple accounts by a single user. This violation mostly happens because a member does not want their acquaintances, friends, family 'circles' intermingling and overlapping. Consequently, they may create several accounts as a way to protect their privacy and manage their circles by allowing only one type of "friends" access to a specific account and to some information, and another type of friends access to a different account and different information and so on.

In this work, we propose that WOSNs systems could provide members with a way to create multiple profiles, so that they are not forced to create multiple accounts, one for each digital persona. Consequently, with a single account, a user can associate multiple profiles: one for their professional acquaintances, one for their family, etc... Our approach enables members to create several profiles for themselves, and add friends or acquaintances to a profile. Their online interaction, their postings, or comments will be made through a profile. This separation, we believe, will allow a member better control over their privacy and more freedom in posting without fear of disclosure to an unwanted audience. This approach will, in addition to protecting a member's privacy, also remove the incentive to violate the WOSN terms of use against creating multiple accounts and increase social transparency and accountability.

The rest of this paper is organized as follows: The next section will present the main components of WOSNs. Next, we will present an overview of research done to assess privacy mechanisms in the most commonly used WOSNs. This will be followed by a section that presents the privacy mechanisms in Facebook. Then, we will present the Friend Of A Friend (FOAF) machine readable ontology that will be used to formally define the concepts used in our system. We will then present our system design and we will finally conclude.

Organization of Online Social Networks

A Web-based Online Social Network is a web application that consists of programs and settings that allow members or subscribers to post content. This content can be text or multi-media. A WOSN aims for user participation to be easy and continuous; therefore their platform is usually simple and user friendly.

Members: The main asset of a WOSN is its membership. Participation is free to the individual member and is subject to few constraints. However before being able to use the service, a person must register. Most common membership requirements are:

1. For the person to be of a given age (13 or 18).
2. For the person to provide a valid email address.
3. For the person to select a user id, which may be a pseudonym, and a password. Both will constitute the participant access credentials to the WOSN.

In order to limit the use of "fake" identities, pseudonyms and the creation of multiple accounts, some WOSNs, such as Google+, have a "Real Name" policy which requires users to use their real world identity or the name they commonly go by in the real world. However this requirement is easily circumvented by the use of different email addresses, one corresponding to each new account.

In addition to the information above, users may provide additional information to the platform such as their date of birth, employment or school and marital status, if they so wish.

Member's Network: Members are encouraged to set up relationships with one another and invite non-participants to join the WOSN. A participant establishes a network of friends or followers with whom he/she exchanges information about topics of common interest. Most WOSNs require an agreement between both participants, before their accounts become linked and special privileges in terms of access and sharing of information is granted by the system to both. These relationships between members are best viewed as a network in which each participant's account is a node and links with possibly different labels connect nodes.

User Activity Information: Besides information on a member's network of friends, a member activity on the WOSN is also recorded. This information includes any data that a member uploads to their account, such as photos, status updates, comments and other related information. This information changes over time and is usually accessed and shared by the member's network. However, depending on privacy settings, this information could also be accessible to a wider audience or even the general public.

Our interest is on managing information, related to the user activity since these are the data that most WOSN members care about hiding or sharing and are more tied to privacy concerns.

Most WOSNs provide their members with privacy settings to control access to these data, however members are usually not fully aware of these settings and what they really mean. In the next section, we will present studies that have focused on WOSN members' beliefs of who can view and access their data and how correct is their understanding of the WOSN privacy settings.

Privacy Mechanisms in WOSN

Privacy of web-based online social networks has been investigated from the perspective of access control and the extent to which WOSNs showed concern about their participant's privacy and afforded them control over who can access their information and communicate with them (AlSumait, 2011). Facebook and Myspace (MySpace Wiki, 2003) have, most notably, been put under scrutiny both by the media and in academia because they are either the oldest or the most popular online social networks (Dwyer, Hiltz & Passerini, 2007; Johnson, Egelman & Bellowin, 2012). In particular, the attitude of Facebook (FB) participants towards the information they post and who they think can view it, was examined and it was discovered that about 20% of FB users were totally unaware of privacy settings (Gross & Acquisti 2005; Acquisti & Gross, 2006). Another work (Liu, Gummadi, Krishnamurthy & Mislove, 2011) showed that almost 50% of the content that participants upload on FB was shared using the default privacy settings, which effectively made it accessible to everybody. Members, on the other hand, reported that the public access setting really matched what they wanted only 20% of the time, suggesting that the default settings that FB assigned did not correlate with most users' wishes. Madejski also examined FB members' privacy settings and their accuracy with respect to the types of audiences in FB (Friends, Friends of Friends, Network Member, and Stranger) with whom information about topics such as work, religion, sex, was shared. She found that FB privacy framework did not match user's wishes on how to control the material they post (Madejski & Bellovin, 2010; Madejski, Johnson & Bellovin, 2011). As a result of this body of research and numerous complaints, FB has only recently changed its default settings from "Public" to "Friends Only" (Magid, 2014).

