Enabling Privacy-awareness in Social Networks

Ted Kang and Lalana Kagal
MIT Computer Science and Artificial Intelligence Lab
32 Vassar Street Cambridge MA 02139
Email: {tkang, lkagal}@csail.mit.edu

Abstract

Most social networks have implemented extensive and complex controls in order to battle the host of privacy concerns that initially plagued their online communities. These controls have taken the form of a-priori access control, which allow users to construct barriers preventing unwanted users from viewing their personal information. However, in cases in which the access restriction mechanisms are bypassed or when the access restrictions are met but the data is later misused, this system leaves users unprotected. Our framework, Respect My Privacy, proposes an alternative approach to the protection of privacy. Our strategy is similar to how legal and social rules work in our societies where the vast majority of these rules are not enforced perfectly or automatically, yet most of us follow the majority of the rules because social systems built up over thousands of years encourage us to do so and often make compliance easier than violation. Our project aims to support similar functionality in social networks. Instead of focusing on enforcing privacy policies through restricted access, we focus on helping users conform to existing policies by making them aware of the usage restrictions associated with the data. The framework has two main functions - generating privacy or usage control policies for social networks, and visualizing these policies while exploring social networks. We have implemented this functionality across three platforms: Facebook, OpenSocial and Tabulator, a Semantic Web browser. These applications enable users to specify privacy preferences for their data and then display this privacy-annotated data prominently enabling other users to easily recognize and conform to these preferences.

Introduction

From their inception, social networks have suffered from a host of privacy issues. When social networks were first gaining in popularity, privacy mechanisms were sparse with most profiles being publicly available to all members. As social networks like Facebook and MySpace exploded in popularity, however, many users were shocked to find that the information that they had posted on their profiles were coming back to have unintended consequences in their real life: employers were reported to be using Facebook as a way to vet possible employees; universities were using Facebook pictures to identify people that had attended illegal functions; and children were being preyed on by sexual offenders on MySpace. Social networks responded to these highly publicized privacy concerns by implementing complex privacy controls that allowed users to construct barriers preventing unwanted users from looking at private information. This method of privacy protection, called access control, seeks to close off and hide information from those that are not explicitly given access to it. It is a binary system in which those that obtain access to the data, legitimately or not, have full reign over the use of that data while those without access cannot view anything.

These access restriction systems, while useful in blocking out unwanted viewers, are ineffective for a large, decentralized system like the World Wide Web. It is easy to copy or aggregate information, and it is often possible to infer ”private” information without actually having explicit access to the information itself. In addition, there are always human factors that a technical access restriction system will have trouble handling. For example, Facebook’s access restriction systems did not prevent users from unwillingly publicizing their purchases when Facebook introduced Beacon, a controversial advertising program. Only a mass protest from users caused Facebook to readjust their privacy controls (Story and Stone 2007). Given all these ways for data to escape from behind access restriction systems, we propose a more social approach to privacy.

The Respect My Privacy (RMP) framework offers an alternative approach to protecting privacy in social networks. It is based on Information Accountability (Weitzner et al. 2008), which argues that in addition to access control, there need to be ways of ensuring that people know exactly what they can and cannot do with personal or sensitive information. This approach is similar to the system in place for legal and social rules in society. In society, a set of legal or social norms govern what we can or cannot do, and they have been ingrained into our way of thinking such that most people go through life without any problems. When problems occur, there are mechanisms that ensure that those who broke the set of legal or social norms are reprimanded. Likewise, social networks should be policy-aware and have mechanisms in place that allow users who violate privacy or usage policies within the network to be identified and held accountable. However, an accountable system cannot be adequately implemented on social networks without assistance from the social network itself (such as in (Story and Stone 2007)), without detailed provenance trails to identify violators, and without regulation, which causes violators to be adequately punished. Though our long term vision includes a full accountable system, the RMP framework concentrates on technical soluctions for making social networks aware of privacy policies.

