Trust Management in Online Social Networks

Bo Fu, Declan O'Sullivan

School of Computer Science & Statistics,
Trinity College, Dublin
bofu@cs.tcd.ie, declan.osullivan@cs.tcd.ie

Abstract

The concept of trust has been studied significantly by researchers in philosophy, psychology and sociology; research in these fields show that trust is a subjective view that varies greatly among people, situations and environments. This very subjective characteristic of trust however, has been largely overlooked within trust management used in the online social network (OSN) scenario. To date, trust management mechanisms in OSNs have been limited to access control methods that take a very simplified view of trust and ignore various fundamental characteristics of trust. Hence they fail to provide a personalized manner to manage trust but rather provide a "one size fits all" style of management. In this paper we present findings which indicate that trust management for OSNs needs to be modified and enriched and outline the main issues that are being addressed in our current implementation work.

Keywords: Trust, Online Social Networks, multi-faceted, personalisation, ratings.

1 Introduction

The concept of social networking dates back to 1930s, when Vannevar Bush first introduced his idea about "memex" [Vannevar, 1996], a "device in which an individual stores all his books, records, and communications, and which is mechanized so that it may be consulted with exceeding speed and flexibility", and predicted that "wholly new forms of encyclopedias will appear, ready made with a mesh of associative trails running through them, ready to be dropped into the memex and there amplified."

Since the launch of the first online social networking website *USENET* [Usenet] in 1979, we have seen a dramatic increase of online social networks such as *Bebo* [Bebo], *Facebook* [Facebook] and *MySpace* [MySpace] just to name a few, these OSNs allow users to discover, extend, manage, and leverage their personal as well as professional networks online.

OSNs serve various purposes, mostly center around the following topics: business, education, socializing and entertainment.
Business oriented OSNs help registered individuals make connections, build business contacts and maintain professional networks for potential career opportunities; as well as allowing organizations to advertise their products and services. Examples of such OSNs are *LinkedIn* [LinkedIn], *Ecademy* [Ecademy], *Doostang* [Doostang], *XING* [XING] and *Plaxo* [Plaxo].
Educational OSNs usually focus on groups of people who wish to gain knowledge in the same field through the forms of blogs and link sharing with a great variety of subject matters. Examples of such networks can be found in many institutions, where intranets are set up for specific schools, faculties, or classes.
Socializing OSNs aim to provide users with a virtual environment in which online communities can exchange news, keep in touch with friends and family, and make new connections. Usually, various features are implemented which allow users to keep journals, post comments and news, upload pictures and videos as well as send each other messages. Such OSNs tend to centre around themes, such as music, movies, personal life, etc., and are designed to be either user-centric or topic-centric, where online communities can focus on developing profiles all about oneself or developing particular

hobbies. Several examples of this type of OSNs are *43 Things* [43 Things], *CarDomain* [CarDomain], *Friendster* [Friendster], *Hi5* [Hi5], and *MOG* [MOG].
Closely associated with socializing OSNs are entertaining OSNs, where focus on personal aspects of the online communities is less visible, compared to the entertainment attributes these communities may offer to a network. For example, on *YouTube* [YouTube], focus is shifted away from personal profiles, and video sharing feature is greatly valued. Since its launch in early 2005, *YouTube* has quickly become the home of video clip entertainment, it now accounts for 29% of the U.S. multimedia entertainment market [USA Today, 2006].

According to registration requirements, OSNs can be grouped into two main categories, sites that are open to anyone and sites that are invitation only.
Anyone is welcomed to set up an account and put up a representation of oneself in open invite OSNs, such as *Graduates.com* [Graduates], and *Friends Reunited* [Friends Reunited]. However, in order to join some sites, you need to be invited by a trusted member, *aSmallWorld* [aSmallWorld] is an example of such OSNs, where high profile celebrities are among its registered members.

The predominant business model for most OSNs is advertising. It is free for anyone to join, and revenue is made by selling online advertising on these websites. However, a number of OSNs charge their members for the information or services they provide, such as *LinkedIn* where employers can advertise their vacancies looking for suitable candidates.