Beyond member-to-member unwanted disclosures, research also focused on how WOSNs treat data collected by the service provider. These data usually include the user's profile, network data together with click history. Results from these studies, showed that most WOSN sites often leak private information to third party sites and tracking sites (Krishnamurthy & Wills, 2010**;** Krishnamurthy, Naryshkin & Wills, 2011). In the same vein, it was also shown that even 'anonymized" and aggregated members' data, which some WOSNs admit to sharing with, or selling to third party applications, can be reconstructed using other publicly available sources (Narayanan

& Shmatikov, 2009). The discovery of these privacy breaches and issues has led researchers to propose new approaches that aim at making it easy for users to establish their privacy settings. A color coded scheme was proposed to set privacy options by Paul (Paul, Stopczynski, Puscher, Volkamer & Strufe, 2012), whereas Brusnel proposes setting privacy in terms of strength and frequency of interaction between members rather than a static classification (Brusnel, Serrano-Alvarado & Lamarre, 2010). A design of privacy aware social network that relies heavily on access control has also been proposed with the purpose of mitigating privacy (Aïmeur, Gambs & Ho 2010).

Because of the popularity of Facebook and the available literature about it, our work has focused on Facebook and ways to improve the privacy of Facebook members. In the next section, we present the privacy structure of Facebook.

Facebook Privacy Framework

One of the most famous online social networks today is Facebook. Facebook is a social network created to share information. Facebook has more than 800 million users, 900 million pages, organizations or events, and more than 2 billion *likes* and comments posted every day (Noyes, 2014). Nowadays, Facebook is the second most visited website after Google. Each member in Facebook has a Timeline, which is a combination of the member's personal information (previously profile), and their activity data (previously wall) (Duffy, 2012). There are three 'generic' audiences defined in Facebook: *Public, Friends+* and *Only Me*. Each audience defines who can see a member's data and their activity information. Each item in a member's profile, such as their date of birth, their marital status, is independently allocated a privacy setting, ranging from *'Only Me'* to *'Public'*

a. ***Only Me:*** With this option, a member can only post to their timelines and their postings are not shown on their friends timelines. Only people tagged in a posting can see the posting on their timelines. The only way to see a member's posting under this setting is to be a 'Friend' and to visit their Timeline.
b. ***Friends of Friends and Friends+:*** *Friends of Friends* includes the member's friends and their friends. *Friends+*: includes *Friends of Friends* and anyone tagged in a Post. With this option, a member's friends posting are displayed on their timelines. Their comments are also posted and seen on their friends' timelines. Anyone tagged in a post can also see the post. If a member does not want their postings to be seen by other than their friends, they have to custom delete each unwanted viewer. When a person is tagged in a posting, they automatically can see the posting. This feature has been exploited by a virus that accesses a member's account and tagged all their "Friends" in a posting and thus spread through Facebook (Facebook, 2015).
c. ***Public*:** allows access to everybody, even people with no Facebook account.
In addition to these generic classes, Facebook also allows customized selection and lists.
d. ***Custom:*** this setting allows a member to share an item with specific people or hide it from them, by specifically (de)selecting each member
e. ***Lists:*** Facebook further defines three categories of "Friends": Close Friends", "Acquaintances" and "Restricted". Each of these categories has more constraints on notifications, viewing of postings, etc. In addition, A member can also custom define an audience through the creation of lists in which Friends can be added or removed as needed.
Table 1 below summarizes Facebook and viewing/posting privileges for audience.

