Respect My Privacy

by

Ted Taiho Kang

S.B., C.S. M.I.T., 2008

Submitted to the Department of Electrical Engineering and Computer Science

in Partial Fulfillment of the Requirements for the Degree of

Master of Engineering in Electrical Engineering and Computer Science

at the Massachusetts Institute of Technology

May 2009

Author_____
Department of Electrical Engineering and Computer Science
May 22, 2009

Certified by_____
Lalana Kagal
Research Scientist, Computer Science and Artificial Intelligence Lab
Thesis Supervisor

Accepted by_____
Arthur C. Smith
Professor of Electrical Engineering
Chairman, Department Committee on Graduate Theses

Respect My Privacy
by
Ted Taiho Kang
Submitted to the
Department of Electrical Engineering and Computer Science

May 22, 2009

In Partial Fulfillment of the Requirements for the Degree of
Master of Engineering in Electrical Engineering and Computer Science

Abstract

Most social networks have implemented extensive, complex privacy controls in order to battle the host of privacy concerns that initially plagued their online communities. These privacy controls have taken the form of access restriction, which allows users to specify who is and who is not allowed to view their personal information. This binary system leaves users unprotected in the, hopefully rare, cases in which the access restriction mechanisms are bypassed. Respect My Privacy offers a different approach to privacy protection, founded on the philosophies of Information Accountability. Respect My Privacy aims to allow users to clearly declare the policies that govern the use of their data, and implement mechanisms that promptly notify the user of misuse after the fact. In its current state, the Respect My Privacy project has been implemented across three platforms: Facebook, OpenSocial, and the Tabulator extension with a focus on defining a clear vocabulary for discussing restrictions on use of data and making it simple for users to display and edit the restrictions users wish to place on their personal information. There is also a discussion on decentralized social networks and their role in the future of Respect My Privacy and social networks in general.

Thesis Supervisor: Lalana Kagal
Title: Research Scientist, Computer Science and Artificial Intelligence Lab

Acknowledgements

I would like to thank my supervisor, Lalana Kagal, for her patience and guidance throughout the thesis process. I would not have been able to finish this thesis without her. I would also like to thank Daniel Weitzner for his foundational ideas on applying Information Accountability to social networks. Thanks also goes out to Tim Berners Lee and the DiG students for help and suggestions with the Tabulator extension. Finally, I would like to thank my mom and dad for all the support and sacrifices throughout the years.

Contents

List of Figures

Chapter 1

Introduction

There has been a recent trend on the Internet characterized by a focus on the user and user-generated content. This trend, popularly deemed the "Web 2.0 revolution" includes a variety of technologies: blogs, social networking sites, wikis, and Web services that rise above simple, read-only websites. With the spread of Web 2.0, there has been an explosion of potentially sensitive, user-generated content; unsurprisingly, a glut of privacy issues have followed suit. A large source of these privacy issues arise from social networks, such as MySpace or Facebook, which allows users to create profiles, upload pictures, and have their own "space" in an online community.

In response to these privacy concerns, most social networks have adopted privacy controls that attempt to prevent 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 strictly given access; however, this seems to be contrary to the spirit of social networks. As evidenced by Facebook's statement of purpose: "Giving people the power to share and make the world more open and connected,"[1], the general goal of social networks is to

allow people to share information about themselves while making it easier to connect with people around the world. Given this clash between the spirit of social networks and the privacy protections they employ, Respect My Privacy offers a new way for members of social networks to protect their privacy.

The Respect My Privacy project falls under the general philosophy of information accountability, which argues that in addition to access control, there need to be ways of holding people accountable when they misuse personal or sensitive information. Respect My Privacy aims to allow users to clearly declare how they want their data handled, ensuring that users who somehow bypass access restriction mechanisms are still made aware of the policies governing the data. In addition, Respect My Privacy hopes to eventually implement accountable systems that will be able to understand the policies governing a user's data and notify those responsible for that piece of data when the data is misused.

This is a distant goal but progress has been made in developing the initial stages of the Respect My Privacy project. The Respect My Privacy project currently offers members of social networks a vocabulary with which to declare restrictions that they want applied to their data usage. In addition, the current implementation of the Respect My Privacy is designed to be simple and easy to use so that the Respect My Privacy restrictions can gain widespread traction on the Internet before accountability mechanisms are put in place. This will allow users of Respect My Privacy to utilize social pressure to ensure that the policies governing their data are met.

The rest of this paper will be organized as follows. Chapter 2 will discuss the philosophy of Information Accountability in depth before delving into the design goals and

strategies of the Respect My Privacy project. Chapter 3 will introduce the five restrictions that are implemented in Respect My Privacy: *no-commercial*, *no-depiction*, *no-employment*, *no-financial*, *no-medical*. Chapter 4 will describe the current implementations of Respect My Privacy on the mainstream social networks, Facebook and OpenSocial, before discussing why these social networks were deemed inadequate for future work in Respect My Privacy. Chapter 5 will describe the work done on decentralized social networks and why they are a more appropriate platform for future work on Respect My Privacy. Finally, Chapter 6 will discuss the future work on the project and end with some final thoughts.

Chapter 2

Background & Overview

2.1 Information Accountability

Information Accountability is a general philosophy that argues for a shift in focus when designing systems meant to comply with certain policies. There are two general strategies that one can take when protecting private information: access control and information accountability. Access control is the predominant strategy used to protect information online, and usually involves building impediments that prevent access to private information. These impediments could take the form of passwords, cryptographic signatures, certificates, or any other technical mechanism that attempts to restrict access to sensitive information to certain individuals or groups. Most of the current privacy research focuses on developing better and better mechanisms to keep people away from private information.

Proponents of information accountability argue that this approach is not effective for a large, decentralized system like the World Wide Web. In a system such as the World Wide Web, it is simply too easy to copy or aggregate information, and it is often possible to infer

"private" information from external sources without actually ever having explicit access to the information itself. In addition, systems that rely solely on access restriction are woefully inadequate in cases where information is somehow compromised. This, unfortunately, happens to even the most meticulously designed technical systems as factors like human error often provide ways to completely circumvent the access control mechanisms. An apt analogy from *Information Accountability* by Weitzner et al. compares sole reliance on access restriction to "focusing all one's attention on closing the barn door and ignoring what might happen to the horses after they've escaped."[2]

Given the shortcomings of access restriction, information accountability proposes an increased focus on building systems that promote transparency and appropriate use. The idea of transparency is important as accountable systems are partly dependent on the notion that most people, when clearly told how sensitive data can and cannot be used, will not maliciously misuse data. In an accountable system, transparency is vital when dealing with provenance, or history, and policy, the rules that govern what is considered appropriate use, for a piece of data. Provenance is important in ensuring that there is a clear and accurate transcript regarding the history of a piece of data. In a world where information is trivial to copy, it is important to know where a piece of data was obtained and how it has been used along the way. For example, the creator of a piece of information might have allowed people to use his data as long as he was properly attributed and the data was not changed in any way. It could be the case that several users copy this piece of data and use it appropriately, unchanged with the proper attribution. However, if any user then takes the data from these users and, accidentally or maliciously, presents it as his own work without restrictions, anyone that takes the data from this user might

continue to use the data inappropriately without even knowing that he is violating the wishes of the creator of the data. This kind of situation can be solved if data were somehow attached with providence information such that one could trace a piece of data back to its point of inception and see exactly where misuse occurred.

Transparency in policy is important to ensure that anyone that uses a piece of data has clear knowledge of what can and cannot be done with the data. It would be unfair to punish people who misused a piece of data merely because it was not obvious to them how they could use the data appropriately. This implies that policies must be presented in a way that is clear and simple to understand but unobtrusive to the casual browsing experience.

When policies and provenance information pertaining to a piece of data are transparent, information accountability also argues for systems that promote accountable use. This means that there needs to be some sort of way to ensure that inappropriate use is quickly unearthed. When inappropriate use is found, those responsible for the piece of data should be notified as quickly as possible with information regarding how their data was misused and who misused it. From there, the creator can deal with the misuse according to his discretion. This requirement implies that policies should be machine-readable so that systems can read and understand policies and report violations promptly as it is unrealistic to expect that a system as large and as decentralized as the Internet can be monitored for misuse simply through manpower.

We can then imagine an accountable system that has machine-readable policies that can be presented clearly to users. The data in the system are all attached with provenance information such that when information is used, the system can trace backwards and ensure that all policies pertaining to that piece of data have been met. If not, the provenance information can

be used to find the creator, or people originally responsible, for the misused data and inform them promptly. This system is similar to the "system" in place for ensuring that we act appropriately in our daily lives. We have a set of laws, or social norms, that govern appropriate use of behavior. These laws are made transparent, for the most part, to everyone in society. Most people in society are aware of what is considered appropriate use and follow the laws willingly. When laws are broken, police officers and attorneys use evidence, which in our case is provenance, to confirm the breaking of a law, after the fact. Those that are found to have broken the law are dealt with appropriately.

Finally, it is important to recognize that Information Accountability does not call for the replacement of access restriction systems with accountable ones. It merely argues that there is no reason to focus the entirety of one's efforts into making a system that keeps unwanted users out without focusing some attention to tracking the use of that information in the case that it is compromised. When information accountable systems are used in conjunction with access restriction systems, one can imagine a system in which users can not only specify who is able to view their data but what they can do with it. However, when the access restrictions are somehow bypassed, there is another line of defense that will inform the user that his data has been misused. In addition, given the provenance information, administrators will have a clear trail of how the information bypassed the access restriction system, which can only serve to strengthen it.