Our framework uses Semantic Web (Berners-Lee 2005) technologies for defining different kinds of privacy/usage restrictions and declaring restrictions associated with data. Through the use of these technologies, the RMP framework is able to support dynamic definition, extension, and re-use of meta-data describing privacy policy, intended purpose or use of data, mechanisms to attach this meta-data to any Semantic Web data to indicate its policy, and interoperability between different meta-data definitions.

The implementation of the RMP framework consists of four main parts: an ontology that defines classes of privacy restrictions and properties for attaching them to Semantic Web data, applications in Facebook and OpenSocial that allow users to create RMP restrictions and display them on their profile pages, a converter that translates a Facebook/OpenSocial profile into a widely used Semantic Web social ontology, Friend of a Friend (FOAF), and extensions to Tabulator (Berners-Lee et al. 2008) for adding restrictions to data and viewing restricted data in different colors to make it easier to responsibly browse and re-use social data.

Implementation

The current architecture of the RMP framework consists of two distinct parts. The first is RMP applications on mainstream social networks such as Facebook and OpenSocial. These applications are aimed at introducing RMP restrictions and attempt to spread some familiarity with the restrictions. The second is the Semantic Web aspect, which is aimed at supporting privacy/license/usage-aware browsing of data ultimately leading to decentralized social networks (Yeung et al. 2008).

Connecting these two parts is the FOAF converter, originally developed by Matthew Rowe, that was extended to support the RMP restrictons. The FOAF converter takes the personal information stored in Facebook along with associated RMP restrictions and creates a FOAF file that is stored on a Web server. This, in effect, becomes a profile in a decentralized social network if navigated through the Tabulator Extension.

RMP Restrictions and Ontology

Following the Creative Commons model, the RMP application aims to offer an easy user experience that allows users quickly declare the restrictions they wish to place on their data. However, unlike Creative Commons that provides a standard set of licenses, communities of users can easily generate their own privacy/usage ontologies to be used with our RMP framework.

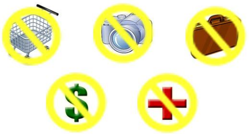


Figure 1: *The images for the five restrictions we've defined: no-commercial, no-depiction, no-employment, no-financial, and no-medical.*

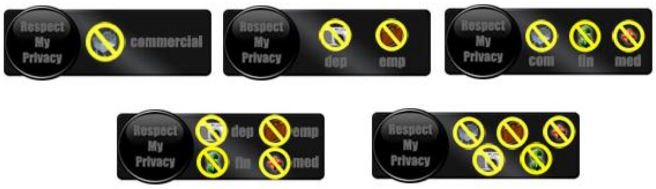


Figure 2: *RMP icons that can be placed on a social network profile page to indicate a certain privacy policy. Each policy is composed of several individual RMP restrictions and the icon link to a page containing additional information about the specific policy.*

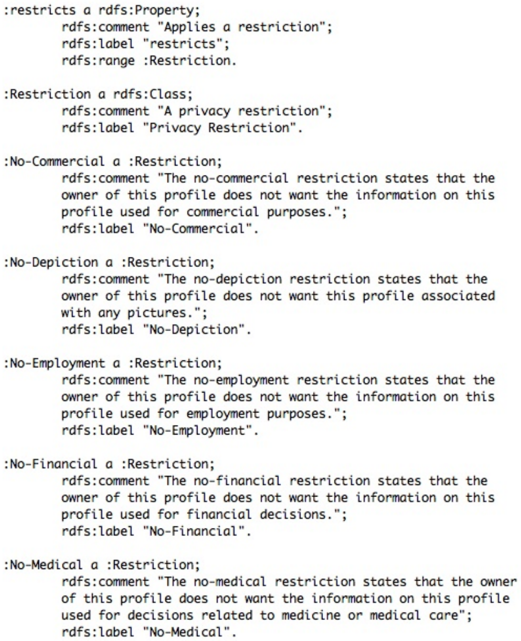
RMP offers simple privacy/usage restrictions for users through an ontology[1]. There are currently five restrictions that are implemented on RMP: *no-commercial*, *no-depiction*, *no-employment*, *no-financial*, and *no-medical*. Each of these restrictions has a corresponding picture as seen in Figure 1. For combinations of restrictions, these pictures are combined in different ways to create simple icons that can be placed on social network pages and link to additional information. A sample of these icons is shown in Figure 2. When associated with a Facebook or OpenSocial profile, these icons link to a page that offers additional information about each of the restrictions that has been applied. Users may choose to apply one or any combination of the five restrictions on their social network profiles and related pages. The lack of any of these restrictions on a profile page implies that the use is allowed. For example, not including the no-financial restriction would imply that you are willing to allow your personal information to be used for financial purposes.

