Managing Privacy for Transitive Sharing on a Social Networking Site

J. David Beutel
Fall 2009 Semester
ICS 668
Dr. Dan Suthers
2009 December 20

1 Introduction

On a social networking web site, it's hard to stop someone from finding out too much about you. Even if you don't join the site, you may be tagged in pictures your friends publish that you wouldn't want your boss or parents to see. If you do join, your friends may pass along your personal profile to third-party application developers. Even direct privacy settings have proven difficult to manage, so the transitive exposure of your information adds another level of complexity.

On the other hand, these powerful networks are useful for connecting with people and sharing information. More users than ever are joining them; Facebook alone has over 350 million now. If transitive privacy could be handled well on a social networking site (SNS), users could collaborate to share and maintain even sensitive information, such as addresses or phone numbers for their friends, family, or business contacts. Many SNS users don't provide such details (Young & Quan-Haase, 2009), connecting to their physical world, out of concern for their safety and privacy.

The present paper is concerned with exchanging information about and with your friends, family, business contacts, and other acquaintances, as appropriate, on an SNS. It is a review of literature relevant to understanding and implementing this goal while allaying privacy concerns.

1.1 Trends

Although much has been published about SNS and privacy, little of it touches on the transitive aspects. Overall, research into the users' perspective is often in terms of "privacy", with user studies such as interviews, focus groups, surveys, usability testing, and observing behavior. Meanwhile, proposals for system implementations are often in terms of "access control".

Much of this access control literature is concerned with the use of cryptography and which parts of the system must be trusted or exposed. (Gollu et al, 2007), (Tootoonchian et al, 2008, 2009), (Baden et al, 2009), and (Guha et al, 2008)

suggest several ways to avoid exposing data to an SNS, while still using the SNS to some extent. (Dwoskin & Lee, 2007) propose a way to avoid trusting the user, so an SNS can revoke access to data stored on a mobile device (similar to a digital-rights-management scheme). Those are not examined by this paper, because they do not directly address transitivity.

1.2 Organization

The start of this paper defines issues and requirements of SNS privacy management, from the results of several user studies, in section 2. What kind of privacy choices or decisions do users want to have, and how can they best understand the choices they make? User concerns, expectations, and strategies are examined.

The rest of this paper analyzes a variety of designs and implementations that address aspects of managing privacy for transitive sharing on an SNS. Section 3 explains a conceptual framework for this, called contextual integrity, with a logical model for describing and analyzing privacy policies. Section 4 outlines design guidelines. Section 5 proposes an implementation based on subjective, uncertain trust. Section 6 examines a semantic-web-based implementation. Section 7 introduces an implementation that uses an auction, and contrasts it with an alternative. Section 8 highlights social control. Finally, section 9 concludes.

2 User Studies

As more people are utilizing SNS--350 million on Facebook alone now--researchers have examined their concerns, expectations and strategies relating to privacy. Some of that research specifically addresses instances of transitive sharing, such as tagging photos. Other research can be applied to transitive applications, such as sharing addresses or phone numbers.

2.1 Concerns

(Besmer & Lipford, 2009) performed a user study on tagged photos in Facebook. They had 3 focus groups totaling 14 Facebook users, mostly between the ages of 18 and 24, all found on campus. Participants were keenly aware of groups or specific individuals, especially parents or siblings, who they were concerned would see an unwanted photo of them. Surprisingly, none ever mentioned concern for a stranger finding their photos and figuring out their location or personal details.

Participants were very concerned with their inability to remove other people's photos of them from Facebook. Although they could untag themselves from the photos, they were still indirectly connected to them via their friends' profile. Photos with "incriminating evidence", such as being intoxicated, were another

common concern. Finally, they were interested in shaping their identity based on associations with different people, sometimes untagging photos to disassociate from certain groups.

(Young & Quan-Haase, 2009) took a survey of 77 undergraduate university students, and interviewed 21 others as they showed their Facebook profile. No interviewees gave Facebook their physical address or phone number, some noting it was to reduce their risk of physical harm or unwanted contact from unknown others. Other concerns noted were that their information would be sold or used without their consent or knowledge, and that known others would see photos or information not intended for them. The paper categorized two kinds of privacy concerns: expressive (i.e., image, making an impression on known others), and informational (i.e., unwanted audiences with potentially harmful purposes).