2.2 Respect My Privacy

Respect My Privacy is a project aimed at employing the strategies of information accountability on social networks. There have been countless cases of members of social

networks unthinkingly posting sensitive information and suffering negative consequences, ranging from embarrassment to expulsion from school or termination of employment. As a response to these well known incidents, most large social networks implemented access control mechanisms that allow users to specify who can and can't look at their information. Facebook, for example, has complex access restriction settings that specify various types of data that users can post on Facebook and the people who are allowed to view that information. As with most access restriction systems, the systems are not perfect and people have found ways to get around the system, inappropriately accessing and using private information. When these access restriction systems are bypassed, sometimes unknowingly, users are unprotected from abuse of the information they intended as private.

To successfully apply the strategy of information accountability to social networks, one must ensure that transparency and ensuring accountable use is stressed. Transparency implies making appropriate usage clear to users. This includes allowing people to clearly declare how they want their personal data to be used. Although this may seem obvious, current access restriction systems do not allow a person to actually declare to the public how they want their data handled. Instead, users set conditions on who can view their data, a binary system in which users that have access have free rein to do what they will while those that do not have access are not allowed to even look at the data. This leads to cases where users stumble upon holes in access restriction systems and do not even realize that they are looking at private information that the user wanted protected.

Another important aspect of transparency and appropriate use, as previously discussed, is provenance. This, however, is a difficult problem in its own right as there are a

plethora of data types online and one must find a way to attach lightweight provenance information to these piece of data that is difficult to alter or remove, but still easily available for the systems that need to access it. This problem is out of the scope of this thesis, as most of my work on the Respect My Privacy project deals with establishing rules of appropriate use and increasing transparency for editing and viewing these rules.

In trying to establish a set of social norms on how personal information on social networks can be used, we looked towards Creative Commons model to try to achieve widespread acceptance.

2.2.1 Creative Commons

Creative Commons is a nonprofit corporation founded by Lawrence Lessig that is "dedicated to making it easier for people to share and build upon the work of others, consistent with the rules of copyright."[3] One of the main reasons that Creative Commons has reached its level of widespread acceptance and success is its simplicity. To receive a free Creative Commons license, users merely have to log onto the Creative Commons website and choose one of their six licenses. The users choose whether they want to allow commercial uses of their work, a simple yes or no, and if they want to allow modifications of their work. Users can choose whether they want to disallow the modification of their work completely, allow free modification of their work, or allow modification of their work as long as those that modify their work apply the same Creative Commons license to the new work. Creative Commons then employs a small, simple icon that notifies users about the type of license that is placed on a piece of work. The icon is a simple rectangle with the common "CC" logo on the left and smaller intuitive icons that represent the type of restrictions on the license. By clicking on the icon, users

are redirected to a page that gives additional details about the license. The Creative Commons icons and a sample associated information page is shown in Figure 2-1.

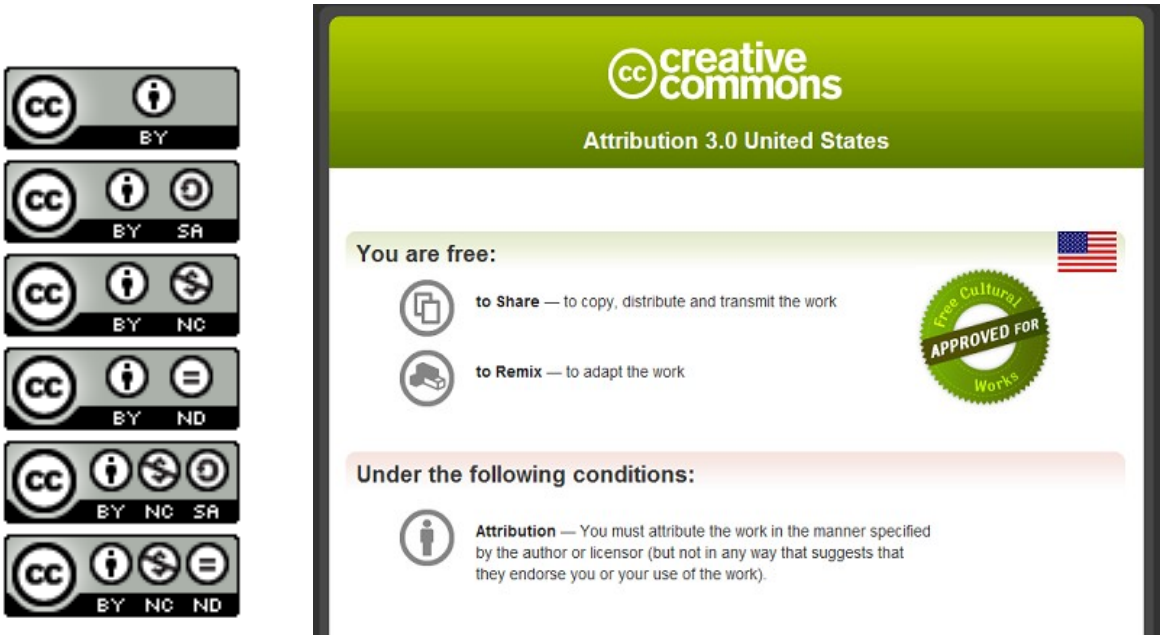


Figure 2-1: The six Creative Commons icons, and a sample information page

2.2.2 Branding

When attempting to enforce a new set of policies on a massive decentralized system such as the Internet, it is vital to have mechanisms that are simple for people to recognize and implement; in effect, it is important to create a "brand." Like the Creative Commons licenses, we wanted to offer an easy user experience that allows users to specify how they want their personal information to be used. Afterwards, users would be given a small, simple, and recognizable icon that could be posted on their profile and personal pages on social networks. As with the Creative Common's licenses, we hope that as more and more people see the Respect My Privacy icons attached to profile pages, it will gain traction and widespread acceptance.

The first step in branding the Respect My Privacy project involved brainstorming appropriate names for the project itself. Some possible options included Reciprocal Privacy, Social Commons, My Brother's Keeper, Privacy in Public, Secure Commons, and many more. We finally decided on Respect My Privacy as it was a simple, easily recognizable name that made the project's intentions clear. In addition the idea of respect is important within the project as we are aiming to institute a kind of 'social norm' online that is founded on the fact that the online community needs to respect each other's privacy in order to move away from the barriers and access restriction systems that act in opposition to the goals of social networks.

Another important component of the Creative Commons brand is the simple “CC” icons. Similar to the six difference licenses offered by Creative Licenses, Respect My Privacy has five different restrictions that users can pick and choose from: no-commercial, no-depiction, no-employment, no-financial, and no-medical. These restrictions and their associated icons will be discussed at length in the following chapter. Also like the Creative Commons icons, the Respect My Privacy icons will link viewers to an extended informative page where the applied restrictions are explained.

Chapter 3

Restrictions

In keeping with the Creative Commons model, we offer predetermined restrictions for Respect My Privacy users. By offering predetermined restrictions, we ensure a better user experience and are able to create simple and recognizable icons that will assist in the widespread acceptance of Respect My Privacy. Many of these restrictions were created by Danny Weitzner, based on the Creative Commons licenses, but slightly altered for use on social networks[4]. There are currently five restrictions that are implemented on Respect My Privacy: *no-commercial*, *no-depiction*, *no-employment*, *no-financial*, and *no-medical*. Users may choose to apply none or any combination of the five restrictions on their social network profiles and related pages.

This set of restrictions is currently aimed more at organizations as they, more than individuals, have a vested interest in protecting privacy interests. This can be seen by the current trend of appointing CPOs, or Chief Privacy Officers, who ensure that companies are aware of

and protect privacy interests. There is a market place for privacy that is being created and surveys report that consumers prefer organizations that respect privacy interests to those that do not[5]. The hope is that the competition between organizations to protect privacy will make them respect privacy declarations, fearing bad public relations, more so than individuals would.

3.1 no-commercial

Figure 3-1: The icon for the *no-commercial* restriction

The first restriction is *no-commercial*. The icon, shown in Figure 3-1, for the no-commercial restriction features a shopping cart and a yellow circle with a slash overlaying it. The yellow circle with a slash will be a common feature in every restriction's icon. In the informative page linked to by each icon, the text for the *no-commercial* restriction reads: “This restriction communicates that this user does not want his/her profile and anything associated with it used for commercial purposes. For example, no one has permission to use the user's picture or information located on the profile for any commercial use.” This restriction is similar to its counterpart in the Creative Commons and protects the user's information or his pictures from being used in any context to make money. This restriction is important as social networks are constantly adding new functionality that allow users to showcase their work, whether it be pictures, writing, or more. Given that at the time of the project's inception, no social networks

currently allow users to apply Creative Commons licenses to the data they choose to upload, this license would offer the same protections that a Creative Commons cc:commercial license would offer. This restriction will also hopefully encourage users of social networks to feel safe sharing their original works with others without fear of others stealing their work for commercial use. The absence of the no-commercial restriction implies that one is allowing commercial use of his work.

3.2 no-depiction

Figure 3-2: The icon for the *no-depiction* restriction

The second restriction is no-depiction. The icon, shown in Figure 3-2, for the no-depiction restriction is a camera overlayed with the yellow circle and slash. In the informative page linked to each icon, the text for no-depiction reads: "This restriction communicates that the user does not want his/her profile and anything associated with it used to depict him/her in a picture. For example, no one has the user's permission to use his/her profile to identify the user in an image. Furthermore, no one may use any pictures of the user on his/her profile page and related pages for any purpose." This restriction protects a user's information from being used to identify him in a picture or from anyone taking the user's pictures for any purpose. This restriction is important as it has become standard in nearly all social networks to be able to

upload photos albums onto the social network and choose a profile picture that is shown on the profile page. This restriction was specifically created owing to the numerous, well-publicized cases of photos causing people to suffer unintended consequences. Universities have been known to use pictures of Facebook to identify people that attended illegal functions, and employers have been found to use pictures on Facebook to prove that employees were not doing what they claimed to be doing. This restriction will allow users to declare that they do not want the pictures of themselves on the social network used to identify them.

