Privacy Awareness: Icons and Expression for Social Networks

Renato Iannella[1] and Adam Finden[2]

[1] Semantic Identity
ri@semanticidentity.com
[2] Stacked Creations
adam@stackedcreations.com

Keywords: Privacy, ODRL, Semantics, Social Networks

1 Introduction

Much has been written about privacy on social applications (aka social networks). Popular social applications, such as FaceBook and MySpace, have brought the spotlight onto this often polarising issue. As social networks deal with the growing demand to support portable profiles [1] - that allow the user to easily move between social networks - they grapple with finding business models that can monetize their efforts.

Most privacy interactions on social networks are through dialog windows with multiple selections on offer and pulldown menus for selecting specific criteria. Very little thought is paid to any form of graphical representation for the privacy options.

In this paper we discuss and review some early research on designing and testing graphical icons to represent common privacy concepts. The icons are evaluated in a series of experiments to better understand the users interpretation of these graphical images.

Finally, to support interoperability across social networks, will review and propose extensions to the ODRL policy language to match the new graphical icons. The combination of a user- and compatible machine-view for privacy concepts should further the move towards open interoperable social networks.

2 Background and Related Work

The phenomena of Social Networks has put the media spotlight on Privacy as new and existing web companies drive to gain the attention of the global web community. From Facebook [2] to the more recent Google Buzz [3], Privacy has polarised the community as they try to meet the balance of user acceptability. This trend is not unique to the Social Web, with eHealth records [4] gaining just as much media attention.

The common new approach is to give the user-control of their identity [5] and hence, greater control over their own privacy as there is now “strong evidence

that the social networking market is failing to provide users with adequate privacy control" [6]. Many report on how users are "confused by the existing and extensive privacy settings" [7] and how "unconcerned users appear to privacy risks" on social networks [8]. There is unease that Social Networks were not defaulting to the highest privacy levels [9] and that directly related to the key goal of privacy; to "protect from harm" [10].

Taking a step back, it is important to review and define what we exactly mean by privacy in this context. There have been many definitions over the years and more recently; "Privacy...means the right to self-determination regarding data disclosure...each user should be able to control how much personal information he is willing to give to whom and for what purpose" [11].

Applying this to new technology, such as Social Networks, produces a "high degree of ambiguity over appropriate norms of conduct" as users and providers have a potential conflict of interest in the way the technology is used [12]. Designing privacy-preserving systems relevant to social media is "quite a challenging goal and it still deserves a significant research effort in the years to come" [13] and although potentially achievable through opt-in/opt-out systems, "a more careful consideration of the problem involves flexible privacy policy specification and...access control" [14].

Technical approaches to privacy in Social Networks have varied greatly with disparate results for the end user. These range from crypto-based solutions [15], game-theory techniques [16], role-based mechanisms [17], obfuscation and deniability [18], faked information [19], mobility and geographic locality [20] and social attestations [21]. Some novel techniques propose an auditing approach [22, 23] to allow the owner to track use of their personal data, and others base the privacy on how intensive interactions are between users [24], and the use of peer-to-peer networks for trusted privacy [25].

Expressing privacy via machine-readable languages began with the W3C P3P specification [26] but has not been widely adopted and is now relatively obsolete. Attempts have been made to extend the XACML access control language to support privacy [27], new languages have been proposed [28], and even the use of natural language to capture policies for social platforms [29].

The use of Semantic Web representations (ie RDF/OWL) in privacy languages has been minimal with a number of proposals, but very little, if any deployment by industry. A review of a number of these semantic privacy languages [30] has found them unclear and lacking in a number of key areas. We have looked at this issue and have proposed extending the ODRL permission-based language to support social privacy policies [31] and we continue that work in this paper. The motivation for extending ODRL is that this language is already widely deployed in the mobile sector for DRM applications.

Awareness through graphical icons offers a challenging way to map the terms of an machine-readable privacy expression into something that could be useful for end users by hiding the complexity of the (typically verbose) language. Without this visibility and awareness, web users could make decisions that are not consistent with their expectations [32].