Table 1: Facebook Audiences Privileges

Posting\ Viewing	Only Me	Friends of Friends	Friends+	Public
Only Me	Posting/ Viewing	Viewing on Owner's Wall/ No Posting	Viewing if Tagged/Posting on their wall	No Viewing/ No posting
Friends of Friends	Posting/ Viewing	Viewing/ Posting	Viewing/ Posting	No Viewing/ No Posting
Friends+	Viewing/ Posting	Viewing/ Posting	Viewing/ Posting	No Viewing/ No Posting
Public	Viewing/ Posting	Viewing/ Posting	Viewing/Posting	Viewing/Posting

Facebook privacy framework has evolved over time to respond to members concerns about privacy. It looks unwieldy and as an afterthought. Additionally, very few members are fully aware of the intricacies of this framework and how to manage all the settings to keep them true to their wishes. A notable "feature" in Facebook is that if a member chooses to make a specific posting *public,* then all their subsequent postings will become *public.* This is tantamount to resetting the default setting to "*public*".

Our approach is, we believe, much easier for a WOSN member to understand and more intuitive to work with. It also differs from the one described above in two ways. First, our view is that privacy should be taken into account at the outset, as the member is creating their account and not as an afterthought in order to patch an untenable situation. Furthermore, in our system, a member is fully in control of creating their profiles and adding people to this profile; there is no imposition on classes of Friends and related permissions that are automatically given to them. For each posting, the member can select the destination profile. Consequently, a member knows exactly who sees what, and who can comment on what.

The Friends of a Friend Framework

In order to realize our vision and be able to express social relationships in a machine understandable format that is sufficiently powerful to express complex social relationships and also flexible to allow for changes of over time, we adopted the Friend of a Friend (FOAF) framework (FOAF, 2014). FOAF is ontology of the Semantic Web (Fensel, Hendel & Lieberman, 2003). FOAF is fast becoming the standard vocabulary for representing online social networks. Currently, many large social networking websites, such as hi5 and Buzznet, use FOAF to produce profiles of their users that are compatible with the Semantic Web (FoafSites, 2013). Because of its success in terms of use, FOAF is frequently used as an example of how the Semantic Web will evolve. FOAF concepts specialize in representing relationships amongst people on the Web and integrate three kinds of networks:

Social networks that describe human collaboration, friendship and association;

Information networks that link documents in order to share their common information; and *Representational networks* which are still somewhat less well defined and for which no current applications could be found (FOAF, 2014).

FOAF aims at providing a language in which users, groups and organizations, their attributes and their relationships can be expressed in a clear and concise manner. Constraints, such as membership, ownership can also be expressed and enforced without human intervention.

FOAF is machine readable and is defined using Resource Description Framework (RDF) and the Web Ontology Language (OWL) (Fensel, et al, 2003). 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. The work, presented in this paper, is one such effort.

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 to one another. Since it 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 in FOAF is that of ***foaf:Document***, which is used to express a user's authorship of a given document.

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***. Authorship of a document is specified using the relation ***foaf:maker***. Table2 defines the base FOAF ontology.

Table 2: FOAF Base Ontology (FOAF 2014)

FOAF Classes	FOAF Properties	FOAF relations
Agent/Person	account name age gender birthday mbox weblog holdsAccount	maker member knows (Person)
Group	member membershipClass	
Document/PersonalProfileDocument/Image	topic primaryTopic	openid isPrimaryTopicOf

Since FOAF is built on top of RDF, all FOAF concept and relation definitions include a header that indicates the RDF schema used:

<rdf:RDF xmlns:
rdf= “http://www.w3.org/1999/02/22-rdf-syntax-ns# “
xmlns:rdfs= "http://www.w3.org/2000/01/rdf-schema#"
xmlns:foaf="http://xmlns.com/foaf/0.1/">

Expressing Online Social Networks in FOAF

The concepts relevant to our application are the following:

1. A subscriber to an online social network as a Person.
2. A subscriber’s account is an Agent. This distinction between a person and their account is necessary to protect the privacy of the subscriber. Profiles will be created and linked with an account and not directly with a subscriber
3. A subscriber’s Profile is a Group, created by the subscriber’s account .
4. A member in a Profile is a Person’s account belonging to a Group.
5. A Posting, represented as a document shared with a group.