3.3 no-employment

Figure 3-3: The icon for the *no-employment* restriction

The third restriction is no-employment. The icon, shown in Figure 3-3, for the no-employment restriction is a camera overlayed with the yellow circle and slash. In the informative page linked to each icon, the text for no-employment reads: “This restriction communicates that this user does not want his/her profile and anything associated with it used for employment purposes. For example, employers do not have permission to use information from the user's profile to influence a hiring or firing decision.” This restriction allows a user to declare that he does not want the information he posts on his profile page and related pages to be used for or against him in the context of employment. This represents another class of problems

that were highly prevalent when social networks first became popular online. There were again several, highly publicized incidents where it was reported that employers were making hiring decisions based on information found on a prospective employee's Facebook page. These problems were the first catalysts for the current access restriction systems that most social networks have in place. Given that there are an increasing number of niche social networks, such as LinkedIn, which focuses specifically on networking in a business context, this restriction would be useful for users that would like to allow information on certain social networks to be used for employment purposes while precluding employers from using information on some other social networks.

3.4 no-financial

Figure 3-4: The icon for the *no-financial* restriction

The fourth restriction is no-financial. The icon, shown in Figure 3-4, for the no-depiction restriction is a green dollar sign overlayed with the yellow circle and slash. In the informative page linked to each icon, the text for no-financial reads: “This restriction communicates that the user does not want his/her profile and associated with it used for financial purposes. For example, financial institutions do not have permission to use information from the user's profile to influence a loan, credit, or insurance decision.” This restriction allows a user to

declare that he does not want his profile used in the context of financial decisions. Insurance providers and banks often run background checks to ensure that their clients are worth offering coverage or capital to. Although there have not been any widely publicized cases of any organizations basing financial decisions on information from social networks, this is a problem that will forseeably occur in the future. This also presents a wide class of problems that could be especially important to social network users as unwanted consequences pertaining to financial decisions are probably the most important case of problems that users want to protect themselves from.

3.5 no-medical

Figure 3-5: The icon for the *no-medical* restriction

The final restriction is no-medical. The icon, shown in Figure 3-5, for the no-medical restriction is the red plus, the sign for first aid, overlayed with the yellow circle and slash. In the informative page linked to each icon, the text for no-depiction reads: “This restriction communicates that the user does not want his/her profile and anything associated with it used for medical purposes. For example, medical institutions do not have the user's permission to his/her information to influence a medical insurance decision or justify a medical condition.” This restriction allows users to declare that they do not want any information on their profile to

influence a decision pertaining to medical insurance or use it to make inferences about someone's medical status. Although the insurance aspect of the *no-medical* restriction overlaps part of the *no-financial* restriction, this restriction also allows users to declare that they do not want their personal information on a social network to be used to infer anyone's medical status. Social networks could be a place for groups of people that are afflicted or know someone afflicted with a certain disease to come together and offer support for each other. There could be a fear, however, that discussing one's medical matters could cause unwanted consequences if it were to be made public outside the bounds of the social network and its groups. This restriction will hopefully allow people to feel more comfortable using social networks as a positive vehicle for support during distressing times without fear of unwanted consequences.

3.6 The Respect My Privacy Icon

Using these five restrictions and their associated icons, the Respect My Privacy gives each user a simple and easily recognizable icon that can be posted on their profile page or other relevant pages on a social network. The background template for the Respect My Privacy icon is shown below in Figure 3-6.

Figure 3-6: The background template upon which the individual restriction icons are placed.

On this template, the icons for the restrictions that the users have chosen are placed. Some

example icons with different settings are shown below in Figure 3-7. The Respect My Privacy icon has a simple design that purposefully mimics the Creative Commons licenses to increase widespread traction. As with the Creative Commons licenses, these icons can be placed on a profile page and related pages to notify users of the restrictions that are placed on the user of data. In addition, they will similarly link to a page that gives extended information on each of the restriction that the user has selected.

Figure 3-7: Sample Respect My Privacy icons with one through all five restrictions

Chapter 4

Respect My Privacy on Facebook & OpenSocial

4.1 Introduction

The first two implementations of Respect My Privacy were on Facebook and OpenSocial. Facebook is one of the largest and fastest growing social networking sites on the Internet, with about 150,000 new users signing up daily and 2 billion page views per day[6]. Founded in 2004 by two Harvard undergraduates, Mark Zuckerberg and Dustin Moskovitz, it has quickly risen to become the fourth most visited site on the Internet[7], with more than 50 million unique users, and has recently been valued at $15 billion dollars based on a small percentage investment by Microsoft[8]. Facebook has been on the forefront of social networking sites, offering users the option to publish photo albums, post blogs, and develop and insert third-party applications into their profile pages. As one of the largest social networking sites, it is also one of the most controversial, and has one of the most complex and extensive access restriction

systems of all social networks. Given it's large size and the fact that it offered a fairly extensive set of application programming interfaces (APIs) with it's third-party application feature, Facebook was a natural first choice for implementing Respect My Privacy.

OpenSocial is a initiative spearheaded by Google and MySpace, another one of the largest social networks, to provide a common set of APIs that could be used to produce applications that would work across a wide variety of social networks[9]. It was released fairly recently, in November of 2007, but includes a large number of social networks that are popular throughout the world. MySpace, as mentioned, is probably the second most recognizable name in social networking behind Facebook. Other social networks, like Orkut, hi5, and Friendster, all have large userbases throughout the world, although not as popular in the United States. Since producing an application on OpenSocial is tantamount to producing an application across several different social networks, OpenSocial became the second mainstream “social network” on which to implement Respect My Privacy.

4.2 Respect My Privacy on Facebook

4.2.1 Creating Respect My Privacy settings

The Respect My Privacy application on Facebook is a MySQL/PHP driven web application that uses the Facebook Application API and is hosted on the Decentralized Information Group's server. In order to mimic the ease of use for Creative Commons, the creation of a Respect My Privacy setting is simple, taking mere minutes. When a user decides to add the Respect My Privacy application, they are directed to a page that explains the philosophy behind Respect My Privacy. This page is very important as Respect My Privacy on Facebook is

currently a project entirely dependent on its members. As more users create the Respect My Privacy 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. This page, and screenshots of all the important Facebook pages, is included in Appendix C. 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 the profile page so that everyone that visits a user's profile page can clearly see the restrictions that the user has placed on his personal information.

4.2.2 Description of Features

Once a user has created a set of Respect My Privacy restrictions, there are several features that become available to them. First, the user's Respect My Privacy 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 that visits the user's profile page will be able to view the Respect My Privacy icon. A typical Facebook profile page with the Respect My Privacy box is shown in Figure 4-1.

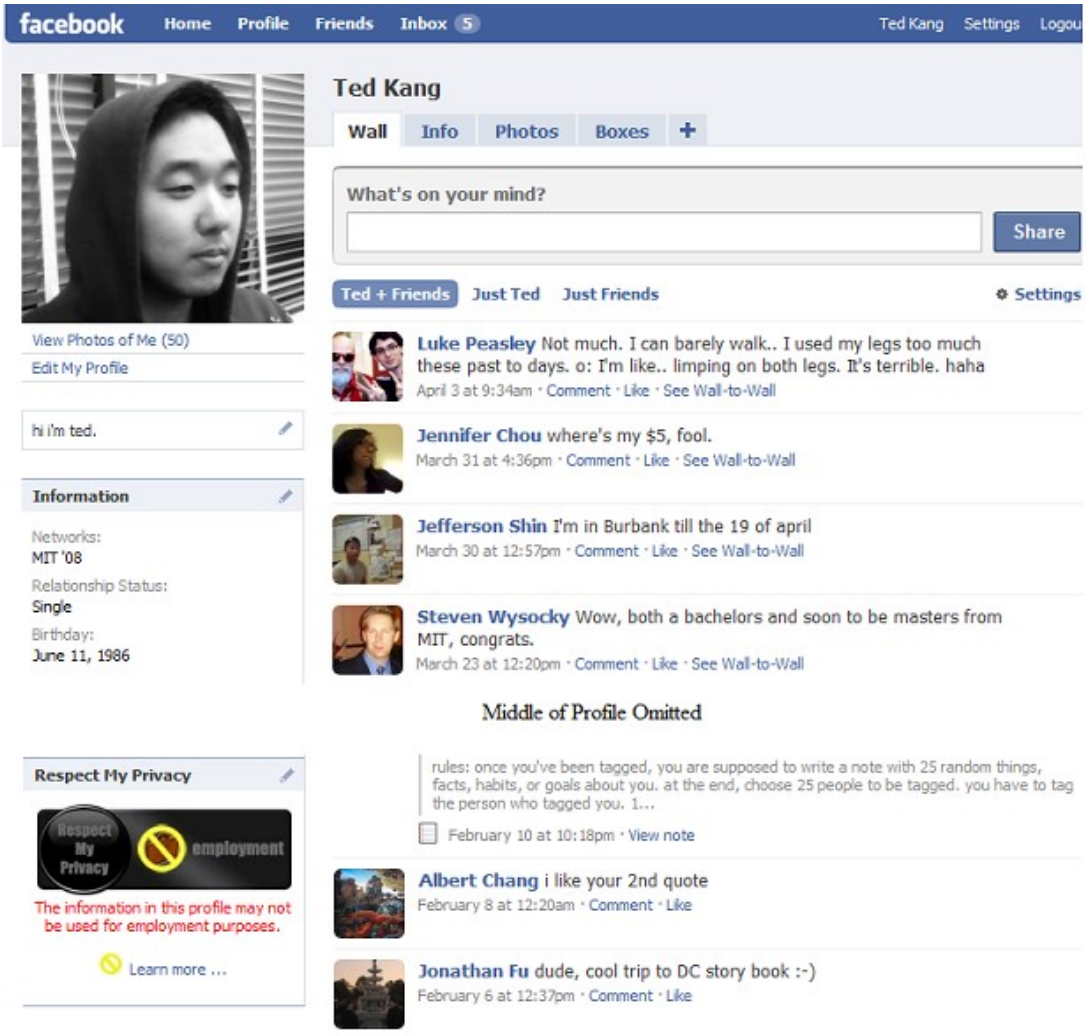


Figure 4-1. A Facebook profile page with the Respect My Privacy icon in the lower left corner

If any visitor clicks on the Respect My Privacy 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 Respect My Privacy movement on Facebook by creating their own set of licenses. A sample informative page that a visitor might see is who in Figure 4-2.