The remainder of this paper is organized as follows. We first examine the state of the art in trust management mechanisms deployed in OSNs in section 2, which has led to our belief that very little attention is being paid to personalized trust management in OSNs. Next, in order to explore this, we designed an online questionnaire to determine if our initial belief was well founded. The design and execution of the survey is then presented in section 3, followed by the findings in section 4. These findings have helped us identify issues, discussed in section 5, that users have with current trust management in OSNs. And finally, these identified issues have provided a backdrop for the prototyping of our solution that is currently underway and briefly described in section 6.

2 State of the Art

2.1 Trust – Definitions and Characteristics

Trust is an elusive notion that is hard to define, the term "trust" stands for a diversity of concepts depending on the person you approach. To some, trust is predictability, where evidence of one's reputation suggests a most-likely outcome; to others, trust is dependability, where one truly believes in and depends upon another; yet, to many, trust is simply letting others make decisions for you and knowing that they would act in your best interest.

Several notable definitions of trust are presented below.
Grandison and Sloman [Grandison & Sloman, 2000] defined trust as "the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context."
Mui et al. [Mui et al., 2002] defined trust as "a subjective expectation an agent has about another's future behaviour based on the history of their encounters."
Olmedilla et al. [Olmedilla et al., 2005] stated that "Trust of a party A to a party B for a service X is the measurable belief of A in that B behaves dependably for a specified period within a specified context (in relation to service X)."

In summary, trust can not be defined by a single consensus, there is a wide and varied range of synonyms for trust, and the answer to "what is trust" can not be easily provided. Hence, significant challenges are presented for modelling trust in the semantic Web, therefore, it is important for us to concentrate on the core characteristics of trust [Golbeck, 2005; Dey, 2001] which remain true regardless of how trust is modelled.

Trust is Asymmetric. Between two parties, trust level is not identical. A may trust B 100%, however, B may not necessarily feel the same way about A; B may only trust A 50% in return for example.
Arguably, trust can be transitive. Let us say that A and B know each other very well and are best friends, B has a friend named C whom A has not met. But since A knows B well and trusts B's choices in making friends, A may trust C to a certain extent even though they have never met. Now let us say C has a friend named D whom neither A nor B knows well, A could find it hard to trust D. Hence, it is reasonable to state that as the link between nodes grow longer, trust level decreases.
However, others [Grandison, 2003; Abdul-Rahman, 2004] disagree and argue that trust is non-transitive, [Zinnermann, 1994] states that if I have a good friend whom I trust dearly, who also trusts that the president would not lie, does that mean that I would therefore trust that the president would not lie either?
Trust is personalised. Trust is a subjective point of view, two parties can have very different opinions about the trustworthiness of the same person. For example, a nation may be divided into groups who strongly support the political party in charge and groups who would strongly disagree.
Trust is context-dependent. Trust is closely associated with overall contexts, in other words, trust is context-specific [Gray, 2006]. One may trust another enough to lend that person a pencil, but may find the person hard to trust with a laptop for instance.

2.2 Current Trust Mechanisms in Online Social Networks

Current trust mechanisms used in OSNs have been limited to simple access control mechanisms, where authorization is required to contact, to write on, and to read all or part of a user's profile, given that blogging and commenting features are enabled. Communities in OSNs are usually categorized into groups, i.e., one's family, friends, neighbours, etc., with all or limited access to one's photos, blogs and other resources presented.

In *Bebo* for instance, a user can acquire URL for his/her profile which then is viewable to anyone with a browser, or he/she can set the profile "private" which means that only the connected friends to this user are authorized to view the profile and everything presented in it.
In *Yahoo! 360°* [Yahoo!360], access control mechanism is refined by letting users set their profiles and blogs viewable to the general public, their friends, friends of their friends or just the users themselves. The site allows users the freedom to create specific friend categories, such as friends in work, friends met while travelling, etc. Users can then control whether to be contacted via email or messenger by anyone in the *Yahoo! 360°* network, people whom one is connected to, or only those in the defined categories.
In *Facebook*, privacy settings of a profile is further refined by allowing the owner of a profile grant different levels of access to sections of a profile such as contact information, groups, wall, photos, posted items, online status, and status updates. Also, users can decide whether they would like the search engine to list their profiles in search results; as well as whether they would like to notify friends with their latest activities. Finally, a user can select which parts of the profile are to be displayed to the person who tries to contact him/her through a poke, message, or friend request.