Simple user interface constructs like a locked padlock and colour shading (eg red for no access, yellow for semi-public, and green for open access [33]) can help to indicate to the end user the potential audience of the information. Use of the "watching eye" that was graded from fully open to closed [34] was another general privacy indicator, as well as a "green happy face" and a "red conflict face" [35] to show the privacy status. Another icon used is that of the "Privacy Bird" [36] that used fixed images to indicate the privacy matching to a user's preferences. A "happy green bird" matched, a "confused yellow bird" indicated no policy found, and a "angry red bird" indicated a mis-match in polices.

Some icons representing the specific privacy restrictions for social networks were also developed [37]; non-commercial use (circle-backslash symbol over a shopping cart), no false depiction (circle-backslash symbol over a camera), no use for employment (circle-backslash symbol over a brief case), no use for financial purposes (circle-backslash symbol over a dollar sign), and no use for medical purposes (circle-backslash symbol over a red cross). These icons are indicative of the said purposes, but do pose legal issues, for example, as to if a person can state that what they posted on a social network site (eg derogatory remarks) cannot be used by their employer to terminate their contract.

Our earlier work [40, 41] on supporting Policies in the new Web 2.0 world categorised the next phases as:

- Policy Expression
- Policy Transparency
- Policy Conflict
- PolicyAccountability

With better representations and clearer semantics - both at the user interface and machine levels - we can start to address Policy Expression and Transparency for privacy.

3 The Privacy Icons Experiments

We reviewed common terms/concepts used in popular Social Networks for allowing the user to express privacy settings [38]. The most common set were focussed on allowing access to certain groups of people and included:

- Everyone
- Only Friends
- Some Friends
- All my Networks/Groups
- Some of my Networks/Groups
- Friends of Friends

Additionally, the default setting of "no access" was common.

An initial set of icons were developed (see Figure 1) that represented these concepts but varied by using different combinations of ticks, crosses, open and

closed padlocks, and colours across the same icon. We used the same representation of a person in each icon, with the rounded box representing a "group" and many people together (directly) to be "friends". The biggest challenge was an icon for "friends of friends" and we decided to offset the group of friends behind the user.

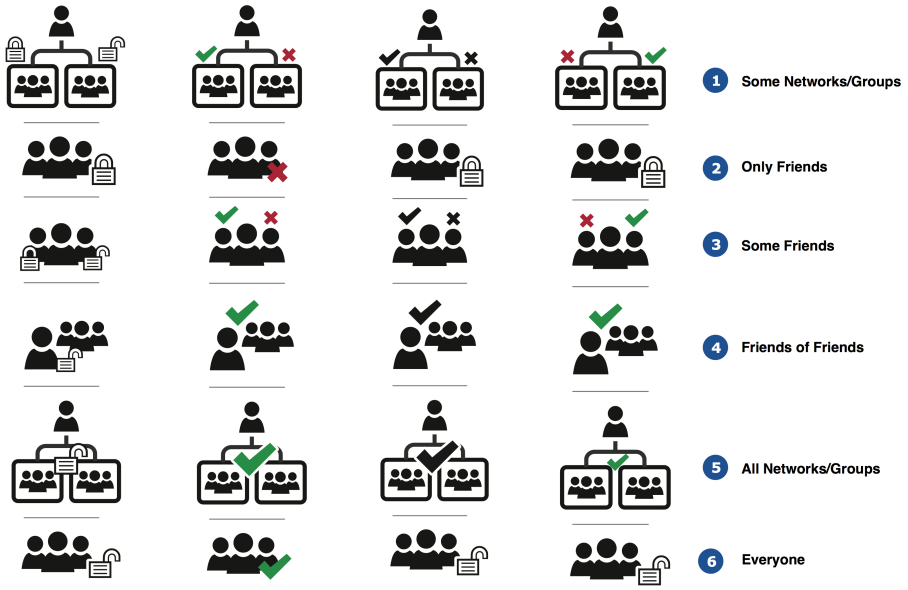

Fig. 1. Ticks V Crosses V Padlocks V Colours

We decided to use the icon set on the far right of Figure 1 for the first experiment. It used both ticks and padlocks and we wanted to see what, if any, preference the user had. We showed the icons to nine staff at our lab with a separate list of the six concepts and asked them to map between them. We also added a 7th "control" question to ensure they did not just map 6 icons to 6 concepts. This was called the "Some Friends and Networks/Groups" concept which mixed the two "Some Friends" and "Some Networks" concepts. It also helped us to see is there are some misconceptions with the other icons.