Figure 4-2: A sample informative page that users can reach by click on a Respect My Privacy icon. This user had only applied two of the five restrictions.

Hopefully, the similarity to the Creative Commons is obvious in the two figures above and will increase the adoption rate of Respect My Privacy in a manner similar to Creative Commons.

The user is also able to access the main page of the Respect My Privacy application. The main page contains a section for news where updates and new features are posted for

Respect My Privacy members. It also includes a section that displays the user's current settings with the appropriate icon. Directly below this is a list of current friends that are also members of Respect My Privacy with their corresponding Respect My Privacy icons.

From the main page, the user is able to access a page that allows them to edit their Respect My Privacy restrictions. This page is similar to the page used by the user to pick his initial set of restrictions but with his current restrictions checked. Once a user has edited their set of restrictions, a new Respect My Privacy icon is pushed to the profile page.

The user is also able to access a page that allows them to invite their friends to Respect My Privacy. This page makes it trivial to invite some or all of their friends to join the Respect My Privacy movement on Facebook. User can choose to invite all their friends, filter the list of friends by different social groups, or select the friends they want to choose individually.

Finally, users are able to port their Facebook profiles to Friend of a Friend (FOAF) files. FOAF is a machine-readable vocabulary for describing people in the Resource Description Format (RDF). FOAF and the motivations for this feature and will be discussed in subsequent sections and chapters; however, the FOAF converter takes data about the user from his profile page and stores it in a file using the FOAF vocabulary. The FOAF converter was originally developed by Matthew Rowe[10] and altered to include the Respect My Privacy restrictions that one has applied to one's profile page.

4.3 Respect My Privacy on OpenSocial

The Respect My Privacy 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. As more and more users become members of multiple social networks, it was important to make sure that the user experience is simple and similar across all implementations of Respect My Privacy in order to ensure that acceptance will not be discouraged by disparate features on different implementations. As such, all the features of Facebook are mimicked in the OpenSocial application.

4.4 Discussion

At the inception of the project, Facebook and OpenSocial were chosen as the first platforms for the Respect My Privacy project owing to their large base of members and the availability of extensive APIs for developer use. It became clear, however, that traditional social networks do not offer enough control over a user's personal data to become the platforms that Respect My Privacy would grow on. As the traditional social networks are all corporations aiming to produce a profit, there is little incentive on their part to make their user's data easily available and usable outside of the constrained space allotted to applications. In fact, there is a greater incentive to protecting user information from outside use that does not directly benefit it as a social network's most valuable capital is its users and their associated data. Facebook and OpenSocial, even with their extensive APIs, offer just enough of user's data so that developers can produce interesting applications but have strict restrictions on introducing any functionality outside the constraints of the predetermined set of pages given to third-party applications. For example, it is strictly prohibited to track any actions or visits to a user's profile page.

As can be seen in the current implementations of Respect My Privacy on Facebook and OpenSocial, there are no accountable systems that help people pinpoint misuses of their data.

A large reason for this is that the user's data belongs to whatever social network it is posted on and there was no way to access and track usage of that data given the constraints placed on developers by social networks. This presented problems for the future steps in the project, which include ways of attaching provenance information to a user's personal information and developing accountable systems that report misuse of private information based on that provenance information.

This led to the implementations of Respect My Privacy on Facebook and OpenSocial being used primarily as a way to increase the awareness of the set of Respect My Privacy restrictions. One of the key tenants of accountable systems is transparency, especially transparency of policy. With their large userbases, Facebook and OpenSocial offer great places to introduce users to the different restrictions, or policies, that are offered by the Respect My Privacy project. If the Respect My Privacy gains traction in Facebook and OpenSocial communities, we hope that a relative large set of Respect My Privacy users will adapt to other platforms for Respect My Privacy that offers greater control of one's data.

This new platform is the decentralized social network, which offers the greatest control of data, as each user has full control over his/her personal information. The FOAF converter feature on the Facebook and OpenSocial applications is meant to offer users easy ways of transitioning to members of these decentralized social networks. This will be discussed at length in Chapter 5.

Chapter 5

Respect My Privacy on a Decentralized Social Networking

5.1 Background

The main problem with the Facebook and OpenSocial implementations of Respect My Privacy was the constraints in place that prevented modification of or addendums to user data. This led to the third implementation of Respect My Privacy on a decentralized social network. As no established decentralized social network exists at the moment, we looked for a set of technologies that had the beginnings for the creation of a viable decentralized social network while still offering the functionality needed for future work on the Respect My Privacy project. Luckily, the work done on Tabulator and the Semantic Web by Tim Berners Lee of the Decentralized Information Group form a foundation for a decentralized social network and the set of Semantic Web technologies offered the perfect platform for future work on the project. As there are a variety of technologies used for the Tabulator project, I will introduce them briefly.

5.1.1 The Semantic Web

The Semantic Web is an extension of the World Wide Web that was proposed by Tim Berners Lee[11]. The World Wide Web currently contains primarily HTML documents that are able to link to each other and display other sort of data, but the data in an HTML document, for the most part, does not have any technical relation to data on another HTML document. There is no way for people to know that the "Ted Kang" who has a profile on Facebook is also the same "Ted Kang" listed on the MIT student directory without looking at both websites and inferring that enough information coincides on the two pages to conclude that they describe the same person. The Semantic Web wants to add to the current World Wide Web by introducing a set of technologies that can be used to describe nearly anything and using these descriptions to annotate content with machine-readable, semantic meaning to the text on an HTML page.

This descriptive language is called the Resource Description Format (RDF). It has a triple structure consisting of (subject, predicate, object), which can be thought of as an arc in a graph connecting the subject and object nodes with a predicate arc. Nodes can be universally identified using a unique URI. For example, one could construct a statement about a person such as (http://web.mit.edu/tkang/www/foaf.rdf, foaf:name, "Ted Kang"). In this statement "http://web.mit.edu/tkang/www/foaf.rdf" is a URI that represents the person, Ted Kang, online. The predicate, "foaf:name," is a relation defined in the foaf namespace that signifies that the object represents the name of the subject. The object is a literal, "Ted Kang," that represents the name of the subject URI. One can then build descriptions of people, or any arbitrary thing, by using sets of triples to describe a single subject. One can also build relationship between URI's with a statement like (http://web.mit.edu/tkang/www/foaf.rdf, foaf:knows,

http://people.csail.mit.edu/lkagal/foaf.rdf), which states that the person represented by the subject URI knows the person represented by the object URI. Using these triples, one can build a large semantic graph that can be traversed to learn about the relations among different URIs.

In the previous two examples, foaf, or Friend of a Friend[12], is an ontology, or vocabulary, defined at the URI, http://xmlns.com/foaf/spec/. It offers users a standard set of vocabulary to describe people. Similarly, one can produce one's own vocabulary, such as a vocabulary that talks about Respect My Privacy and its restrictions. With this vocabulary, we would be able to create triples that apply to certain pieces of data and signify that the data is protected by such restrictions.

The main advantage of RDF is that it is a machine-readable data model such that systems can be made to perform tasks that would normally require manual searching of the Internet. For example, systems are able to traverse a semantic graph to collect information not necessarily located at URI and discover more useful information about that URI. On the current Internet, this would require the use of search engines and manpower to compile and aggregate data that shared certain relationships.

Another important technology, not directly related to the Semantic Web, is N3 Logic[13]. N3 Logic is an extension of RDF that allows users to represent a wider variety of things, specifically rules. This is especially useful as N3 can be used to describe policies that determine appropriate or inappropriate use based on semantic data. Users would be able to configure servers to read in RDF descriptions, convert it to N3 Logic, then apply preconfigured policies to determine whether or not the RDF data has been correctly used.

5.1.2 The Tabulator

The Tabulator is a project led by Tim Berners Lee that aims to create a generic data browser and editor for RDF data, similar to how a web browser is used to navigate HTML pages[14]. The 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, the Tabulator offers an easy interface with which to view the RDF data. Furthermore, the Tabulator allows the user to request and retrieve further data about any URI's found in the RDF statements by simply click on URIs presented to the RDF triples. The Tabulator's browsing interface is shown below in Figure 5-1.