Among many notable OSNs, we have found that controlling access seems to be the only way to express trust, where users group their connections into categories and grant all or limited access to these specified categories. Studies [Ralph, Alessandro et al. 2005] of *FaceBook* have shown that many people who are connected to a person are not necessarily "friends" as such, but simply people whom this person does not dislike. Hence, there is a great variety of the levels of trust among these connected "friends" of a person. However, this variety of trust level has not been captured in OSNs, and users can not annotate their variety of trust in a person, nor can they personalise that trust depending on the situation. In some cases, we want private information to be known only by a small group of people and not by random strangers. Such information may be where you live, how much money you make, etc., in an OSN environment, you probably would dislike the idea of letting random strangers read comments left by your friends detailing a trip you are about to take, for safety reasons. In other instances, we are willing to reveal personal information to anonymous strangers, but not to those who know us better. For example, if desired, one can state one's sexuality on a profile page and broadcast that to the world, however, one may not be ready to reveal that very piece of information to the family and friends whom one trusts most.

2.3 Related Work

Much research has been carried out in the field of computer science in relation to trust management, various algorithms, systems and models have been produced, such as PGP [Zimmerman, 1995], REFEREE [Chu et al, 1997], SULTAN [Grandison et al, 2001], FOAF [Dumbill et al, 2002], TRELLIS [Gil et al, 2002], Jøsang's trust model [Jøsang A., 1996], Marsh's trust model [Marsh, 1994] and many more. In particular, a multi-faceted model of trust that is personalisable and specialisable [Quinn, 2006] has been designed in the Knowledge and Data Engineering Group (KDEG) [KDEG] from the Computer Science Department in Trinity College Dublin.

While reviewing trust management systems in computer science, Quinn found that current methods "tend to use a single synonym, or definition in the use of trust… such approaches can only provide a generic, non-personalised trust management solution". To address this problem of the lack of potential for personalizing trust management, a multi-faceted model of trust that is both personalisable and specialisable was proposed, implemented and evaluated. In the proposed model, trust is divided into concrete concept and abstract concept with attributes of their own, where the former includes credibility, honesty, reliability, reputation and competency attributes, and the later with belief, faith and confidence attributes. Ratings are then given to each of the eight attributes, and trust is calculated as the weighed average of these ratings.

The claim for this model is that it has "the ability to capture an individual's subjective views of trust, also, capture the variety of subjective views of trust that are exhibited by individuals over a large and broad population", which in turn, provides "a tailored and bespoke model of trust". In addition to demonstrating its personalization capabilities, Quinn demonstrated how the model could be specialised to any application domain.

The two applications that were used to trial the model and approach were web services composition and access control in a ubiquitous computing environment. However, Quinn did speculate in his conclusions that the model would be suitable for use in the OSN domain.

3 Survey Design and Execution

Given the lack of trust management features within OSNs and our belief that such features would be welcomed, we decided to explore with users whether Quinn's multi-faceted model of trust that enables personalization and provides the freedom of annotating trust subjectively be welcomed in OSNs? And what would be the desired functionalities if such a trust model would be integrated into OSNs? With these questions in mind, *A Survey of Online Social Networks* was designed.

The questionnaire groups participants into three categories as follows, people who are currently using OSNs, people who have used OSNs in the past but are no longer active, and finally, people who have never used OSNs. With the former two categories, the survey aimed to find out user behaviour in relation to trust management aspect in OSNs, and gather user experience with existing trust mechanisms. With the last category, we aimed to find out why some have not or will not use OSNs. Most importantly, without excluding anyone, regardless of participants' experience with OSNs and current trust mechanisms, we asked for their desired trust features as well as their opinions on the multi-faceted model of trust.

A trial questionnaire was first designed and road tested in a computer science postgraduate class, where a group of thirteen people took part in the survey, which has helped the refinement of the official questionnaire.

Considering their flexibility, feasibility and easy data gathering factors, online questionnaires was convenient as we were aiming at a large audience, therefore, *SurveyMonkey* [SurveyMonkey] was chosen to host the online survey on the 27th of May, 2007, over a period of two weeks time. Invitations to take part in the survey were sent out via email, to targeted third level institutions in Ireland, and interested parties were encouraged to distribute the questionnaire further.