There is a discrepancy between that survey response and earlier research. 64% of the respondents claimed to have limited their profile visibility to "only friends". However, 4 years earlier, (Gross & Acquisti, 2005) found that only 0.06% actually had their profile visibility limited to friends or friends of friends. The respondents in 2009 indicated that they were mainly influenced by negative reports in the media, not by personal experience. Still, the discrepancy is three orders of magnitude. Further research may be needed to see how many actually did something different from what they reported, or how many thought they had but actually failed because of the user interface.

2.2 Expectations

Regarding photos, (Besmer & Lipfort, 2009) participants perceived that the uploader is the owner, despite who the photo contains, and that he has the right to do whatever he wants with it, even posting it online. They were hesitant to take away those rights, even if a photo violated their own privacy. On the other hand, they also felt that the photo owner has a "moral obligation" to protect the privacy of those in the photo.

(Kwasny et al, 2008) held 5 focus groups of 26 Georgia Tech students and 6 women aged 65-80. Groups were of similar age and gender, to encourage disclosure. The biggest difference with age was that the older adults tended to define privacy in terms of space instead of information. They mentioned information as being something official that they are given, such as a social-security number. Younger adults brought up ideas of control, decisions, disclosure, the right to privacy, mutual respect, and personal information; they tended to define privacy mostly in terms of the desire to limit disclosures to others.

Regarding gender differences, women were more likely to talk about privacy "involving others", and only women brought up topics of "respect", "seclusion",

"the 'personal' nature of privacy", "safety", and "having to protect one's privacy". On the other hand, men mentioned "convenience", "freedom", "anonymous", "comfort", and "not being seen or heard".

(Strater & Lipford, 2008) also interviewed 18 undergraduate students about their SNS privacy motivations, opinions, and decisions. Each logged into his or her own Facebook profile, showing the privacy settings and what information was disclosed. The participants judged disclosures based on two main factors: "what they deemed safe and appropriate", and "what seemed to be socially acceptable and normal within their networks."

2.3 Strategies

(Kwasney et al, 2008) classified 82% of its participants, based on a questionnaire of privacy beliefs, as Westin *privacy pragmatists*, willing to trade off privacy for other benefits. This may be skewed by the predominance of younger adults in its sample, considering that half of the older adults were *privacy fundamentalists*, feeling they had already lost much of their privacy and strongly resisting any further erosion.

(Strater & Lipford, 2008) noted two things about Facebook privacy strategies: they tend to be all or nothing, and a one time decision. New users make this decision, but don't modify the settings based on ongoing use. Two approaches to all or nothing were observed:

- Changing privacy settings: 5 participants (28%) restricted all of their profile to only their friends, and 8 participants (44%) added no restrictions (leaving their whole profile open to their network). Only 5 (28%) had settings between all and nothing.
- Limiting the information given: the participants chose to either leave all the fields blank, or fill in most of them (except those that may be considered redundant or had been added later by Facebook).

There were few users who did anything between these all or nothing strategies.

(Young & Quan-Haase, 2009) found that one consideration for information revelation was if it had been previously mentioned in an offline context. It also found that students did not use inaccurate or fake information as a protective measure, primarily because their friends would question that information's validity, causing confusion.

2.4 Conclusion

Transitive sharing via SNS of personal information such as photos, addresses, or phone numbers involves complex and special user concerns, expectations, and strategies. Current SNS do not provide a comprehensive solution for this, but some research has suggested frameworks, guidelines, methods, and implementations that could help meet the needs of users in this area.