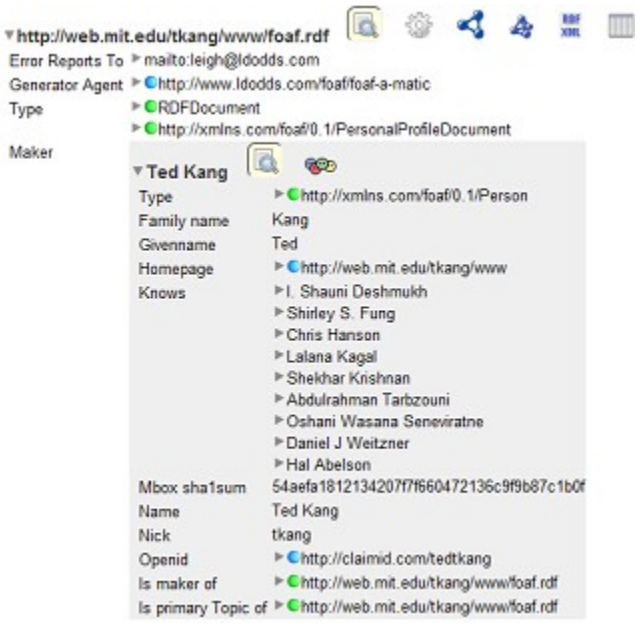


Figure 5-1: An example of the Tabulator browsing Semantic Information

Again, this is similar to how a web browser allows users to navigate hyperlinks to access different web pages. The tabulator offers many different panes for viewing the RDF data, but the

one relevant to Respect My Privacy is the FOAF pane. This pane appears when the Tabulator browses data that is of type "foaf:person", which means that the data describes a person using the FOAF ontology. This pane attempts to present data in a style similar to that of most social networks. A sample view of the FOAF pane is shown in Figure 502.

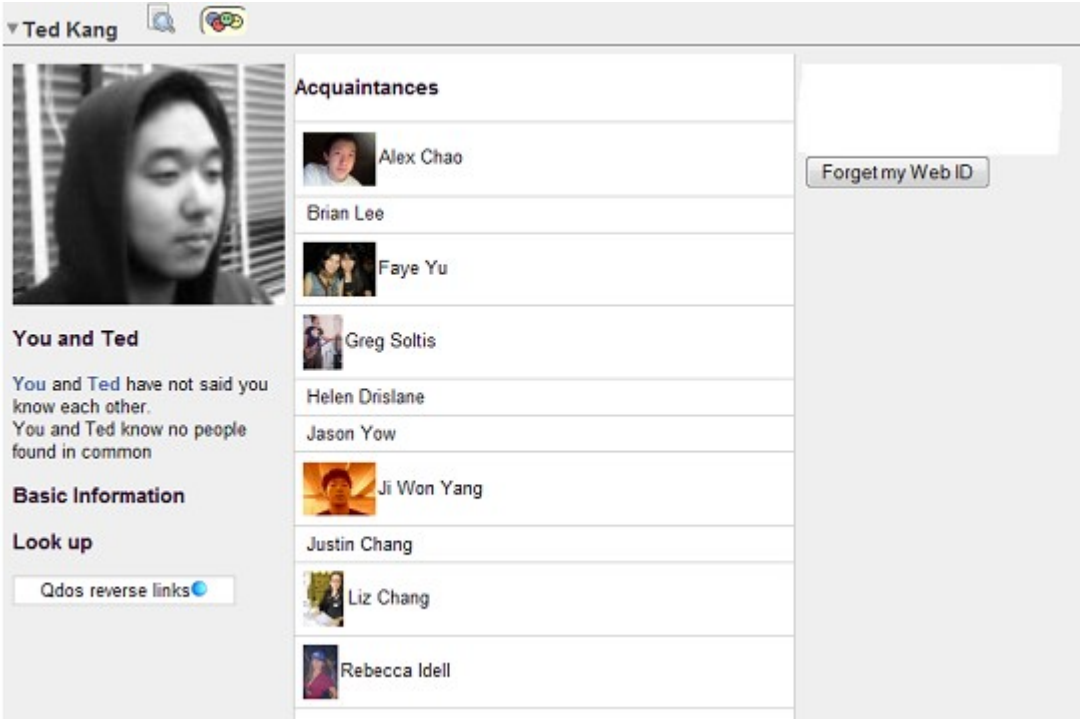


Figure 5-2 An example of the Tabulator's FOAF pane.

The FOAF pane also allows users to edit FOAF files that are stored on a WebDAV server using SPARQL updates[14].

Given the Tabulator's new social pane, the Tabulator can become the platform for a decentralized social network in which users host their own FOAF files and the Tabulator can be used to browse and edit the FOAF file, similar to how we browsers can be use to browse and edit social network like Facebook. The decentralized social network based on the Tabulator will be discussed at length in the next section.

5.2 The Decentralized Social Network on Tabulator

The Tabulator extension and it's FOAF pane is merely the first step in the creation of a decentralized social network. It offers users a way to clearly present and view FOAF files that are hosted in a decentralized manner. An advantage of a decentralized social network is that users can choose the mechanism that is used to present the underlying social data and the Tabulator is just one option; however, we will assume that the Tabulator extension is the default presentation mechanism when discussing our decentralized social network. "Decentralization: The Future of Online Social Networking,"[15] described how a decentralized social network could actually be implemented using Tabulator as a framework. We can imagine a decentralized social network being organized as follows. A user would choose a trusted server on which to host his FOAF file. The user could choose a server that is operated by a third-party and offers a preconfigured server operation or the user could host the FOAF file on his own server, which would give him full control over his data.

The servers that are hosting the FOAF files can be configured to implement any access restriction mechanism that the user wanted to implement. For example, the Decentralized Information Group's blog uses an access restriction mechanism for comments in which commenters must first authenticate with the server using an OpenID and associated FOAF file. The server which the blog is hosted on then only allows users to post comments if they are within a certain degree of separation from any of the members in the Decentralized Information Group. This is done by traversing through all the registered FOAF files for members of the Decentralized Information Group and traversing the objects of foaf:knows predicates, a FOAF predicate that is similar to acknowledging a friend on a social network, to create a whitelist. It

would be possible to configure similar access restriction mechanisms for viewing FOAF files using simple N3 rules. As implementing these server configurations are not trivial, one can expect organizations that offer hosting services for FOAF files to also offer a set of preconfigured access restriction policies that the less computer-savvy users could choose from. In addition, users could register their FOAF files to trackers, similar to trackers that assist in the connection of BitTorrent users, in order to assist in the creation of organized, yet decentralized, social networks.

Editing data on a decentralized social network would also be possible through the use of SPARQL, a query language similar to SQL that was created for querying and editing RDF data. Server could be configured to allow users to authenticate with an OpenID, then give them the ability to edit their FOAF profiles through interfaces like the Tabulator extension. SPARQL queries can also be used to implement the more "interactive" features of social networks. Most social networks allow users to leave comments or write messages on other user's profile pages, which allows users to easily communicate with each other in short blurbs. This kind of service could be implemented in a decentralized social network by allowing users that satisfy a certain policy to edit a special section of the FOAF file that corresponds to the wall. The Tabulator, or any other framework for displaying FOAF file, can then display this information in a unique way to make the functionality obvious to users.

The Respect My Privacy project would be able to implement accountable systems on a decentralized social network. Users could be allowed to create Respect My Privacy restrictions and apply them to their FOAF files using the Tabulator extension. In addition, servers could implement ways of attaching provenance information through SPARQL updates to the FOAF

file. This provenance information can be used by servers to collect information about the origins of a piece of data, and ensure that policies were followed during the use of that data.

5.3 Respect My Privacy on Tabulator

As no decentralized social network has been implemented yet, the current Respect My Privacy implementation on Tabulator is focused on implementing the Respect My Privacy restrictions on the RDF data model, trying to build a larger userbase of FOAF users that utilize the RDF Respect My Privacy restrictions, and additions to the Tabulator that allow the user to easily view and edit the Respect My Privacy restrictions on a FOAF profile. The first step involves creating an ontology for the Respect My Privacy restrictions so that RDF statements would have a vocabulary with which to speak of Respect My Privacy restrictions. The ontology for the Respect My Privacy restrictions are included in Appendix A, in RDF, and in Appendix B, in N3. They define an "rmp" namespace and define the notion of a restriction along with the five restrictions currently implemented in Respect My Privacy. In addition, the ontology defines a predicate, rmp:restricts, which can be applied to FOAF documents with the specific restriction serving as an object. For example, to add a restriction to the FOAF file that represents me, I would add the triple (http://web.mit.edu/tkang/www/foaf.rdf, rmp:restricts, rmp:no-employment) to my FOAF file.

In order to build a larger userbase that have FOAF files with Respect My Privacy restrictions, we use the FOAF generator from the Respect My Privacy Facebook and OpenSocial applications. The FOAF generator pulls user data, including the list of friends, and creates a copy of the Facebook or OpenSocial profile using the FOAF vocabulary. It also includes the Respect My Privacy restrictions that the user has chosen into the FOAF file and hosts in on the

DiG server. This allows users of Facebook and OpenSocial to easily create and host FOAF files that already have their Respect My Privacy restrictions applied. They can then use the Tabulator to browse their FOAF files in a manner similar to browsing a social networking like Facebook.

Finally, the current implementation of Respect My Privacy on Tabulator has extra additions that assist in viewing and editing the Respect My Privacy restrictions on a FOAF page. First, a license/restriction highlighting sidebar was created that aggregates Creative Commons licenses and Respect My Privacy restrictions as the user browses data protected by those restrictions or licenses. The sidebar allows users to choose colors for the gathered licenses and restrictions, and highlights any data protected by a license or restriction with the appropriate color. This ensures that as users are using the Tabulator extension to browse semantic information, they will be able to easily recognize what limitations there are on the use of any new data that has been displayed. In addition, if a user is using the social pane to view FOAF files and Respect My Privacy licenses are located on a page, a Respect My Privacy icon is placed on the social pane and linked to an informative page giving extended details on the restrictions applied. This gives a similar user experience for users browsing a decentralized social network with the Tabulator extension as those browsing Facebook with the Respect My Privacy application installed. Figure 5-3 below displays the Tabulator extension and accompanying highlighting sidebar, which has recognized that it has browsed upon data protected by a Creative Commons license. As can be seen, the tripes protected by the Creative Commons license are highlighted with the chosen color.