no-commercial: The no-commercial restriction is similar to its counterpart in the Creative Commons. At the time when the RMP restrictions were being developed, there was no way to apply Creative Commons restrictions on the content that one posted to a social network. This restriction states that the user does not want anything on his profile or related pages to be used for a commercial purpose.

no-depiction: The no-depiction restriction implies that the user does not want her picture used for any reason and does not want her private information used to identify her in an image. This restriction was meant to specifically protect the pictures that users often post on social network sites. These posted pictures have been the most troubling with universities using student photos as evidence for infractions and employers using Facebook pictures to prove that employees were not doing what they claimed to be doing.

no-employment: The no-employment restriction declares that the user does not want any personal information used

[1] http://dig.csail.mit.edu/2008/02/rmp/rmp-schema.n3



```
:restricts a rdfs:Property;
        rdfs:comment "Applies a restriction";
        rdfs:label "restricts";
        rdfs:range :Restriction.

:Restriction a rdfs:Class;
        rdfs:comment "A privacy restriction";
        rdfs:label "Privacy Restriction".

:No-Commercial a :Restriction;
        rdfs:comment "The no-commercial restriction states that the
        owner of this profile does not want the information on this
        profile used for commercial purposes.";
        rdfs:label "No-Commercial".

:No-Depiction a :Restriction;
        rdfs:comment "The no-depiction restriction states that the
        owner of this profile does not want this profile associated
        with any pictures.";
        rdfs:label "No-Depiction".

:No-Employment a :Restriction;
        rdfs:comment "The no-employment restriction states that the
        owner of this profile does not want the information on this
        profile used for employment purposes.";
        rdfs:label "No-Employment".

:No-Financial a :Restriction;
        rdfs:comment "The no-financial restriction states that the
        owner of this profile does not want the information on this
        profile used for financial decisions.";
        rdfs:label "No-Financial".

:No-Medical a :Restriction;
        rdfs:comment "The no-medical restriction states that the owner
        of this profile does not want the information on this profile
        used for decisions related to medicine or medical care";
        rdfs:label "No-Medical".
```

Figure 3: *Part of the RMP ontology in N3 that defines possible types of privacy restrictions.*

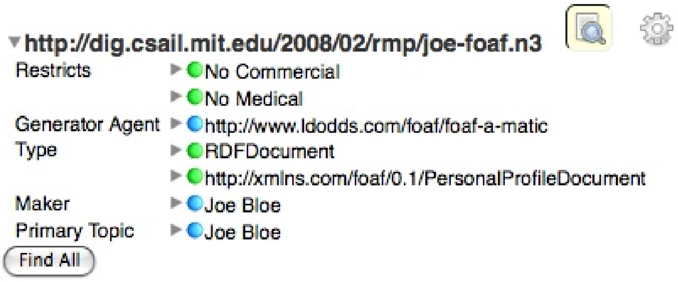
for the purposes of any kind of employment decision. For example, this would make companies aware that the user does not want them using their social network page as a way to vet them for a job. In addition, this would imply that an employer could not use personal information from a social network as justification for a firing. This restriction was meant again as a response to common incidents of users not being hired or being fired from a job owing to something they posted on a social network.

no-financial: The no-financial restriction declares that the user does not want any personal information used for any financial purposes. For example, the user would not want banks using personal information from the social network to influence a loan or credit decision, or have any influence in divorce proceedings.

no-medical: The no-medical restriction declares that the user does not want any personal information used for any medical purposes. For example, the user would not want hospitals or insurance providers using personal information from the social network to research into her lifestyle habits or more.