4 Findings

In total, 393 people took part in answering the online questionnaire. Among which, 59% were male, 41% were female. 68% of respondents were undergraduate students, 21% were postgraduate student and with the remaining being college employees. Most survey participants come from science related background, with a high 70% of people either studying for or having a degree in engineering, computer science or information technology related fields.

4.1 Category One – Active OSN users

Among 243 respondents who are currently using OSNs, the majority of the profiles are set to be viewable by the general public, while less than 20% of people allow only direct linked friends to view their profiles, as Figure 1 shows.

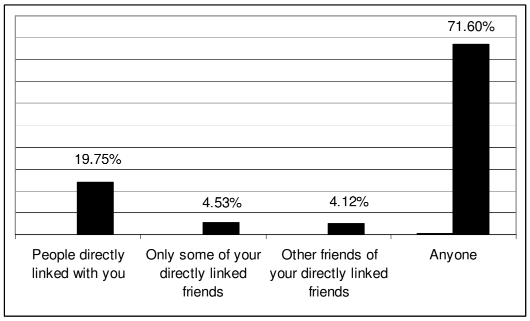

Figure 1: Access settings of user profiles – Category One

We asked the question of whether these users are happy with the available ways of controlling access to their profiles. As Figure 2 shows, most people are pleased with current access control methods, while around 20% of the respondents are not concerned with it and less than 10% of people are not pleased with it. Among reasons given for their dissatisfaction, almost every comment of those 10% of people was in relation to the lack of better access controls to user profiles. For example, many mentioned that in *Bebo*, despite having a private profile, others can still send emails to the profile owner.

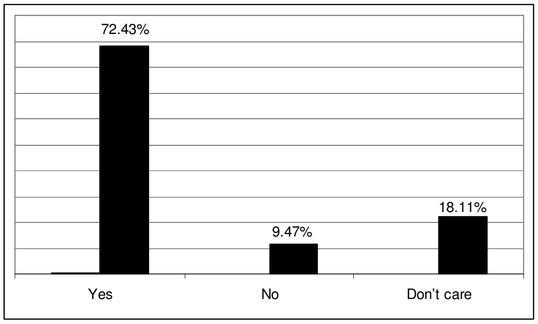

Figure 2: User satisfaction towards current access control methods

Since the majority of this category has public profiles, we asked the question of whether they trust random strangers to view their profiles, as well as the question of whether access control really is necessary. As Figure 3 shows, despite having public viewable profiles, only 25% of these people actually stated the fact that indeed, they do trust anyone and everyone to view their profiles. Most people however, claimed that they do not, while also a large number of people are not bothered by it at the same time. We have found a similar contradictive response regarding the necessity of access control in OSNs, as Figure 4 shows, only less than 20% of these people think it is not necessary, while most people, nearly 55% of the respondents believe that controlling access is necessary, and around 25% of people are not concerned.

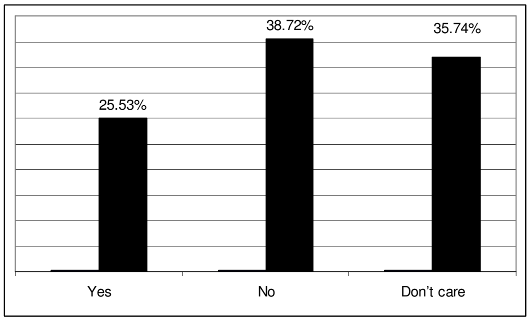

Figure 3. Would you trust random strangers to view your profile?

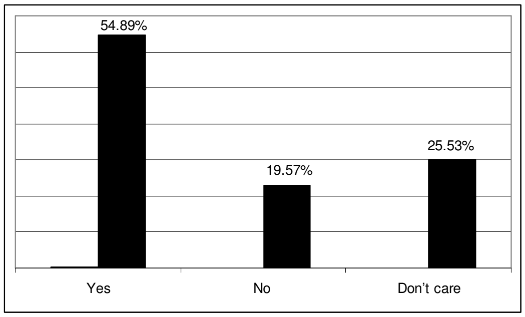

Figure 4. Is it necessary that only certain people can view certain parts of your profile?

4.2 Category Two – No Longer Active OSN users

During their memberships of the 50 respondents in this category, 46% of people had set their profiles accessible by anyone, as Figure 5 shows, 26% allowed only direct linked people to view their profiles.