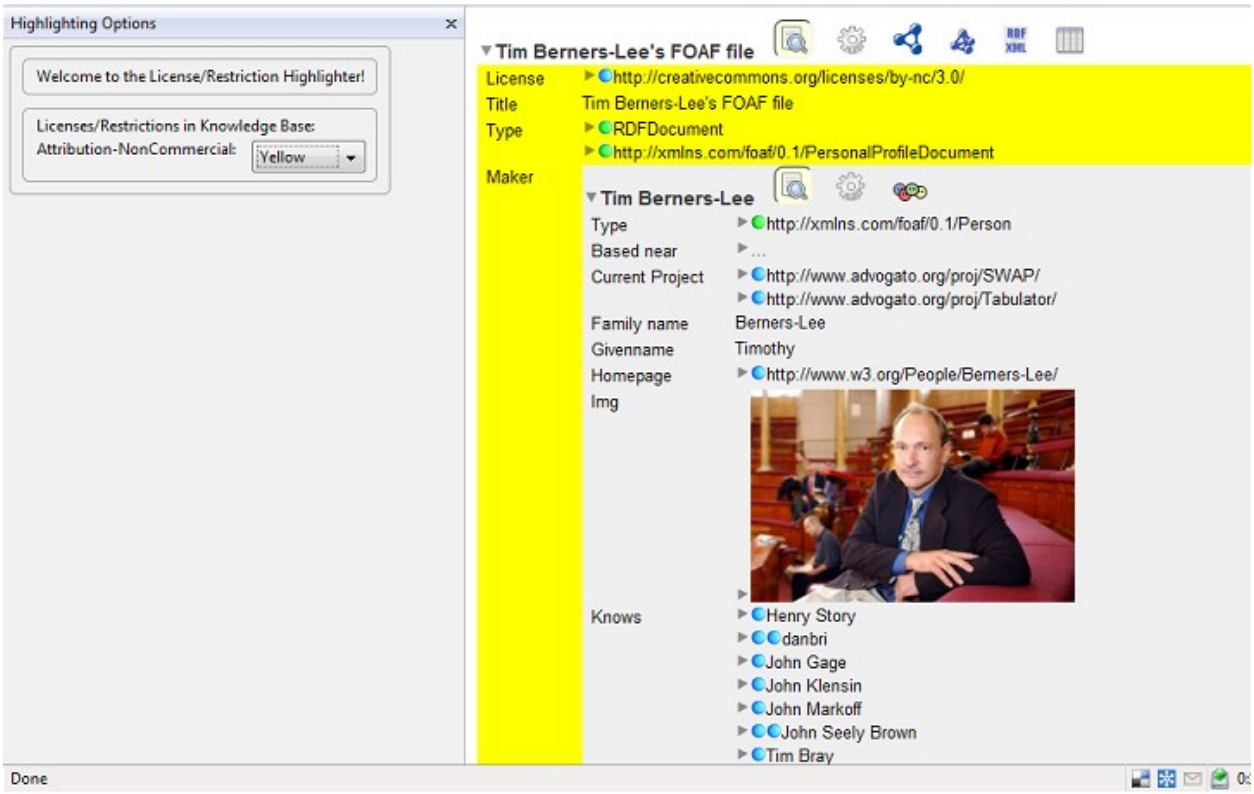


Figure 5-3: The CC/RMP highlight sidebar recognizes the Creative Commons license on the FOAF file and allows the user to choose a color with which to highlight the data protected by the license.

The Tabulator also allows users to declare that certain FOAF file represents them online, or associate their identity with a FOAF file. When this is done, the users have the option to use SPARQL updates to alter their FOAF files as long as the FOAF files are hosted on a WebDAV server. Respect My Privacy on the Tabulator has also added extensions to make it easy for users to create or alter Respect My Privacy protections for their FOAF files directly through the Tabulator. Figure 5-4 below displays a sample FOAF page and the simple interface that users can choose to create or edit their Respect My Privacy settings via a SPARQL query.

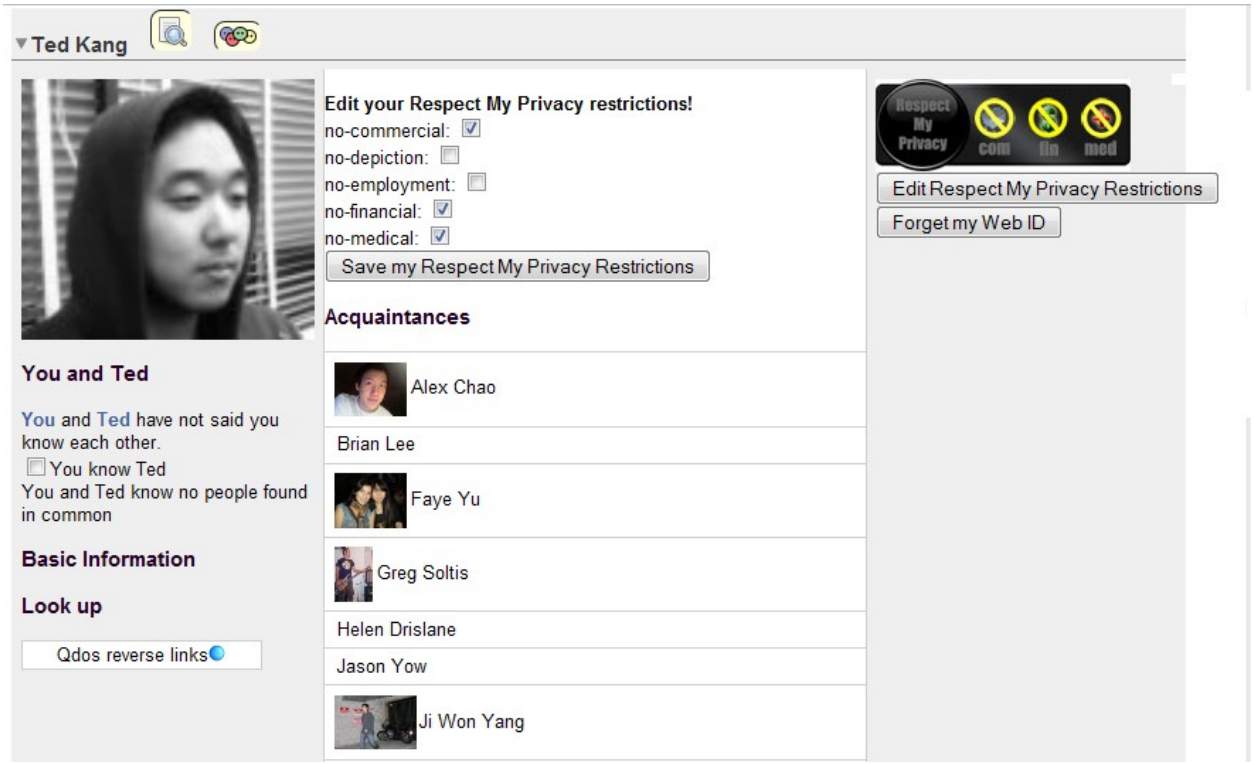


Figure 5-4: Users are able to create or edit the Respect My Privacy restrictions for their FOAF files directly through the Tabulator.

Thus, Respect My Privacy on decentralized social networks use FOAF files as the data back end with the advantage that these files are machine-readable and systems can be built to implement complex policies depending on the contents of these files. The Tabulator is used as a platform for browsing this decentralized network of FOAF files and allows users to clearly view and edit the Respect My Privacy restrictions placed on the FOAF files. In addition, the decentralized social network offers a set of technologies that make it easier to implementing mechanisms that enforce accountable use.

Chapter 6

Conclusion

6.1 Future Work

The Respect My Privacy project still has several areas that require significant work. As discussed in the introduction, an accountable system requires both transparency and mechanisms for appropriate use. The current implementations of Respect My Privacy reside on Facebook, OpenSocial, and the Tabulator extension require significant improvements before a fully functional accountable system can be implemented for privacy in social networks.

6.1.1 Facebook and OpenSocial

The Respect My Privacy implementations of Facebook and OpenSocial both suffer from lack of control over one's own data. Unfortunately, this problem can't be solved without direct assistance from Facebook and OpenSocial itself and it does not seem like there are currently enough of an incentive for the larger social networks to open up their data. Facebook and OpenSocial, however, still offer large userbases with which to recruit users to decentralized social networks. Therefore, future work involves further increasing awareness of the Respect

My Privacy project and attempting to show cases for its usefulness in order to tempt more users to a more decentralized social network. Once the Respect My Privacy restrictions have gained wide enough traction in the social network communities, legal policies will need to be put in place to hold accountable those who maliciously go against the policies governing data usage. Legal backing to these restrictions would give mainstream social networks more incentive to adopt information accountability practices. It would also give users some sort of recourse against misuse of their data and give incentive for the creation of social norms where users protect each other from misuse of data, and assist each other in reporting data misuse.

Ultimately, an accountable system cannot be implemented on mainstream social networks without assistance from the social network itself. One method of gaining more attention from a social network like Facebook could be by working with other large organizations that have similar goals. The Creative Commons recently released a Facebook application that allows users to place blanket Creative Commons licenses on a user's photos, videos, and status updates[16]. It works similarly to the Respect My Privacy application, allowing a user to choose a Creative Commons license and display it on his profile page with a link to more information. Working in unison with a non-profit organization like the Creative Commons to attempt to spread Respect My Privacy restrictions, which hopefully offer restrictions more customized for social networks, could be in the benefit of both projects. In addition, working with a well established organization like the Creative Commons could help draw attention from Facebook, and could help in eventually integrating accountable systems into the privacy protection mechanisms of mainstream social networks.