Each of these concepts is required to represent a WOSN member and their network of friends. The generation of an FOAF person profile can be done automatically as shown in (Dodds, 2003). For example, Table 3 corresponds to the FOAF definition of the concept of Lila Ghemri having a friend called Friend One.

Table 3: FOAF definition of a person with a friend (Dodd, 2003)

```
<foaf:PersonalProfileDocument rdf:about="#LilaGhemri">
<foaf:maker rdf:resource="#LilaGhemri"/>
<foaf:primaryTopic rdf:resource="#LilaGhemri"/>
<admin:generatorAgent rdf:resource="http://www.ldodds.com/foaf/foaf-a-matic"/>
<admin:errorReportsTo rdf:resource="mailto:leigh@ldodds.com"/>
</foaf:PersonalProfileDocument>
<foaf:Person rdf:ID="Lila Ghemri">
<foaf:name>Lila Ghemri</foaf:name>
<foaf:title>Dr</foaf:title>
<foaf:givenname>Lila</foaf:givenname>
<foaf:family_name>Ghemri</foaf:family_name>
<foaf:mbox_sha1sum>1dfc2bd572ac47bd9aa4b01af700effdc73b1e0e</foaf:mbox_sha1sum>
<foaf:homepage rdf:resource="http://cs.tsu.edu/ghemri"/>
<foaf:phone rdf:resource="tel:713-313-0007"/>
<foaf:workplaceHomepage rdf:resource="http://cs.tsu.edu"/>
<foaf:workInfoHomepage rdf:resource="Faculty"/>
<foaf:schoolHomepage rdf:resource="www.bristol.ac.uk"/>
<foaf:knows>
<foaf:Person>
<foaf:name>Friend One</foaf:name>
<foaf:mbox_sha1sum>e6acce4a7f2573862cf57586488d7c88c05c62a1</foaf:mbox_sha1sum>
</foaf:Person>
></foaf:knows>
</foaf:Person>
```

We will now describe the concepts of subscriber, subscriber account, subscriber profile and subscriber profile account through a fictional member called “Hope Byrd”.

Subscriber Definition –Private-:

```
<foaf:Person rdf:nodeID="HopeByrd">
        <foaf:name>Hope Byrd</foaf:name>
        <foaf:firstName> Hope </foaf:firstName>
        <foaf:lastName>Byrd </foaf:lastName>
        <foaf:gender>female </foaf:gender>
        <foaf:account rdf:resource= "http://HopeByrdAccount.org/" />
        <foaf:knows rdf:nodeID="#CrawdAccount" />
</foaf:Person>
```

A WOSN subscriber is defined as a Person by a node ID, a string name and other personal information. This information is not propagated to any other nodes, so as to keep it private.

User Account Definition -Private:

```
<foaf:Agent rdf:nodeID="ByrdAccount">
        <foaf:name>Hope Byrd Account</foaf:name>
        <foaf:homepage rdf:resource= "http://HopeByrdAccount.org/" />
        <foaf:made rdf:resource= " http://HopeByrd.org/ByrdProfessionalProfile" />
        <foaf:made rdf:resource = "http://HopeByrd.org/ByrdFamilyProfile" />
        <foaf:maker rdf:nodeID= “#HopeByrd”>
</foaf:Agent>
```

The definition above describes an agent, named Hope Byrd. Her homepage is defined with an URL. The definition also includes the fact that she is the maker of two URLs; each representing a profile: A professional profile and a family profile.

Professional Profile Definition -Public:

```
<foaf:Group rdf:nodeID= ”ByrdProfessional”>
        <foaf:name>Hope Byrd Professional Profile</foaf:name>
        <foaf:member rdf:nodeID=”#CrawdAccount” />
        <foaf:homepage rdf:resource=" http://HopeByrd.org/#ByrdProfessionalProfile” />
        <foaf:maker rdf:nodeID=”#ByrdAccount”>
</foaf:Group>
```

The definition above describes the professional profile of Hope Byrd as well as a member who is part of that group (#CrawdAccount#).

A profile is a Group entity in which members can be added. It will be associated with a name, and a URL. The owner (maker) of Group is an Account defined using the relationship foaf:maker and the Account ID. Members in the group are defined through the relation foaf:member .