The restrictions are represented as ontological information in N3 (Berners-Lee 1998) as illustrated in Figure 3. This ontology can be easily modified or extended to meet different requirements. A restriction for a data item such a FOAF profile is declared using the *restricts* property from the ontology. For example, to specify that Ted's profile is restricted to *no-commercial*, Ted would include the following in his FOAF profile (where <> refers to his profile)

```
<> a foaf:PersonalProfileDocument;
     rmp:restricts rmp:No-Commercial.
```



▾http://dig.csail.mit.edu/2008/02/rmp/joe-foaf.n3

Restricts	▸ ● No Commercial
	▸ ● No Medical
Generator Agent	▸ ● http://www.ldodds.com/foaf/foaf-a-matic
Type	▸ ● RDFDocument
	▸ ● http://xmlns.com/foaf/0.1/PersonalProfileDocument
Maker	▸ ● Joe Bloe
Primary Topic	▸ ● Joe Bloe

Figure 4: *A sample FOAF file of a user that has applied the no-financial restrictions on her FOAF file as viewed in the Tabulator.*

It is possible to combine multiple restrictions such as in Figure 4, which is a sample FOAF file where the user has selected to apply both the *no-commercial* and *no-medical* restrictions on his FOAF profile. RMP restrictions can be attached to any resource including images, projects, and clinical trials. The example below is a description of a clinical trial that has *no-commercial* and *no-financial* restrictions associated with it.

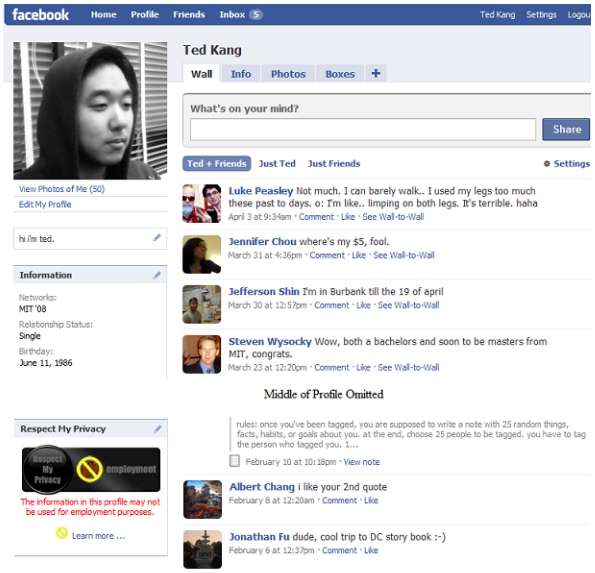
```
@prefix ex: <http://example.cancer.gov#> .
@prefix ma: <http://example.ma.gov#> .

:C123 a ex:ClinicalTrial;
   ex:phase ex:PhaseIII;
   ex:type ex:HealthServiceResearch;
   ex:Status ex:Active;
   ex:sponsor ma:MGH;
   ex:protocolID ex:116892-193;
   rmp:restricts rmp:No-Commercial,
                 rmp:No-Financial.
```

RMP on Facebook and OpenSocial

The RMP application on Facebook is a MySQL/PHP driven Web application that uses the Facebook Application API[2]. In order to mimic the ease of use for Creative Commons, the creation of a RMP setting is simple, taking mere minutes. When a user decides to add the RMP application, they are directed to a page that explains the philosophy behind RMP. This page is very important as RMP on Facebook is currently a project entirely dependent on its members. As more users create the RMP restrictions and expect their restrictions to be respected, organizations will feel more pressure to actually respect those restrictions. Thus, the introductory text attempts to instill the idea that the user is part of a movement that will improve everyone's social network experience the more the user respects others restrictions. The user is then directed to a page that lists the five restrictions with descriptions of each. Each restriction has an accompanying checkbox, which allows the user to decide whether they want to apply that restriction or not. Once they have chosen the restrictions, they are done. The restrictions are saved into the MySQL database and the appropriate icon is pushed to

[2] http://www.facebook.com/apps/application.php?id=10637134047



Ted Kang

What's on your mind?

hi i'm ted.