The results of the first experiment are shown in Table 1 (in the Appendix). There was reasonable agreement for Icons 2, 3, 5, 6, less with Icon 1 (Some Networks/Groups), and confusion with Icon 4. We thought that Icon 4 (Friends of Friends) would be the hardest to graphically represent, and the results confirmed this.

In the second experiment, we also decided to simplify the icons for the Networks/Groups and consistently use coloured ticks and crosses. We also added a "No Access" icon. The new set of icons is shown in Figure 2 and we used

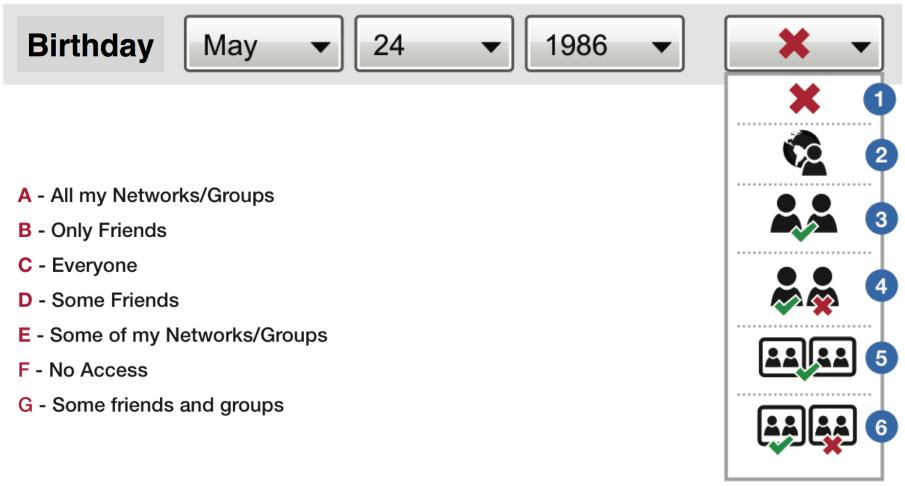

Fig. 2. Experiment 2 Icon Scenario

a scenario of specifying the privacy control over your birthdate (to give more context) with the users asked to link the concept letter with the icon number.

The results are shown in Table 2 (in the Appendix) and was undertaken with 18 final year high school students (an enthusiastic social network user demographic). The results were mixed, with only Icon 1 (No Access) having unanimous support. Icon 6 (Some Networks/Groups) had the most varied responses, followed by Icon 4 (Some Friends) and Icon 3 (All Friends). However, the majority of the survey respondents did get the icons correct which confirmed the direction of the icon design. We performed a separate experiment for the Friends of Friends icons and developed a number of new variations for the icon, as shown in Figure 3. These included "chain links" and the number "2" to indicate 2nd level connections.

The results of the experiment was:

- twelve chose icon 2,
- two chose icon 1, and
- one chose icon 4.

This confirmed the results of the first experiment for the friends-of-friends icon design.

We believe that the final results provide a sound set of graphical icons for indicating privacy preferences. The icons could be stylised by shadow and/or colours to support more fine-grained visualisations, but the key entities (the people, links, boxes, etc) should remain the same. Future experiments, specifically on live social networks, would provide concrete data on user preferences but early indicators are promising.

Fig. 3. Friends of Friends Icons

4 Privacy Machine Expression

It is clear that a set of icons for representing privacy options will differ across Social Network providers. Even though the consistency argument is valid, other design and business issues may lead to independent sets of icons that users will need to interact with. To then support interoperability across Social Networks, we will then need a consistent representation language that can facilitate machine to machine interoperability.

We look at extensions to the ODRL Version 2.0 language [39] to undertake this task. Our approach is to capture the concepts to support interoperability across service providers. This means, for example, that the concept of "only friends" is consistent across FaceBook and LinkedIn. This means that if I specify a Facebook policy that includes "only friends", and this is then transported to LinkedIn, the same concept applies to all my LinkedIn connections. That is, "only friends" is not tied to any one service provider.