A profile also associated with a Profile Account through the foaf:homepage property

---

Professional Profile Account Definition -Public:

```
<foaf:ProfileDocument  rdf:resource=”http://HopeByrd.org/ #ByrdProfessionalProfile/>
        <foaf:name>Byrd Professional Profile </foaf:name>
        <foaf:maker rdf:nodeID="ByrdProfessional"/>
        <foaf:primaryTopic rdf:nodeID="ByrdProfessional"/>
        <foaf:mbox  rdf: mailto:”ByrdPro@myjob.com”  />
        <foaf:homepage  rdf:resource=”http://www.HopeByrdProf.com />
        <foaf:depiction  rdf:resource= “http://www.HopeByrd.com/HopeGraduating.jpg  />
        <foaf:interest  rdf:resource = “http://www.acm.org”  />
         <foaf:interest  rdf:resource = “http://www.3wv.org”  />
</foaf:ProfileDocument>
```

The Profile Document is the web document that contains the information that a user wants to display in that specific profile (e.g. Professional). It includes a name attribute to select the name for the profile, an mbox property to specify an email address, a depiction relation that associate a picture with that profile and interest relation that shows the interests of the user as they relate to that profile (e.g. Professional). Securing the privacy, i.e. disabling the access to the people outside of the Profile is insured by adding restrictions such as: foaf:knows(foaf:UserC, foaf:UserM)

Figure 1 shows the relationships between the various concepts described above and the cardinality of each relationship between concepts using the UML convention. For example, A 1..1 B means that each instance of concept A will be associated with exactly one instance of concept B, whereas A 1 .. * B means that for each instance of concept A correspond many instances of concept B., etc..

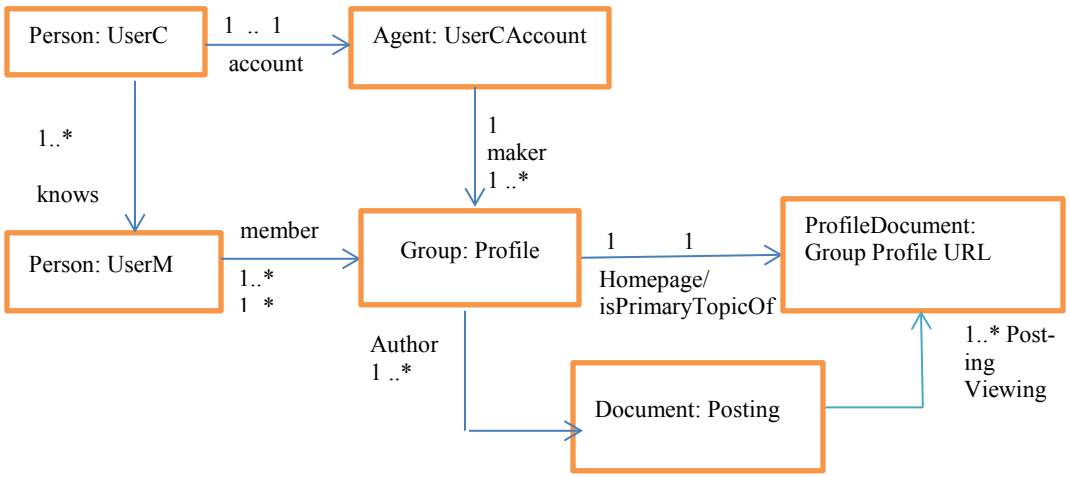

Figure 1: UML Diagram of Social Concepts Relationships (UML, 1989)

We notice that in our framework, there is no direct connection between a Person:User and their profiles document. This separation is required to maintain the privacy of the subscriber

Generic Profile URL Definition –Public:

```
<foaf: ProfileDocument  rdf:resource=URL/>
        <foaf:name>Profile Name </foaf:name>
        <foaf:maker rdf:nodeID="GroupURI"/>
        <foaf:primaryTopic rdf:nodeID=GroupURI>
        <foaf:mbox  rdf: mailto: emailURI />
        <foaf:homepage  rdf:resource= URL/>
        <foaf:depiction  rdf:resource= Photo_URL  />
        <foaf:interest  rdf:resource = URL />
</foaf:ProfileDocument>
```