6.1.2 The Tabulator Extension

The Tabulator extension offers more tangible goals. First, there is the project of creating a decentralized social network. All the technologies required to create a product similar to centralized social networks are present, but no one has yet combined them to create a fully functional decentralized social network. Once a decentralized social network is in place, the Respect My Privacy project has room to grow. One large area of growth is in ways of attaching provenance information to data. This is vital for producing systems that are able to scan through a data's history and ensuring that the policies governing that piece of data have been followed at each step of its use.

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 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.

6.2 Final Thoughts

The efforts of social networks in protecting privacy could be greatly improved with the adoption of information accountability techniques. One of the tenets of accountable systems is transparency in policy, and the Respect My Privacy project currently offers users a clear and simple way to define the restrictions they want to place on their data. In addition, the current Respect My Privacy implementations employ the model used by the Creative Commons to try to gain widespread acceptance of the defined restrictions. This will hopefully lead to legal mechanisms to protect users from malicious misuse of their personal information and encourage adoption of a set of social norms online, which depend on people responsibly helping each other protect their privacy. Finally the Respect My Privacy project's new direction in decentralized social networks offers a foundation upon which to build a fully accountable system for social networks.

Appendix A

Respect My Privacy Schema in RDF

The following is the Respect My Privacy ontology represented in RDF:

```
<!-- The Respect My Privacy Vocabulary Definition -->
<!-- This vocabulary will hopefully be eventually merged into the FOAF ontology. -->
<!-- For now, users can reference the vocabulary in their FOAF files by including: -->
<!--                    <rmp:restricts>no-commercial</rmp:restricts>                    --
>
<!--                    <rmp:restricts>no-employment</rmp:restricts>  ... -->
<!-- author: tkang -->


<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:owl="http://www.w3.org/2002/07/owl#"
        xmlns:vs="http://www.w3.org/2003/06/sw-vocab-status/ns#"
        xmlns:foaf="http://xmlns.com/foaf/0.1/"
        xmlns:wot="http://xmlns.com/wot/0.1/"
        xmlns:dc="http://purl.org/dc/elements/1.1/"
        xmlns:cc="http://web.resource.org/cc/"
        xmlns:rmp="http://recp.scripts.mit.edu/rmp/rmp-schema#">
```

```
  <rdfs:Class rdf:about="http://recp.scripts.mit.edu/rmp/rmp-schema#Restriction"
rdfs:label="Restriction" rdfs:comment="A restriction." >
    <rdf:type rdf:resource="http://www.w3.org/2002/07/owl#Class"/>
    <rdfs:subClassOf><owl:Class
rdf:about="http://web.resource.org/cc/#license"/></rdfs:subClassOf>
  </rdfs:Class>

  <!-- The no-commercial restriction states that the owner of this profile does not want the
information on this profile used for commercial purposes. -->

  <rdfs:Class rdf:about="http://recp.scripts.mit.edu/rmp/rmp-schema#no-commercial"
rdfs:label="no-commercial" 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.">
    <rdf:type rdf:resource="http://www.w3.org/2002/07/owl#Class"/>
    <rdfs:subClassOf><owl:Class rdf:about="http://recp.scripts.mit.edu/rmp/rmp-
schema#Restriction"/></rdfs:subClassOf>
  </rdfs:Class>

  <!-- The no-depiction restriction states that the owner of this profile does not want this profile
associated with any pictures. -->

  <rdfs:Class rdf:about="http://recp.scripts.mit.edu/rmp/rmp-schema#no-depiction"
rdfs:label="no-depiction" rdfs:comment="The no-depiction restriction states that the owner of
this profile does not want this profile associated with any pictures.">
    <rdf:type rdf:resource="http://www.w3.org/2002/07/owl#Class"/>
    <rdfs:subClassOf><owl:Class rdf:about="http://recp.scripts.mit.edu/rmp/rmp-
schema#Restriction"/></rdfs:subClassOf>
  </rdfs:Class>

  <!-- The no-employment restriction states that the owner of this profile does not want the
information on this profile used for employment purposes. -->

    <rdfs:Class rdf:about="http://recp.scripts.mit.edu/rmp/rmp-schema#no-employment"
rdfs:label="no-employment" 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.">
      <rdf:type rdf:resource="http://www.w3.org/2002/07/owl#Class"/>
      <rdfs:subClassOf><owl:Class rdf:about="http://recp.scripts.mit.edu/rmp/rmp-
schema#Restriction"/></rdfs:subClassOf>
  </rdfs:Class>

  <!-- The no-financial restriction states that the owner of this profile does not want the
information on this profile used for financial decisions. -->
```

```
  <rdfs:Class rdf:about="http://recp.scripts.mit.edu/rmp/rmp-schema#no-financial"
rdfs:label="no-financial" 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.">
    <rdf:type rdf:resource="http://www.w3.org/2002/07/owl#Class"/>
    <rdfs:subClassOf><owl:Class rdf:about="http://recp.scripts.mit.edu/rmp/rmp-
schema#Restriction"/></rdfs:subClassOf>
  </rdfs:Class>

  <!-- 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:Class rdf:about="http://recp.scripts.mit.edu/rmp/rmp-schema#no-medical"
rdfs:label="no-medical" 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.">
    <rdf:type rdf:resource="http://www.w3.org/2002/07/owl#Class"/>
    <rdfs:subClassOf><owl:Class rdf:about="http://recp.scripts.mit.edu/rmp/rmp-
schema#Restriction"/></rdfs:subClassOf>
  </rdfs:Class>

  <rdf:Property rdf:about="http://recp.scripts.mit.edu/rmp#restricts" rdfs:label="restricts"
rdfs:comment="Applies a single restriction on a FOAF file.">
    <rdf:type rdf:resource="http://www.w3.org/2002/07/owl#ObjectProperty"/>
    <rdfs:domain rdf:resource="http://xmlns.com/foaf/0.1/Person"/>
    <rdfs:range rdf:resource="http://recp.scripts.mit.edu/rmp#Restriction"/>
  </rdf:Property>


</rdf:RDF>
```

Appendix B

Respect My Privacy Schema in N3

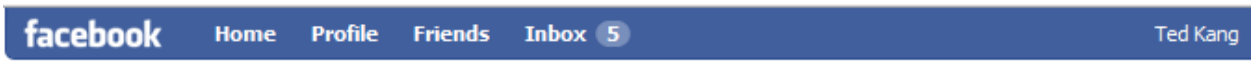
The following is the Respect My Privacy schema writte in Notation3:

```
# The Respect My Privacy Vocabulary Definition
# http://recp.scripts.mit.edu/rmp/rmp-schema.rdf in RDF/N3

# author: tkang@mit.edu

@prefix rdf:  <http://www.w3.org/1999/02/22-rdf-syntax-ns#> .
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#>.
@prefix cc: <http://web.resource.org/cc/>.
@prefix owl: <http://www.w3.org/2002/07/owl#>
@prefix vs: <http://www.w3.org/2003/06/sw-vocab-status/ns#>
@prefix foaf: <http://xmlns.com/foaf/0.1/>
@prefix wot: <http://xmlns.com/wot/0.1/>
@prefix dc: <http://purl.org/dc/elements/1.1/>
@prefix rmp: <http://recp.scripts.mit.edu/rmp/rmp-schema#>


rmp:Restriction a rdfs:Class;
                rdfs:subClassOf cc:license;
                rdfs:comment "A restriction";
                rdfs:label "license."
```

```
no-commercial rdfs:subClassOf rmp: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 rdfs:subClassOf rmp: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 rdfs:subClassOf rmp: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 rdfs:subClassOf rmp: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 rdfs:subClassOf rmp: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".

rmp:restricts a rdfs:Property;
        rdfs:comment "Applies a single restriction on a FOAF file.";
        rdfs:label "restricts";
        rdfs:domain foaf:Person;
        rdfs:range rmp:Restriction.
```

Appendix C

Facebook Application Screenshots



Most social networks offer you ways to protect your privacy; however, they all focus on keeping unwanted users out. This strategy, of building a large fence around the data you want protected, is called access control. Social networks, generally, do a good job of offering you access control and you should take advantage of it! But, like most things, access control systems are not perfect. There's always a chance that someone is going to get unwanted access, and current privacy controls are powerless once that happens.

Respect My Privacy employs a different approach, called Information Accountability, to protecting your personal information online. Instead of trying to protect your personal information from unwanted access (there's already systems for that), we focus on giving you efficient and clear ways to communicate how you want your data handled. In the case that someone, accidentally or purposefully, gains access to private information, there is at least a clear indication of how you expect your private information to be handled.