Reviewing the seven Privacy concepts:

- Everyone
- Only Friends
- Some Friends
- All my Networks/Groups
- Some of my Networks/Groups
- Friends of Friends
- No Access

First, lets look at "Some of my Networks/Groups" and "Some Friends". These can only be feasibly implemented with the user specifying the exact identifiers (through the social network user interface) of their friends and/or Network/Group names. The example below shows how the ODRL Permission to Display the Asset (a photo) can be assigned to multiple friends:

```
<o:permission>
  <o:asset uid="urn:facebook:renatoi:photos:mycat-88"/>
  <o:action resource="o:action/display"/>
  <o:role uid="urn:renato.iannella.it''
      function="o:function/assigner/">
  <o:role uid="urn:facebook:billie''
      function="o:function/assignee/">
```

...list more users here...

```
  <o:role uid="urn:facebook:murphy''
      function="o:function/assignee/" >
</o:permission>
```

For Networks/Groups, the Role identifiers would have "group" scope:

```
<o:role uid="urn:facebook:group:soccer-buddies''
      function="o:function/assignee/"
      scope="o:scope/group">
```

...list more network/groups here...

```
<o:role uid="urn:facebook:group:cousins''
      function="o:function/assignee/"
      scope="o:scope/group">
```

Second, lets look at "Only Friends" and "All my Network/Groups". These would require unique identifiers to be created and understood across social networks. We propose two new identifiers:

```
http://odrl.net/role/allConnections
http://odrl.net/role/allGroups
```

Then "Friend of Friends" can be captured with a third new identifier:

```
http://odrl.net/role/all2ndConnections
```

The "Everyone" concept can be captured with a fourth new identifier:

```
http://odrl.net/role/everyone
```

The key issue for these new identifiers is the context in which they operate. That is, we need to state who the primary person is for which all their connections are allowed access to an asset. (Technically we don't need this for "everyone" but it is still useful to assert who made this rights assignment.) We propose to use

the "scope" attribute in the ODRL role element to indicate the new identifier, and since all these new identifiers are multiple people, we assume they are also in "group" scope.

As an example, if we wanted all my "friends of friends" to see the photo on my social network, I would include the following statement:

```
<o:role uid="urn:renato.iannella.it''
      function="o:function/assignee/"
      scope="http://odrl.net/role/all2ndConnections">
```

Notice that the uid is my own identifier as this is used to determine the starting point of the social graph for all my friends of friends.

Finally, "No Access" is dealt with differently under the ODRL Version 2.0 Model. To support this, we would simply use a Prohibition (instead of a Permission). For example, if one friend is not allowed to access the asset:

```
<o:prohibition>
  <o:asset uid="urn:facebook:renatoi:photos:mycat-88"/>
  <o:action resource="o:action/display"/>
  <o:role uid="urn:renato.iannella.it''
      function="o:function/assigner/">
  <o:role uid="urn:facebook:freddie''
      function="o:function/assignee/">
</o:prohibition>
```

These new semantics for the ODRL Version 2.0 language are currently being discussed and proposed in the ODRL working group to support Social Networks privacy. These proposed extensions would also need to consider other related privacy extensions, such as supporting the P3P [26] set of terms (eg retention, purpose). The final outcome could be a revealing set of new terms to express both traditional privacy concerns and new Social Network privacy issues, all within the stable and reliable ODRL framework.

5 Conclusion and Discussion

This paper has looked at two seemingly different, but related areas; privacy icon design and ODRL extensions to support privacy. Typically these are dealt with in different domains (eg user interface design, rights management). However, our novel approach was to combine the two and see if there are improved outcomes. Our emphasis has been on privacy interoperability - both at the user and machine levels. The key incentive for privacy interoperability depends on your view as a User or Social Network service provider. As a user, privacy interoperability means I can expect similar concepts to be presented to me in different online Social Networks and my own Privacy policies to be recognised as I move between Social Network providers. As a Social Network service provider, privacy interoperability means I can provide a predictable interface and service to all my

users, and I can attract users to my service offering without loss of any Privacy policies.

Privacy is, and will always be, a significant issue on social networks. We clearly need to address the human aspects of privacy with innovative user interfaces supporting easily understood privacy dialogs/screens. At the same time, we need to be aware that users will have multiple social network accounts, and with a future drive towards more portability, will move their social experiences from service to service provider. This requires that privacy policies can interoperate across these service providers.

We have presented some early results from designing graphical icons for common social network privacy concepts followed up with usability experiments to ascertain their match to privacy expressions. We also then proposed extensions to the ODRL policy language to enable the privacy concepts to be captured and represented in a machine language to support social networks interoperability.