Expanding FOAF to Express Social Interactions

The primary role of an online social network is to allow people to connect, interact, share and exchange information about themselves and about each other. We find that the framework, that FOAF provide, proves insufficient to express online interactions. For example, if we assume that communications between connected members can modeled using the concept Document, FOAF only defines the relation foaf:publication that relates a foaf:person to an foaf:document. In our context, and in order to preserve the user's privacy, agents doing the "publishing" are the individual profiles, therefore it is necessary to refine this concept by expanding its domain from foaf:person to foaf:Agent,. We therefore offer the following definitions:

Property: foaf:publication
publication- A link to the publications of this agent.
Status: proposed
Domain: having this property implies being an Agent
Range: Every value of this property is a Document

Additionally, FOAF does not include concepts such as "viewing", "commenting", etc..
Viewing a document is usually done by an authorized agent on a document that has been "published" into a profile they are member of.

We therefore also propose the following FOAF extensions.

Property: foaf:views
views- A link to the document this agent is viewing or has viewed.
Status: proposed
Domain: having this property implies being an Agent
Range: Every value of this property is a Document.

Property: foaf:comments
comments- A link to the document containing the comment.
Status: proposed
Domain: having this property implies being an Agent.
Range: Every value of this property is a Document.

It is necessary that each instantiation of comment creates a document in which the commentator is the "publisher".

In order to address the privacy goals that we have set up, two additional properties need to be defined: **foaf:viewingPermitted** and **foaf:commentingPermitted**. We chose to embed these permissions at the document level, so that each document will define who can view it and who can comment on it.

Property: foaf:viewingPermitted
ViewingPermitted- A link to the agent(s) permitted to view this document
Status: proposed
Domain: having this property implies being an document
Range: Every value of this property is an Agent

Setting the Range of the Property to Agent, will enable the system to set this value to Group, Person and any relevant FOAF concept.

Property: foaf:postingPermitted
postingPermitted- A link to the agent(s) permitted to comment on this document
Status: proposed
Domain: having this property implies being an document
Range: Every value of this property is an Agent

With these additions, we believe that we have a more complete and powerful FOAF framework that provides the flexibility to express the notion of multiple profiles, together with that of social interactions such as postings, viewing and commenting permissions.

Conclusion

For all the advantages that WOSNs offer their members, protecting their privacy and shielding their information from unwanted disclosure still remains an issue. In this work, we proposed a new framework in which a user is allowed to create multiple profiles, one to suit their various digital personae. Each profile groups members or "friends" into classes of the member's choosing, each corresponding to the various circles that a person has in their real life: family, friends, professional, hobbies or anything that a member may want. The member can post to a specific profile without fear of disclosure to an unwanted audience or real-life repercussions.
We used the FOAF ontology and expanded it to describe our framework and express the notions of authentication and authorization for this framework. Authentication is performed as members are added to profiles; at a minimum, they have to satisfy some relation with the user, currently described as "knows". In order to insure authorization, we have expanded the FOAF ontology by adding notions of authorization for viewing and posting that will ensure that each posted item fully specifies its intended audience so as to prevent unwanted disclosures.

Our current effort focuses on the automatic generation of FOAF code corresponding to the various concepts we have defined. This effort will allow a seamless conversion to FOAF code that will enable an automatic application of privacy constraints. In comparison with Facebook, our framework still lacks the ability to "Like" a document. Furthermore, reposting of comments and /or pictures and all its attending privacy issues still need to be defined and expanded within this framework.

References

Acquisti, A., & Gross. R. (2006). Imagined communities: Awareness, information sharing and privacy on Facebook. *Proceedings of the 6th Workshop on Privacy Enhancing Technologies*, Cambridge, UK, 2006.

Aïmeur, E., Gambs, S., & Ho, A. (2010). Towards a privacy-enhanced social networking site. In *The Fifth International Conference on Availability, Reliability and Securit*y. February, 15-18, 2010, Krakow, Poland (172-179).

AlSumait, F.M., (2011). Social network privacy and trust concerns. *Proceedings of the 13th International Conference on Information Integration and Web-Based Applications & Service*s. December 5-7, 2011, Ho Chi Minh City, Vietnam. 416-419.

Busnel, Y., Serrano-Alvarado, P., & Lamarre, P. (2010).Trust your social network according to satisfaction, reputation and privacy. *Proceedings of the Third International Workshop on Reliability, Availability, and Security*. July 25-28, 2010, Zurich, Switzerland.