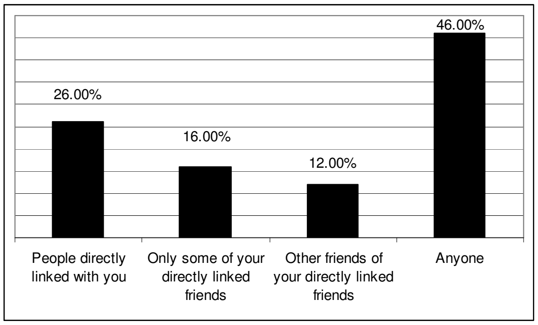

Figure 5. Access settings of user profiles – Category Two

When asked about why have they stopped using OSNs, this category of people gave several interesting reasons. For instance, a lot of people lost interest in OSNs, sometimes due to unpleasant personal experience, or the completion of research or work related projects, or simply do not have time for them any more. In our survey, 5% of people in category two view OSNs as a rather sad way of replacing real life associations, particularly since a lot of sites keep records of the number of visits a profile gets, turning OSNs into forms of popularity contests. However, at the same time, many acknowledge the fact that OSNs are cheap alternatives to keep updated with others, but believe that a refinement in their structure is needed. In particular, privacy concerns were top of the list, with individuals mentioning unpleasant experiences during their membership. For example, on some sites, comments left by close friends are displayed to everyone connected to an individual or sometimes, anyone with a browser; also, being contacted unwillingly by random strangers or friends of a connected friend whom they barely knew. Unfortunately, ways to stop these from happening do not always seem to work, distress and frustration had been caused due to the limited methods that are available.

When asked whether they think access control of profiles are necessary in OSNs, this group of people had a similar response to category one. Among 47 participants who answered this question, 66% of people believe that it is necessary, only 6% of people disagree, with the remaining not caring.

4.3 Category Three – Not Users of OSNs as yet

We were interested to find out why this group of people have never used OSNs, among 57 respondents, some had no interest, some had no time, others dislike the idea of having private information on the Internet and a small number of people have not heard of OSNs, as Figure 6 shows. Again, privacy concerns and the lack of freedom of controlling access to information have been mentioned by the 21.05% of people who stated otherwise when answering this question.

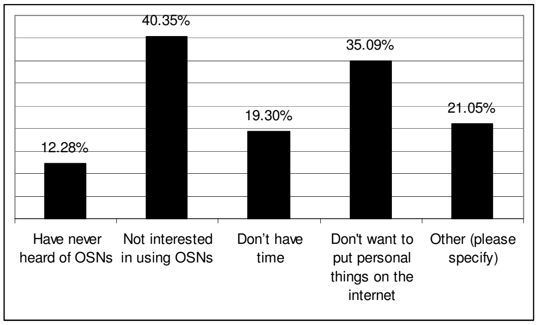

Figure 6. Why have you never used OSNs?

Among 52 participants from this category, we asked whether it is likely for them to use OSNs in the future and whether they believe controlling access to profiles are necessary, 44% of people stated that they would start using OSNs in the future and 69% of whom think it is necessary to control access, only 4% of people disagree and 27% say that they do not care.

4.4 Desired Trust Features and Opinions on a Proposed Solution

If a multi-faceted model of trust with the eight trust attributes: credibility, honesty, reliability, reputation, competency, belief, faith and confidence, is to be integrated into OSNs, would that be welcomed? Would ratings of these eight attributes of a person portrait subjective views of trust in OSNs? With the aim of finding out more on our proposed solution, we asked our participants' views on desired trust features in OSNs as well as their feelings towards a rating feature.

We asked 315 participants, which of those eight attributes of trust are most important in their opinions, as figure 7 shows, honesty appears to be the most important factor, closely followed by credibility and reliability, as well as reputation.

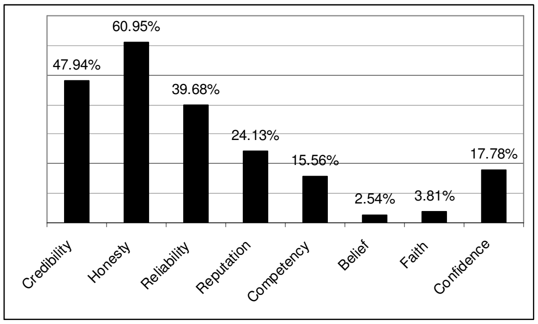

Figure 7. Views on the eight attributes of trust

When asked if a user would like to see the ratings given by others, 44% of participants said yes, 36% said no, with the remaining not caring about it. However, when asked whether they would like to rate others, 67% of people think it is unnecessary, only 9% of respondents believe that it would be helpful, another 10% of people do not care and with the remaining not being able to decide on the subject.