Information

Networks:
MIT '08

Relationship Status:
Single

Birthday:
June 11, 1986

Luke Peasley Not much. I can barely walk.. I used my legs too much these past to days. o: I'm like.. limping on both legs. It's terrible. haha
April 3 at 9:34am · Comment · Like · See Wall-to-Wall

Jennifer Chou where's my $5, fool.
March 31 at 4:36pm · Comment · Like · See Wall-to-Wall

Jefferson Shin I'm in Burbank till the 19 of april
March 30 at 12:57pm · Comment · Like · See Wall-to-Wall

Steven Wysocky Wow, both a bachelors and soon to be masters from MIT, congrats.
March 23 at 12:20pm · Comment · Like · See Wall-to-Wall

Middle of Profile Omitted

Respect My Privacy

The information in this profile may not be used for employment purposes.

rules: once you've been tagged, you are supposed to write a note with 25 random things, facts, habits, or goals about you. at the end, choose 25 people to be tagged. you have to tag the person who tagged you. 1...
February 10 at 10:18pm · View note

Albert Chang i like your 2nd quote
February 8 at 12:20am · Comment · Like

Jonathan Fu dude, cool trip to DC story book :-)
February 6 at 12:37pm · Comment · Like

Figure 5: *A user's Facebook profile with the RMP icon in the lower left. Any Facebook user who clicks on that icon is directed to a page, which offers additional information on the applied restrictions.*

the profile page so that everyone who visits a user's profile page can clearly see the restrictions that the user has placed on his personal information.

Once a user has created a set of RMP restrictions, there are several features that become available to them. First, the user's RMP icon is pushed onto their profile page along with some informative text in the following context: "The information on this profile may not be used for ... purposes." Now anyone who visits that profile page will be able to view the RMP icon. A sample Facebook page with the RMP icon visible in the lower-left is shown in Figure 5.

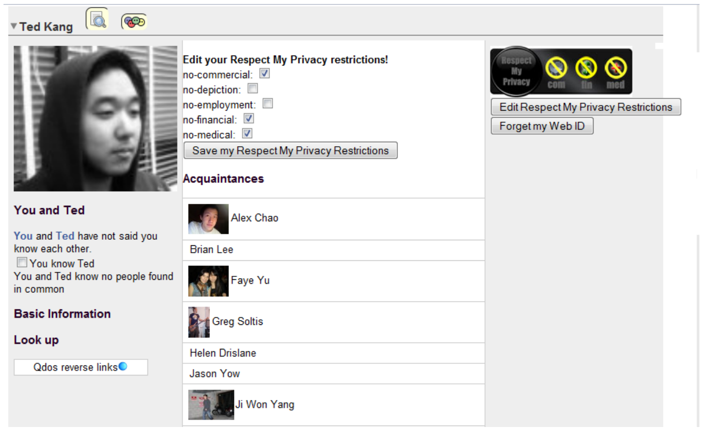
If any visitor clicks on the RMP icon they will be directed to a page that lists the restrictions that the user has decided to apply and a paragraph giving more information on the restrictions chosen. The users are then invited to join the RMP movement on Facebook by creating their own set of licenses.

The RMP application on OpenSocial is driven primarily by Javascript. OpenSocial's API and data storage is fairly different from that of Facebook, relying heavily on Javascript and not an actual database, but the OpenSocial application was designed to be exactly like its counterpart on Facebook.

The FOAF Converter

The RMP application on Facebook allows users to port their Facebook profiles to FOAF files. This acts as a bridge between the RMP applications in Facebook and the corresponding extensions on the Tabulator. Users can download the FOAF file generated from their Facebook profile and host it on a Web server.

This will hopefully introduce members of mainstream social networks to the idea of decentralized social networks. With further work on Tabulator, users might be able to see the advantages of having complete control of their data especially as methods of attaching provenance and more sophisticated accountability mechanisms are developed.