DiMicco, J., & Millen, D. (2007). Identity management: Multiple presentations of self in Facebook. *Proceedings of the 2007 international ACM conference on Supporting Group Work*. November 4–7, 2007, Sanibel Island, Florida, USA. 383-386.

Dodd, L. (2003). *FOAF-a-Matic*. Retrieved February 20, 2015 from rom http://www.ldodds.com/foaf/foaf-a-matic.html

Duffy, J. (2012). 12 things you should know about Facebook timeline. *PC Magazine*. Retrieved from http://www.pcmag.com/article2/0,2817,2393464,00.asp

Dwyer C., Hiltz S. R., & Passerini, K. (2007) Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *Proceedings of the Thirteenth Americas Conference on Information Systems*, August 09 - 12 2007, Keystone, Colorado.

Facebook. (2009). Retrieved March 8, 2015 from http://www.facebook.com

Facebook. (2015). Retrieved March 3, 2015 from https://www.facebook.com/pages/BEWARE-OF-THE-NEW-FACEBOOK-VIRUS-DOING-THE-ROUNDS/112827395427374

Fensel, D., Hendler, J., & Lieberman, H. (2003). *Spinning the semantic web*. Cambridge, MA: MIT Press.

FOAF. (2014). *Vocabulary specification 0.99- Paddington Edition*. Retrieved December 15, 2014 from http://xmlns.com/foaf/spec/

FoafSites. (2013). Retrieved March 10, 2015 from http://www.w3.org/wiki/FoafSites

Gross. R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. *Proceedings of WPES'05*, November 7, 2005, Alexandria, Virginia, USA.

Johnson M., Egelman S., & Bellowin S.M. (2012). Facebook and privacy: It's complicated. *Symposium on Usable Privacy and Security (SOUPS)* 2012, July 11–13, 2012, Washington, DC.

Krishnamurthy, B., & Wills, C. E. (2010). On the leakage of personally identifiable information via online social networks. *ACM SIGCOMM Computer Communications Review*, Jan. 2010.

Krishnamurthy, B., Naryshkin, K., & Wills, C.E. (2011). Privacy leakage vs. Protection measures: The Growing Disconnect. *Web 2.Security and Privacy Workshop*, May 22-25, 2011, Oakland CA

Linked-in. (2003). Retrieved March 8, 2014 from https://www.linkedin.com/about-us?trk=hb_ft_about

Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). Analyzing Facebook privacy settings: user expectations vs. reality. *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, November 2-4, 2011, Berlin, Germany

Magid, L. (2014). *Facebook changes new user default privacy setting to friends only -- Adds privacy checkup*. Retrieved February 28, 2015 from:

http://www.forbes.com/sites/larrymagid/2014/05/22/facebook-changes-default-privacy-setting-for-new-users/

Madejski, M., & Bellovin, S.M. (2010). A study of privacy setting errors in an online social network. *Proceedings of the 4th IEEE International Workshop on Security and Social Networking*. March 29 2010-April 2 2010, Mannheim, Germany

Madejski, M., Johnson, M., & Bellovin, S. M. (2011). *The failure of online social network privacy settings*. CUCS-010-11

MySpace Wiki.(2003). Retrieved March 10, 2015 from http://en.wikipedia.org/wiki/Myspace

Narayanan, A., & Shmatikov, V. (2009). De-anonymizing social networks. *Proceedings of the 30th IEEE Symposium on Security and Privacy*. 173-187 Oakland, CA

Noyes, D. (2014, June). *The top 20 valuable Facebook statistics*. Retrieved February, 20, 2015 from https://zephoria.com/social-media/top-15-valuable-facebook-statistics/

Paul, T., Stopczynski, M., Puscher, D., Volkamer, M., & Strufe, T. (2012).C4PS - Colors for privacy settings. *World Wide Web 2012 Companion*, April 16–20, 2012, Lyon, France.

Unified Modelling Language. (1989). Retrieved March 13, 2015 from http://www.uml.org/

Biography

Lila Ghemri is an Associate Professor at the Department of Computer Science at Texas Southern University.

She holds a PhD in Computer Science from the University of Bristol, Bristol, UK. Before joining academia, she spent ten years in industry developing ontologies, knowledge bases and natural language processing systems. Her current research interest is in privacy of online social networks.