3 Contextual Integrity

Reaching for a conceptual framework to analyze these privacy expectations and implications, (Lipford et al, 2009) references (Nissenbaum, 2004) *contextual integrity*. The paper describes Nissenbaum as suggesting two fundamental types of norms for information sharing:

1. *appropriateness* deals with "the type or nature of information about various individuals that, within a given context, is allowable, expected, or even demanded to be revealed" (for example, sharing your mom's medical history with your doctor, but not your religious views with your employer), and

2. *distribution* covers the transfer of information from one party to another (for example, how it's inappropriate for a friend with a radio show to broadcast your personal details that you shared with her in confidence).

The paper claims that Nissenbaum emphasizes two main points:

1. "information is always tagged, as it were, with the context in which it is revealed: there is no such thing as context-free information."
2. The scope of privacy norms depends on the context. "There is no such thing as a universal privacy norm."

Taking a step in the concrete direction, (Barth et al, 2006) collaborated with Nissenbaum to publish a formal model of contextual integrity, using Linear Temporal Logic (LTL) notation, for privacy policy description and analysis. In that model, the subject of information in a message is just as important as the sender or recipient, so it supports the management of transitive sharing.

The model applies policy formulas to a history of *traces*, which describe the state of knowledge in the world and how it has been changed by messages exchanged between agents. LTL allows the expression of past and/or future conditions or constraints (both positive and negative). The paper compares this model to others—RBAC, XACML, EPAL, and P3P—noting that they do not support past or future conditions as well as it does, if at all.

An organization could develop its privacy policies in this model, using them in its IT systems. The paper gives example policies from three laws: HIPAA, COPPA, and GLBA. Because separate policies are expressed in the same logic formulas, rather than depending on opaque functions, they can be combined and analyzed with software tools (such as an LTL model-checker) for certain things:

- *consistency* – whether it is possible within the policy to achieve a given purpose,
- *entailment* – whether one policy implies or encompasses another, such as a hospital's policy satisfying HIPAA, and
- *compliance* – given the history of messages, whether the policy permits the

present message, what future requirements would be incurred, and whether they could possibly be satisfied.

Compared to the semantic web model in section 6, the formulas in this contextual integrity model are not as unified, because an authorization from a user is data in a message, not an additional policy formula.

This model has some limitations, noted by the paper. First of all, it side-steps the issue of mapping reality to the model, taking as input the classifications and affiliations of the agents, roles, and information. Also, it assumes that all the rules are followed, and cannot express what happens when they are not. It has no numerical notations of time, so it cannot express time limits, expiration periods, frequency, etc.

The last limitation noted by the paper is that this model cannot express that certain information must be forgotten, such as the COPPA requirement that a child's information be deleted when a parent revokes consent. Since messages are copied from agent to agent, there is no way to unlearn them. This is similar to the (Shand et al, 2003) trust implementation, described in section 5. On the other hand, revocation is supported by the (Carminati et al, 2009a) Semantic Web access control method, described in section 6, because the information is assumed to stay in one place, although it may be unrealistic to assume that the agent has not made a copy of the information when originally receiving it.

What the paper does not mention is also of concern. What if an agent has some incorrect or obsolete information, or is malicious and sends messages containing lies? The model has no support for trust or uncertainty, which are explored in section 5. The paper also does not consider the design of the user interface.

4 Design Guidelines

Although a formal model of contextual integrity provides some definition of functionality, the design of the SNS functionality and user interface must be considered before implementation methods.

(Lipford et al, 2009) apply the contextual integrity concepts to support their assertions in (Lipford et al, 2008), (Besmer & Lipford, 2009), and (Besmer et al, 2009) that SNS need better privacy support. They examine privacy issues for profiles, news feeds, photos, and applications, generally in terms of Facebook. As a solution, they propose "to make these flows of information more visible", via the following design guidelines:

- "Information flows should be transparent. Users should always be able to determine what information is shared, and with whom."
- "Increase the awareness of information flows during regular activities, so that the ongoing decisions users make are informed by the context of their

information. This is needed to combat the "shrinking audience" phenomenon."

- "Increase awareness of how much information is archived, and still available. This may influence users' current decisions about what to post, and may also influence users to remove old or outdated information."
- "Make information and context concrete. Provide examples of the specific pieces of information when revealing information flows, and examples of specific people or organizations with whom it will be shared."
- "Provide more control over the information flows. While many sites have some privacy settings, users are still not able to fully control the sharing of all of their information."
- "Do not abruptly modify the flow of information. Give users a chance to modify their behavior before changes that could result in privacy problems.