Ted Kang
Respect My Privacy
com
fin
med
Edit Respect My Privacy Restrictions
Forget my Web ID
Save my Respect My Privacy Restrictions
Qdos reverse links

Edit your Respect My Privacy restrictions!
no-commercial: ☑
no-depiction: ☐
no-employment: ☐
no-financial: ☑
no-medical: ☑

You and Ted

You and Ted have not said you know each other.
☐ You know Ted
You and Ted know no people found in common

Basic Information

Look up

Acquaintances

Alex Chao
Brian Lee
Faye Yu
Greg Soltis
Helen Drislane
Jason Yow
Ji Won Yang

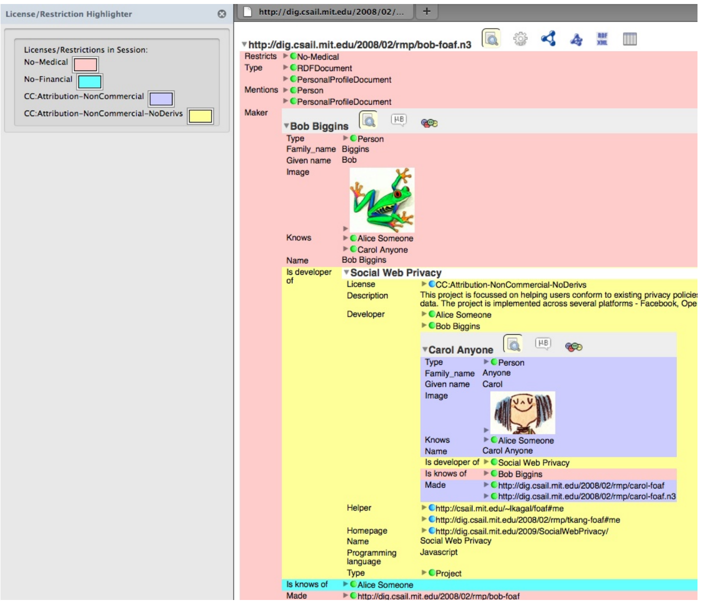
Figure 6: *The social pane on the Tabulator offers a social network profile like view of FOAF information and also allows users to create and edit RMP restrictions.*

Social pane and RMP sidebar for Tabulator

Tabulator is a generic Semantic Web data browser and editor for RDF data, similar to how a web browser is used to navigate HTML pages. Tabulator is currently implemented as a Firefox extension. When a user installs the extension and uses Firefox to go to a URI that contains RDF triples, Tabulator offers an easy interface with which to view the RDF data and allows users to easily explore triple relationships to obtain more data. Tabulator recently implemented a social pane that becomes available when users browse FOAF data. The social pane displays the FOAF data in a format similar to social network profiles, allowing the typical social network experience in a decentralized setting.

We modified the social pane to enable users to attach CC licenses and RMP restrictions to their FOAF files. Users with editable FOAF files can use Tabulator to identify a FOAF files as their identity. Once an identity has been established, users can host their editable FOAF files on WebDAV (Wikipedia) servers and use SPARQL (W3C 2008) updates to create or edit the restrictions they place over their FOAF profiles. The social pane also displays the RMP icons if restrictions are detected, similar to the RMP applications on the mainstream networks. An example social pane that would occur when browsing upon a FOAF file with Tabulator is shown in Fig 6.

In addition, we've implemented a license/restriction aware sidebar. This sidebar makes it easy to recognize protected data while browsing semantic information using Tabulator. The sidebar detects the presence of RMP restrictions or Creative Commons licenses as data is browsed, and prominently displays this protected data in different colors. Users can customize colors for each restriction or license



License/Restriction Highlighter

Licenses/Restrictions in Session:
No-Medical 🟥
No-Financial 🟦
CC:Attribution-NonCommercial 🟪
CC:Attribution-NonCommercial-NoDerivs 🟨

http://dig.csail.mit.edu/2008/02/...