Together, these two outcomes show a potential new direction for Social Networks towards uniform Privacy user experiences and portable Privacy policies across these service providers. The users will ultimately benefit from these changes with consistency and portability as well as the Social Network providers in supporting stable and reliable privacy representations.

Acknowledgments

Portions of this research was undertake whilst the first author was an employee of NICTA and the second author was a Summer Intern at NICTA.

References

1. Iannella, R. Social Web Profiles. 1st Asian Workshop on Social Web and Interoperability, 4th Asian Semantic Web Conference. 7-9 December, 2009, Shanghai, China
2. "Facebook's New Privacy Push Concerns Experts". Mashable The Social Media Guide. 10 Dec 2009 <http://mashable.com/2009/12/10/facebook-privacy-experts/>
3. "Google Plans to Add Filtering Improvements to Buzz". Mashable The Social Media Guide. 15 Feb 2010. <http://mashable.com/2010/02/15/google-buzz-filtering/>
4. "Lack of eHealth standards, privacy concerns costing lives". Computerworld. 2 Oct 2009. <http://www.computerworld.com/s/article/9138791/Report_Lack_of_-eHealth_standards _privacy_concerns_costing_lives>
5. Hansen, M. User-controlled Identity Management: The key to the future of Privacy. International Journal of Intellectual Property Management, Vol 2, No. 4, Pp 325-344, 2008
6. Bonneau, J. & Preibusch, S. The Privacy Jungle: On the Market for Data Protection in Social Networks. The Eighth Workshop on the Economics of Information Security (WEIS 2009). University College London, England. 24-25 June 2009

7. Strater, K. & Lipford, H. R. Strategies and struggles with privacy in an online social networking community. In Proceedings of the 22nd British HCI Group Annual Conference on HCI 2008: People and Computers Xxii: Culture, Creativity, interaction - Volume 1 (Liverpool, United Kingdom, September 01 - 05, 2008). British Computer Society Conference on Human-Computer Interaction. British Computer Society, Swinton, UK, 111-119.
8. R. Gross, A. Acquisti, & H. J. Heinz. Information revelation and privacy in online social networks. in WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society. New York, NY, USA: ACM, 2005, pp. 71-80.
9. Karahasanovic, A. & Brandtzaeg, P. & Vanatenhoven, J. & Lievens, B. & Nielsen, K. & Pierson, J. Ensuring Trust, Privacy, and Etiquette in Web 2.0 Applications. IEEE Computer. June 2009. Pp 42-49.
10. Pekarek, M. & Leenes, R. Privacy and Social Network Sites: Follow the Money! W3C Workshop on the Future of Social Networking, 15-16 January 2009, Barcelona
11. Bergman, M. Testing Privacy Awareness. The Future of Identity in the Information Society, IFIP Advances in Information and Communication Technology, Volume 298. Springer Berlin Heidelberg, 2009, p. 237-253
12. Lewis, K. & Kaufman, J. & Christakis, N. The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network. Journal of ComputerMediated Communication (2008) Volume: 14, Issue: 1, Pages: 79-100
13. Campisi, P., Maiorana, E., and Neri, A. 2009. Privacy protection in social media networks a dream that can come true?. In Proceedings of the 16th international Conference on Digital Signal Processing (Santorini, Greece, July 05 - 07, 2009). IEEE Press, Piscataway, NJ, 254-258
14. Loukides, G. and Gkoulalas-Divanis, A. 2009. Privacy challenges and solutions in the social web. Crossroads 16, 2 (Dec. 2009), 14-18.
15. Baden, R., Bender, A., Spring, N., Bhattacharjee, B., and Starin, D. 2009. Persona: an online social network with user-defined privacy. In Proceedings of the ACM SIGCOMM 2009 Conference on Data Communication (Barcelona, Spain, August 16 - 21, 2009). SIGCOMM '09. ACM, New York, NY, 135-146
16. Squicciarini, A. C., Shehab, M., and Paci, F. 2009. Collective privacy management in social networks. In Proceedings of the 18th international Conference on World Wide Web (Madrid, Spain, April 20 - 24, 2009). WWW '09. ACM, New York, NY, 521-530.
17. Gulyas, G.G. & Schulcz, R. & Imre, S. Modeling Role-Based Privacy in Social Networking Services. Third International Conference on Emerging Security Information, Systems and Technologies, pp. 173-178, 2009
18. Privacy-Preserving Friendship Relations for Mobile Social Networking. W3C Workshop on the Future of Social Networking, 15-16 January 2009, Barcelona, Spain.
19. Luo, W. & Xie, Q. & Hengartner, U. FaceCloak: An Architecture for User Privacy on Social Networking Sites. IEEE International Conference on Computational Science and Engineering, pp. 26-33, 2009
20. Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M., and Rao, J. 2009. Understanding and capturing people's privacy policies in a mobile social networking application. Personal Ubiquitous Comput. 13, 6 (Aug. 2009), 401-412.
21. Tootoonchian, A., Gollu, K. K., Saroiu, S., Ganjali, Y., and Wolman, A. 2008. Lockr: social access control for web 2.0. In Proceedings of the First Workshop on online Social Networks (Seattle, USA, August 18 - 18, 2008). WOSP '08. ACM, New York, NY, 43-48