Finally this paper shows a UI prototype for Facebook's profile privacy settings that is much- improved over (Lipford et al, 2008), including profile items with individual controls, displayed consistently instead of hidden. It also references (Besmer & Lipford, 2009) on privacy settings for photos and (Besmer et al, 2009) for applications.

5 Trust

When someone's personal information, such as address or phone number, is given to another user, contextual integrity calls for the context of that exchange to be attached to the information, and for the receiver to abide by the privacy norms of that context. Since the receiver is in the real world, outside the SNS, and can make a copy, he needs to be trusted to do the right thing.

(Shand et al, 2003) presents a method tailored to managing privacy with transitive sharing, but on PDA instead of SNS. Agents may exchange recommendations advising data, its relevance, and level of trust (confidence, belief). The recommendations are used to decide whether or which data to provide to a requester, and to decide the accuracy and relevance of the data for display to the PDA owner (or not). This method could be applied just as well to an SNS.

The key insight of this paper is "unifying trust assessments with access control." Since the PDA is managing distributed data, not centralized on a web server, control is lost once the data is exchanged. The important thing is to not provide the initial access if the requester is untrustworthy of that data.

The PDA owner can define categories similar to roles, such as immediate family, business contacts, and relatives. Categories go into a hierarchy with four privilege bands: the owner, privileged, groups, and public. Privileges of categories in the "groups" band, for example, could recommend by default that

members be able to read and write data to lower categories, and write data to their own categories. The banding of categories provides intuitive defaults for privileges, which can be customized when necessary. For assessing risk and deciding on access or interruption, the data's location in the category hierarchy implies a value.

Recommendations associate permissions in this trust framework. By treating everything as a permission—agents, categories, and data—it creates a homogeneous recommendation structure for access control. "Recommendations conveniently factorize and encapsulate trust policy." (This could also implement contextual integrity's tagging of data with the context in which it was revealed.)

(Carminati et al, 2006, 2009b) also proposes a method of SNS access control based on the trust level as well as the depth and type of relationships between nodes. It notes that trust is not necessarily transitive, but it uses it transitively anyway. It considers the type of the relationship (e.g., friendOf, colleagueOf, etc), which provides some contextual integrity. However, the main thrust of that implementation is a partly-decentralized proof system that offers dubious advantages.

5.1 Recommendations

Although the data in (Shand et al, 2003) is transitive, because anyone holding data can allow anyone else to read or update it, the recommendations are limited by subjective experience. That mechanism originates from the highly cited (Abdul-Rahman & Hailes, 2000).

These recommendations are similar to those on Netflix. Agents who have a history, in a given context, of recommendations similar to the user's own are given greater weight for new recommendation to that user. (Abdul-Rahman & Hailes, 2000) claims not to support trust transitivity, but it is a kind of smart transitivity, although there are no chains of trust. Agents make evaluations and recommendations based on their direct experiences. The user can leverage those recommendations based on his own experiences in that context and with those agents. All experience is subjective, and all recommendations are interpreted subjectively. This supports contextual integrity.

A weakness of this recommendation system is that users starting with no experience have no basis for trusting other agents. However, that is not a problem in an SNS, where users start with their real-world experience with the people they know. Alice can categorize Bob as "co-worker" and "friend", with confidence of 100% and 30% respectively, and this allows Alice to trust Bob to make work-related recommendations.

5.2 Uncertainty

Recommendations should be able to express uncertainty as well as trust, because users handle uncertainty differently. (Abdul-Rahman & Hailes, 2000) used a simple, linear trust value, as did (Carminati et al, 2006, 2009b), but (Shand et al, 2003) introduced support for uncertainty from (Jøsang, 2001), called *subjective logic*. It distinguishes a neutral belief from the case where there is no experience or knowledge.