http://dig.csail.mit.edu/2008/02/rmp/bob-foaf.n3
Restricts No-Medical
Type RDFDocument
PersonalProfileDocument
Mentions Person
PersonalProfileDocument
Maker
Bob Biggins
Type Person
Family_name Biggins
Given name Bob
Image
Knows Alice Someone
Carol Anyone
Name Bob Biggins
Is developer of
Social Web Privacy
License CC:Attribution-NonCommercial-NoDerivs
Description This project is focussed on helping users conform to existing privacy policie
data. The project is implemented across several platforms - Facebook, Ope
Developer Alice Someone
Bob Biggins
Carol Anyone
Type Person
Family_name Anyone
Given name Carol
Image
Knows Alice Someone
Name Carol Anyone
Is developer of Social Web Privacy
Is knows of Bob Biggins
Made http://dig.csail.mit.edu/2008/02/rmp/carol-foaf
http://dig.csail.mit.edu/2008/02/rmp/carol-foaf.n3
Helper http://csail.mit.edu/~lkagal/foaf#me
http://dig.csail.mit.edu/2008/02/rmp/tkang-foaf#me
Homepage http://dig.csail.mit.edu/2009/SocialWebPrivacy/
Name Social Web Privacy
Programming language Javascript
Type Project
Is knows of Alice Someone
Made http://dig.csail.mit.edu/2008/02/rmp/bob-foaf

Figure 7: *The license/restriction highlighting sidebar detects CC licenses and RMP restrictions and highlights the protected data. Different licenses/restrictions are assigned different random colors that the user can customize.*

identified and any data that is protected by a restriction or license will be highlighted in the chosen color, allowing users to instantly recognize the information that is protected under certain policies. An example of the the policy aware sidebar with the highlighting functionality is shown in Figure 7. The figure shows Bob's FOAF file in pink because his profile has a *no-medical* restriction associated with it. Bob works on the Social Web Privacy project, which appears in yellow as it is restricted by the *CC Attribution Non Commercial Non Derivative* license. Carol is a developer on the project and her privacy preference is the *CC Attribution Non Commercial* license that causes her information to appear in lavender.

Related Work

Shortly after our Facebook application was developed, the Creative Commons released a Facebook application (Lardinois 2009). In this application, users are able to choose from the six Creative Commons licenses and apply them over their entire profiles. Users are given the recognizable Creative Commons icon and are able to publish it on their profiles linking to a page with more information. This application is definitely a step in the right direction as it does not solely rely on access control to prevent unwanted users from viewing data but declares to all viewing users certain restrictions on how they want their licensed information used. However, it restricts users to selecting one of the existing CC licenses whereas with the RMP framework, users and communities are free to define and use their own privacy/usage ontologies or extend and reuse ontologies defined by others.

A second example of users proactively being able to control how their personal information is used is with an extension proposed to Google AdSense ads. Google AdSense includes a notion of policy-awareness by putting a hyperlink "Ads by Google" on all its advertisements (Hansell 2009). When clicked, the user gets general information about why these ads were displayed and is able to slightly modify how further targeting is performed. Turow proposes an extension in which each ad will have an icon that when clicked displays exactly what information was used in order to choose that ad [3]. These approaches are related to our framework in that they attempt to make policy explicit but they focus on the use of search/clickstream data for targeted advertisements versus the use of personal data available in social networks.

Another example, the Platform for Privacy Preferences (P3P) relies on server-side policy markup to describe how user information collected by servers is utilized (Cranor et al. 2002). The main goal is to allow users to understand how servers use their data. Unfortunately enforcement is a problem because it is difficult for users to verify whether servers actually conform to their own policies. In our approach, anyone can markup their own data and our goal is awareness of these privacy annotations and is not so much about enforcement.

Future Work

The RMP project still has areas that require significant work. First, the applications in the framework expect privacy annotations to be associated with resources such as documents or FOAF profiles and are unable to handle more finely grained annotations such as privacy restrictions on a user's participation in a specific clinical trial. We would like to use N3Logic (Berners-Lee et al. 2007) or POWDER (W3C 2007) to allow any RDF sub-graphs within a document to be annotated with RMP privacy restrictions and support this in our Facebook, Open Social applications as well as in Tabulator.