22. Bo Luo, Dongwon Lee. On Protecting Private Information in Social Networks: A Proposal. IEEE International Conference on Data Engineering, pp. 1603-1606, March 29-April 02, 2009
23. Gutierrez, A., Godiyal, A., Stockton, M., LeMay, M., Gunter, C. A., and Campbell, R. H. 2009. Sh@re: negotiated audit in social networks. In Proceedings of the 2009 IEEE international Conference on Systems, Man and Cybernetics (San Antonio, TX, USA, October 11 - 14, 2009). IEEE Press, Piscataway, NJ, 74-79.
24. Banks, L. and Wu, S. F. 2009. All Friends Are Not Created Equal: An Interaction Intensity Based Approach to Privacy in Online Social Networks. In Proceedings of the 2009 international Conference on Computational Science and Engineering - Volume 04 (August 29 - 31, 2009). CSE. IEEE Computer Society, Washington, DC, 970-974
25. L.-A. Cutillo, R. Molva, & T. Strufe. Safebook: A Privacy- preserving Online Social Network Leveraging on Real-life Trust. IEEE Communications Magazine, Dec 2009, Pp 94-101
26. The Platform for Privacy Preferences 1.1 (P3P1.1) Specification, W3C Working Group Note 13 November 2006 <http://www.w3.org/TR/P3P11/>
27. Ardagna, C. A., De Capitani di Vimercati, S., Paraboschi, S., Pedrini, E., and Samarati, P. 2009. An XACML-based privacy-centered access control system. In Proceedings of the First ACM Workshop on information Security Governance (Chicago, Illinois, USA, November 13 - 13, 2009). WISG '09. ACM, New York, NY, 49-58
28. Esma Aimeur, Sebastien Gambs, Ai Ho. UPP: User Privacy Policy for Social Networking Sites. Fourth International Conference on Internet and Web Applications and Services, Venice/Mestre, Italy. May 24-May 28, pp. 267-272, 2009
29. Juri Luca De Coi, Philipp Kärger, Daniel Olmedilla and Sergej Zerr. Using Natural Language Policies for Privacy Control in Social Platforms. First Workshop on Trust and Privacy on the Social and Semantic Web. Heraklion, Greece, June 1, 2009
30. Claudiu Duma, Almut Herzog, Nahid Shahmehri, Privacy in the Semantic Web: What Policy Languages Have to Offer. Eighth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'07), 2007, pp.109-118
31. Governatori, G. & Iannella,R. Modelling and Reasoning Languages for Social Networks Policies. Thirteenth IEEE International EDOC Conference, 1 - 4 September 2009, Auckland, New Zealand
32. Lipford, H. R., Hull, G., Latulipe, C., Besmer, A., and Watson, J. 2009. Visible Flows: Contextual Integrity and the Design of Privacy Mechanisms on Social Network Sites. In Proceedings of the 2009 international Conference on Computational Science and Engineering - Volume 04 (August 29 - 31, 2009). CSE. IEEE Computer Society, Washington, DC, 985-989
33. Hawkey, K. and Inkpen, K. M. 2007. PrivateBits: managing visual privacy in web browsers. In Proceedings of Graphics interface 2007 (Montreal, Canada, May 28 - 30, 2007). GI '07, vol. 234. ACM, New York, NY, 215-223
34. Pousman, Z., Iachello, G., Fithian, R., Moghazy, J., and Stasko, J. 2004. Design iterations for a location-aware event planner. Personal Ubiquitous Comput. 8, 2 (May. 2004), 117-125
35. Levy, S. E. and Gutwin, C. 2005. Improving understanding of website privacy policies with fine-grained policy anchors. In Proceedings of the 14th international Conference on World Wide Web (Chiba, Japan, May 10 - 14, 2005). WWW '05. ACM, New York, NY, 480-488
36. Cranor, L. F., Guduru, P., and Arjula, M. 2006. User interfaces for privacy agents. ACM Trans. Comput.-Hum. Interact. 13, 2 (Jun. 2006), 135-178.