Users perceive uncertainty differently from risk, preferring a strategy to minimize uncertainty. (Jøsang, 2001) illustrated this with a classic example, the Ellsberg paradox, which found that most people prefer a known risk to an unknown one of equal probability (Ellsberg, 1961). This distinction cannot be made with just a single probability value.

Belief and disbelief are not opposite ends of the same scale; there may be evidence both for and against, like pros and cons. (Shand et al, 2003) weighs both into a linear result via rules for limited transitivity of trust in recommendations.

Unfortunately, neither (Shand et al, 2003) nor (Jøsang, 2001) examines a user interface for expressing opinions in subjective logic. A simple probability could be just a number between 0% and 100%, 0 and 1, some enumeration of discrete choices in a language, or perhaps a scale on a GUI with some point indicated between those numbers inclusive. But, opinions in (Shand et al, 2003) have two components, belief and disbelief, each a probability. Two of the probability UI components could be used, one for each. Or, a GUI could be based on the visualization used in (Jøsang, 2001), a triangle with a vertex for belief, disbelief, and uncertainty, with some point indicated in the triangle for the opinion. Finding a good UI would require more research, but one is needed, because users will want to express uncertainty in some of their opinions and to want those recommendations to be handled differently from neutral opinions.

6 Semantic Web

The contextual integrity model uses an LTL reasoning engine, while the (Shand et al, 2003) recommendation system has its own algorithm. Although this is an internal matter for the SNS, an elegant notation for security policies allows for more and better implementations. (Carminati et al, 2009a) suggests leveraging a semantic web reasoning engine for this.

Its security policies are written in the Semantic Web Rule Language (SWRL). These rules are run through a rule-based inference engine that can do both forward and backward chaining on the Social Network Knowledge Base, to generate a Security Authorization Knowledge Base, which enumerates which users can perform which actions on which objects.

These rules are reflexive, uniformly processing meta-rules (on who can make what rules). For example, if user Bob submits the following SWRL to say that his friends can see the photos he owns:

Owns(Bob, ?targetObject) & Photo(?targetObject) & Friend(Bob, ?targetSubject) => Read(?targetSubject, ?targetObject)

then the SNS can simply preface that SWRL with "AdminRead(Bob, ?targetObject) &", since it was submitted by Bob and produces "Read(x, ?targetObject)", so Bob will need the AdminRead authorization on ?targetObject for his rule to be enforced. That authorization can be inferred from a bootstrap rule such as "Owns(?grantor, ?target) => AdminAll(?grantor, ?target)", meaning that an owner of something can make rules about who is able to do whatever with it (AdminRead inheriting from the AdminAll class).

The paper does not detail support for transitivity, but the powerful notation has that potential. For example, a bootstrap rule of "Read(?grantor, ?target) => AdminRead(?grantor, ?target)" could allow anyone with read authorization to a target to grant anyone else read authorization to that target.

The paper's reification of the rules as data, rather than programming logic dynamically crawling the social network, raises the possibility of leveraging a journal of rule and authorization changes to make them visible to the user as a history, event notification, and explanation of how or by whom a particular object or user can be accessed. This may satisfy a number of design guidelines in section 4, or help implement the audit functionality in section 8. It would also resemble the traces in section 3, and supports similar positive and negative hierarchies of rules, although not supporting concepts of time.

This implementation lacks support for trust levels. The paper acknowledges that flaw by reference to (Carminati et al, 2009b), from some of the same authors, as mentioned in section 5. Nevertheless, the present paper puts trust outside the scope of this implementation, assuming that its calculation is beyond the mathematical capabilities of SWRL and will be handled by some other component of the system.

Of course, users cannot read or hand-craft SWRL syntax. This paper doesn't cover the user interface or other usability issues.

7 Auction

Unwanted disclosure of photos, particularly to certain known individuals, is a major concern of users. However, it is one of the more difficult transitive situations, because there may be multiple people in a photo. Several papers have proposed enhancements to Facebook's photo sharing and tagging, which

Facebook claims receives over 80 million new photos per day now.