As social networks move from being centralized hosted applications to more decentralized applications (Yeung et al. 2008), the role of RMP becomes more important. In these decentralized networks, accessing, copying, and reusing data inappropriately becomes even easier. Using RMP will enable users to specify their privacy requirements and encourage third party application developers to develop tools such as the RMP Tabulator sidebar that clearly identifies the restrictions of social data.

Another area of future work is in building accountable systems that will be able to use the provenance attached to data to pinpoint cases of misuse. Systems that are able to model and implement policies have been created and demonstrated in the case of data mining, but there has been no clear conclusion on how to detect misuse in the context of social networks. One problem in this area is the difficulty in pinpointing "use" in a social network. In many contexts, such as an employer doing a background check on a potential employee, merely looking at unflattering data on the prospective employee's social network profile might

[3] http://www.asc.upenn.edu/ascfaculty/FacultyBio.aspx?id=128

be enough to eliminate him from getting a job. A possible solution is to allow users to create multiple FOAF files on the decentralized social network, and have servers hosting the FOAF files to query visitors for their intent in viewing the profile. Based on the visitor's intent, the server can display one of the user's more appropriate profiles. This strategy is similar to those taken by niche social networks, like LinkedIn, that are made specifically for a certain purpose, such as networking. Nonetheless, determining what defines a "use" in the context of social network information is a problem that requires future work.

Summary

The efforts of social networks in protecting privacy could be greatly improved with the adoption of information accountability techniques. One of the main tenets of accountable systems is transparency in policy that the Respect My Privacy project follows by providing simple mechanisms for defining privacy restrictions on social data and encouraging responsible re-use of this data by making it privacy-aware.

Acknowledgements

The authors wish to thank their group members for their contributions to this project. This work was carried out with funding from NSF Cybertrust award number CNS-0831442, IARPA award number FA8750-07-2-0031 and AFOSR award number FA9550-09-1-0152.

References

Berners-Lee, T.; Connolly, D.; Kagal, L.; Scharf, Y.; and Hendler, J. 2007. N3logic: A logical framework for the world wide web. *Journal of Theory and Practice of Logic Programming*.

Berners-Lee, T.; Hollenbach, J.; Lu, K.; Presbrey, J.; Prud'ommeaux, E.; and mc schraefel. 2008. Tabulator Redux: Browing and Writing Linked Data . In *Linked Data on the Web Workshop at WWW08*.

Berners-Lee, T. 1998. Notation 3. http://www.w3.org/DesignIssues/Notation3.html.

Berners-Lee, T. 2005. Primer: Getting into RDF and Semantic Web using N3. http://www.w3.org/2000/10/swap/Primer.

Cranor, L.; Langheinrich, M.; Marchiori, M.; Presler-Marshall, M.; and Reagle, J. 2002. Platform for Privacy Preferences (P3P). http://www.w3.org/P3P.

Hansell, S. 2009. An Icon That Says They're Watching You. http://bits.blogs.nytimes.com/2009/03/19/an-icon-that-says-theyre-watching-you/.

Lardinois, F. 2009. Creative Commons Releases Facebook App: Choose a License for Your Photos, Videos, and Status Updates - ReadWriteWeb. http://www.readwriteweb.com/archives/creative_commons_releases_facebook_app.php.

Story, L., and Stone, B. 2007. Facebook Retreats on Online Tracking. http://www.nytimes.com/2007/11/30/technology/30face.html.

W3C. 2007. Protocol for Web Description Resources (POWDER). http://www.w3.org/2007/powder.

W3C. 2008. Sparql rdf query language (sparql). http://www.w3.org/TR/rdf-sparql-query/.

Weitzner, D. J.; Abelson, H.; Berners-Lee, T.; Feigenbaum, J.; Hendler, J.; and Sussman, G. J. 2008. Information accountability. *Communications of the ACM*.

Wikipedia. Web-based Distributed Authoring and Versioning. http://en.wikipedia.org/wiki/WebDAV.

Yeung, C. A.; Liccardi, I.; Lu, K.; Senevirante, O.; and Berners-Lee, T. 2008. Decentralization: The Future of Online Social Networking. In *MSNWN Position Paper*.