5 Analysis

Several issues have been discovered during the survey, as discussed below:
Current trust mechanisms need to be refined. Most mentioned unpleasant experiences are related to a lack of, or unsatisfying privacy control, while a large number of OSNs fail to allow users to express their various degrees of trust in a person, or a group of people context-specifically. Hence, refinement of current trust mechanisms is welcomed in OSNs.
Personalisation is not provided in current trust mechanisms. Users cannot personalise trust with their subjective views in OSNs at the moment; important trust characteristics as mentioned in section 2 are not captured in OSNs. Even though trust levels vary among members of defined groups, users can not adjust their levels of trust among their connected friends using current trust mechanisms deployed in OSNs.
Users are unsure about a multi-faceted model of trust with rating features. Contradictive findings in relation to a trust rating feature suggest that on one hand, users think that such facilities would help in gaining better control of online profiles, but on the other hand, they find it hard to rate someone they know personally. Such opinions could be the result of a lack of understanding regarding the proposed solution, as for a large percentage of candidates, the word "rating" is very open to interpretation, it would be hard for them to simply imagine what ratings could be like without having the slightest ideas of how-to go about doing it. Also, we need to recognise limitations of the questionnaire, phrasing of the questions and limited open-ended questions in the survey may have restricted the amount of quality data.

6 Current Work

In order to find out whether the proposed multi-faceted model of trust would truly satisfy user requirements regarding trust management in OSNs, currently, implementation of a small scale OSN named *miniOSN* is in progress, powered by *Ruby on Rails* [RoR] and a trust management approach strongly influenced by Quinn's multi-faceted model of trust.
miniOSN has functionalities of a basic online social networking website, it allows users to create accounts for themselves with a username, password and a valid email address. Users of *miniOSN* can then set up representations of themselves, upload photos, post blog entries, as well as leaving comments in connected friends' profiles. The trust management approach implemented in *miniOSN* aims to capture the fundamental characteristics of trust found in the literature review and has the following main features:

- Each user holds ratings of his/her connected friends in the database, which are only viewable to this particular owner and can be adjusted at any time

- Ratings can be given to credibility, honesty, reliability, reputation, competency, belief, faith and confidence attributes of a person
- The owner of a resource - be it a picture, a blog, or a comment - can set trust requirements before distributing that resource
- All users and resources have the highest ratings by default unless specified otherwise
- Users decide whether to transfer a same set of trust values to all other friends of a connected friend
- Users decide which connected friends should start with what ratings

Profile owners can then express trust with personalization, adjust minimum trust rating requirements when granting access to certain resources in their profiles. For example, a family member with a high rating in honesty but a low rating in competency cannot read a certain blog entry; while a work colleague with high ratings in reputation and competency but low rating in reliability cannot see a particular group of photos. Evaluating such an OSN integrated with the multi-faceted model of trust is part of our continuing research agenda.

References

[43Things] 43Things website, http://www.43things.com

[Abdul-Rahman, 2004] Abdul-Rahman, A., (2004). “A Framework for Decentralised Trust Reasoning”, Ph.D. thesis, University of London, UK.

[aSmallWorld] aSmallWorld website, http://www.asmallworld.net

[Bebo] Bebo website, http://www.bebo.com

[CarDomain] CarDomain website, http://www.cardomain.com

[Chu et al, 1997] Chu, Y., Feigenbaum, J., LaMacchia, B., Resnick, P., and Strauss, Ma., (1997). ‘REFEREE: Trust Management for Web Applications.’, The World Wide Web Journal, 1997, 2(3), pp. 127-139.

[Dey, 2001] Dey, A., (2001). “Understanding and Using Context”, Personal and Ubiquitous Computing 5(1): 4-7.