37. Kang, T.T. Respect My Privacy. Masters of EECS Thesis, MIT, May 2009
38. Policy Commons. W3C Social Web Incubator Group. 2010. http://www.w3.org/2005/Incubator/socialweb/wiki/PolicyCommons
39. S. Guth & R. Iannella (eds). Open Digital Rights Language (ODRL) Version 2.0 - Core Model. Draft Specification, ODRL Initiative, 23 September 2009. http://odrl.net/2.0/DS-ODRL-Model.html
40. Iannella, R. A Framework for the Policy-Oriented Web in Social Networks. 7th International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods incorporating the 5th International ODRL Workshop. 22 Sep 2009, Nancy, France.
41. Iannella, R. Towards E-Society Policy Interoperability. 9th IFIP Conference on e-Business, e-Services, and e-Society, Nancy, France 23-25 Sept 2009

Appendix

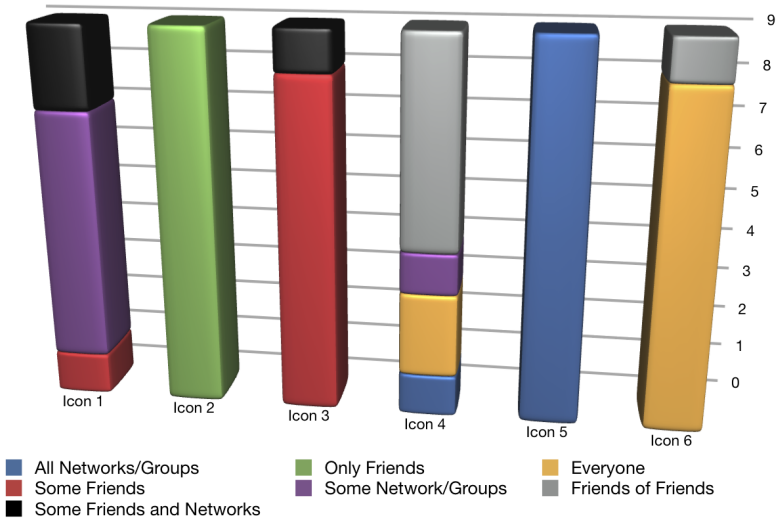

Table 1. Experiment 1 Results

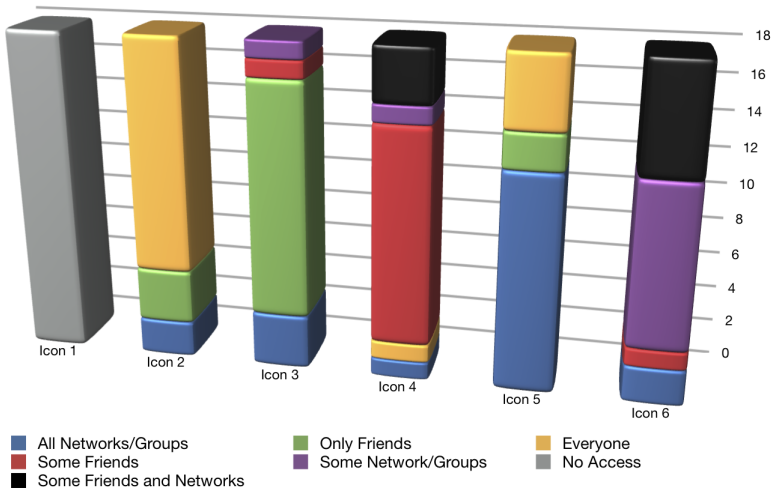

Table 2. Experiment 2 Results