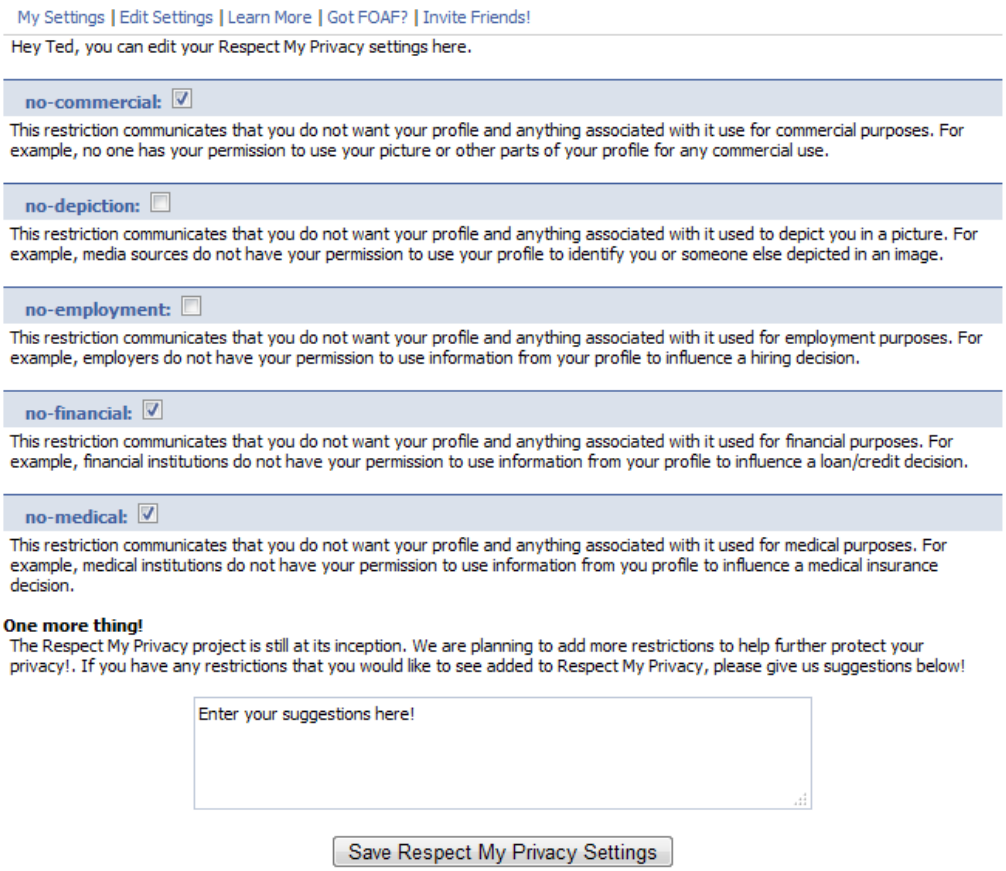
We have created a set of simple restrictions that communicates how you want your personal information to be used. These tags aren't going to magically stop anybody from using your information, it is merely a vocabulary for communicating how you want your data to be used. This is, however, an important first step in that we can now at least talk about the expectations we have on our data.

In the future, we hope to be able to allow you to display your Respect My Privacy settings across a variety of different social networks. With a well-adopted set of vocabulary to talk about how we want our data protected, we can then add legal backing to the protections we want voiced.

Time to create your settings!

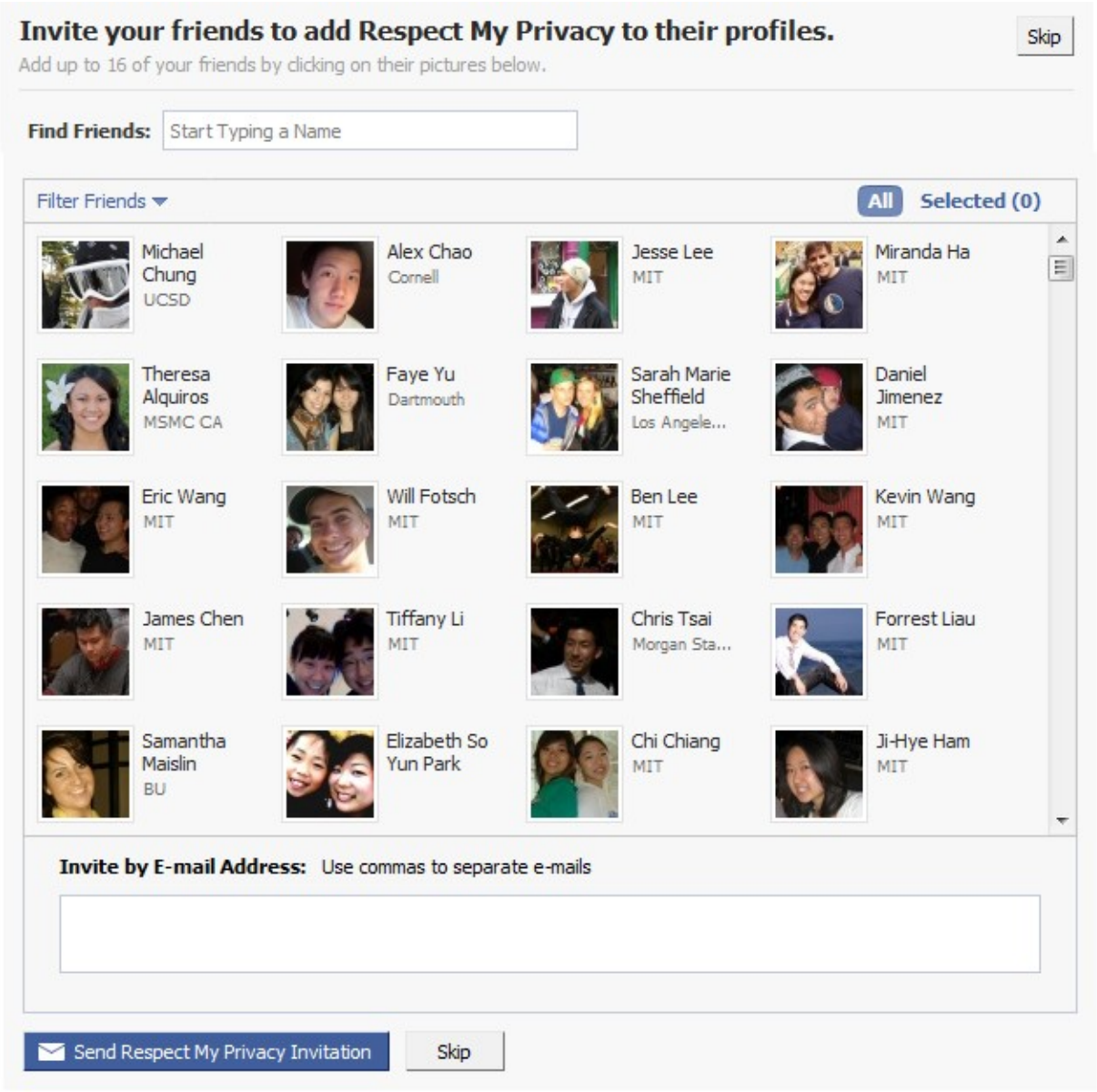
This is the page that is shown to users when they decide to install the Respect My Privacy application on Facebook. This page is important as the current implementation on Facebook relies on social pressure to try to make users appropriately use data.

This is the main page of the Respect My Privacy application. Users are directed to this page when they click on the Respect My Privacy application. The left side of the page contains a news feed that announces updates to the Facebook application. The right side of the page displays the user's current restrictions and the restrictions of all the user's friends that are also members of Respect My Privacy.



This is the "Edit Settings" page of the Respect My Privacy application. This allows users to change the restrictions applied to their data, and also suggest new features for the application. When a user saves his new settings, the appropriate Respect My Privacy icon is pushed onto his profile page.

This is the "Got FOAF?" page of the Respect My Privacy application. When the user visits this page, the FOAF exporter converts the user's Facebook profile page into a FOAF file. It then hosts it on the DiG server and provides a link to FOAF file to the user.



This page allows users to invite their friends to add the Respect My Privacy application. Users can invite all their friends or select those that they want to invite.

Bibliography

[1] Facebook <http://www.facebook.com/home.php#/facebook?ref=pf> (May 1, 2009)

[2] Weitzner, Daniel et al. "Information Accountability" MIT Computer Science and Artificial Intelligence Laboratory Technical Report. 13 June 2007. MIT-CSAIL-TR-2007-034.

[3] "About – Creative Commons" <http://creativecommons.org/about/> (May 1, 2009)

[4] "Reciprocal Privacy (ReP) for the Social Web" <http://dig.csail.mit.edu/2007/12/rep.html> 12 Dec 2007. (May 1, 2009)

[5] Harris Interactive Inc. *Privacy Notices Research Final Results.* Privacy Leadership Initiative (PLI). (2001)

[6] Laura Locke. "The Future of Facebook" *TIME* <http://www.time.com/time/business/article/0,8599,1644040,00.html> (Nov 16, 2007)

[7] Alexa Web Search. <http://www.alexa.com/site/ds/top_sites?cc=US&ts_mode=country&lang=none> (Nov 14, 2007)

[8] Erick Schonfeld. "Facebook Takes the Microsoft Money and Runs." TechCrunch < http://www.techcrunch.com/2007/10/24/facebook-takes-the-microsoft-money-and-runs/> (Nov 16, 2007)

[9] "OpenSocial – Google Code" <http://code.google.com/apis/opensocial/> (May 1, 2009)

[10] Rowe, Matthew. "FOAF Generator" <http://www.dcs.shef.ac.uk/~mrowe/foafgenerator.html> (May 1, 2009)

[11] Berners-Lee, Tim. "Semantic Web roadmap" <http://www.w3.org/DesignIssues/Semantic.html> (May 1, 2009)

[12] FOAF Vocabulary Specification - <http://xmlns.com/foaf/spec/> 2007

[13] Berners-Lee, Tim. "Notation 3 (N3) A readable RDF Syntax". <http://www.w3.org/DesignIssues/Notation3.html>, 1998

[14] "The Tabulator Extension". <http://dig.csail.mit.edu/2007/tab/ > (May 1, 2009)

[15] Ching-man Au Yeung, Ilaria Liccardi, Kanghao Lu, Oshani Senevirante, Tim Berners-Lee. "MSNWN Position Paper". <http://dig.csail.mit.edu/2008/Papers/MSNWS/> 2008.

[16] Frederic Lardinois. "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 > (May 21, 2009)