[Doostang] Doostang website, http://www.doostang.com

[Dumbill et al, 2002] Dumbill, E., (2002). ‘XML Watch: Finding friends with XML and RDF.’, IBM Developer Works’, June 2002. Last retrieved from
http://www-106.ibm.com/developerworks/xml/library/xfoaf.html

[Ecademy] Ecademy website, http://www.ecademy.com

[Facebook] Facebook website, http://www.facebook.com

[Friends Reunited] Friends Reunited website, http://www.friendsreunited.com

[Friendster] Friendster website, http://www.friendster.com

[Gil et al, 2002] Gil, Y., Ratnakar, V., (2002). ‘Trusting Information Sources One Citizen at a Time’, Proceedings of the First International Semantic Web Conference (ISWC), Sardinia, Italy, June 2002.

[Golbeck, 2005] Golbeck, J. A., (2005). “Computing and Applying Trust in Web-Based Social Networks”, Ph.D. thesis, University of Maryland.

[Graduates] Graduates website, http://graduates.com

[Grandison, 2003] Grandison, T., (2003). “Trust Management for Internet Applications”, Ph.D. thesis, University of London, UK.

[Grandison et al, 2001] Grandison, T., Sloman, M., (2001). ‘SULTAN - A Language for Trust Specification and Analysis’, Proceedings of the 8th Annual Workshop HP Open View University Association (HP-OVUA), Berlin, Germany, June 24-27, 2001.

[Grandison & Sloman, 2000] Grandison, T., and Sloman, M., (2000). “A survey of trust in internet applications”, IEEE Communications Surveys and Tutorials, 4(4):2–16.

[Gray, 2006] Gray, E. L., (2006). “A Trust-Based Management System”, Ph.D. thesis, Department of Computer Science and Statistics, Trinity College, Dublin.

[Hi5] Hi5 website, http://www.hi5.com

[Jøsang A., 1996] Jøsang A., (1996). “The right type of trust for distributed systems”, Proceedings of the 1996 workshop on new security paradigms. Lake Arrowhead, California, United States, ACM Press.

[KDEG] Knowledge and Data Engineering Group website, http://kdeg.cs.tcd.ie

[LinkedIn] LinkedIn website, http://www.linkedin.com

[Marsh, 1994] Marsh S., (1994). “Formalising Trust as a Computational Concept”, Ph.D. thesis, Department of Mathematics and Computer Science, University of Stirling.

[MOG] MOG website, http://mog.com

[Mui et al., 2002] Mui, L., Mohtashemi, M., and Halberstadt, A., (2002). “A computational model of trust and reputation”, In Proceedings of the 35th International Conference on System Science, pages 280–287.

[MySpace] MySpace website, http://www.myspace.com

[Olmedilla et al., 2005] Olmedilla, D., Rana, O., Matthews, B., and Nejdl, W., (2005). “Security and trust issues in semantic grids”, In Proceedings of the Dagsthul Seminar, Semantic Grid: The Convergence of Technologies, volume 05271.

[Plaxo] Plaxo website, http://www.plaxo.com

[Quinn, 2006] Quinn K., (2006). “A Multi-faceted Model of Trust that is Personalisable and Specialisable”, Ph.D. thesis, Department of Computer Science and Statistics, Trinity College, Dublin.

[Ralph, Alessandro et al. 2005] Ralph, Alessandro et al., (2005). “Information revelation and privacy in online social networks”, Proceedings of the 2005 ACM workshop on Privacy in the electronic society. Alexandria, VA, USA, ACM Press.

[RoR] Ruby on Rails project homepage, http://www.rubyonrails.org

[SurveyMonkey] Survey Monkey website, http://www.surveymonkey.com

[USA Today, 2006] USA Today, (2006). “YouTube serves up 100 million videos a day online”, last retrieved from http://www.usatoday.com/tech/news/2006-07-16-youtubeviews_x.htm

[USENET] USENET website, http://www.usenet.com

[Vannevar, 1996] Vannevar, B., (1996). "As we may think." interactions 3(2): 35-46.

[XING] XING website, http://www.xing.com

[Yahoo!360] Yahoo!360 website, http://360.yahoo.com

[YouTube] YouTube website, http://youtube.com

[Zimmermann, 1994] Zimmermann, P., (1994). “PGP(tm) User's Guide”, October 1994.

[Zimmerman, 1995] Zimmerman, P.R., (1995). “The Official PGP Users Guide”, MIT Press, Cambridge, MA, USA, 1995.