(Squicciarini et al, 2009) implemented a bidding system between shared owners of Facebook photos to determine each photo's visibility. The "shared owners" default to whichever users are tagged on the photo, but this must be approved by the actual owner. The bidding system is a "Clarke- Tax mechanism", to prevent users from gaming the system. The photo is visible to owners- only until all owners bid. Then the privacy setting with the greatest "social welfare", defined in terms of each owner's bid, wins the auction. Bidding is done in fiat points, but the paper does not specify how users get those points to begin with.

It detailed an algorithm for this auction, in mathematical set notation. The algorithm went into some detail about how it could take into consideration multiple hops of various types of relations, such as friend- of- friend or co-worker- of- friend.

For ease of use, it proposed an inference technique to base the default bid on the user's previous bids on photos with similar content tags (not id tags). The proof of concept did not implement this, however, and no user study was done.

For users with concerns about certain photos, (Besmer & Lipford, 2009) proposes an alternative design that may be more practical than an auction. It suggests that a social network allow users tagged in a photo to request of the photo owner that certain individuals, groups, or networks be restricted from viewing it. The user can define groups, or choose from recent selections. The request would tell the photo owner how many people the tagged user wants to restrict, but not reveal their identities, to provide the user some privacy and avoid blackmail. (The tagged user previews the request before sending.) Sending the request also temporarily untags the user, until the owner decides whether to honor the request. If not, the user can still permanently untag himself from the photo.

The authors believe this would reflect the users' perceptions of the photo owner's rights, but also his "moral obligation" to protect the tagged users. Their aim was to "relieve some tension on a user over untagging and place more tension on the owner to comply with the request." Users can also keep a watch list of photos they have requested restrictions on. This makes them easy to review, check who has been prevented from seeing each, and add new requests if necessary. This design may be more credible than the bidding system because user studies were taken into account.

One thing not clear in the paper is whether or not the restricted individuals are chosen from the set that currently has access. On the one hand, limiting choices like that could reveal who other users want to restrict, and unwanted users could gain access later by friending someone or having their restriction dropped by the original user. On the other hand, selecting from all users widens the choices to several hundred million Facebook users.

Neither design is applicable to information owned by a single user, such as profile details, but even some of those may be shared, such as members of a family living at the same address.

8 Social Control

Access control is not the only approach. (Rasmusson & Jansson, 1996) introduced *social control* for open systems, distinguishing *soft* security from *hard* approaches like access control. With hard security, once the user has gotten past it, there is no accountability. Soft security allows potentially unwanted intruders, but enables identification and neutralization if they take actions that harm other users. Social control indirectly forces group members to conform to norms. Enforcement mechanisms include reputation or recommendation systems, such as in section 5, or even the Clarke Tax voting-by-bid mechanism of section 7. A user's real-world social network can enforce norms inside an SNS if information flows are made visible, as suggested in section 4. One way to make them visible is to record and expose audit trails, which is a typical part of security in depth.

(Simpson, 2008) asserts that SNS users should be able to know who has seen their data. It calls for the availability of tailored or transformed audits. The research is derived from the context of online medical records. It also asserts that SNS users have the right to decide who can see what of their data, and that it is essential for SNS to support flexible and fine-grained models of access control. However, it doesn't suggest how to accomplish this in a way that users can effectively use.

(Olson et al, 2005) propose an audit trail as a kind of access control, by *informing* the person requesting access that the owner of the data will be able to see the record of that access. This social control would provide the kind of flexibility that our legal system does in every-day life. People are generally free to do whatever they want, without prior restraint, but most are deterred from committing crimes by the knowledge of the consequences, engendering self-restraint. Some SNS have support for this by allowing users to see who has viewed their profile, and some users are self-conscious because of it.

9 Conclusion

Transitive sharing on SNS is becoming prevalent as sites like Facebook become more popular. Users are concerned about managing privacy on such sites, especially for compromising photos or their physical address and phone number. Unfortunately, this author was unable to find any comprehensive research on how to enable users to do this. Several papers address various aspects of this issue in a piecemeal fashion, but they do not address each other, so they may be considered complementary rather than competitive. The most promising

approach is the contextual integrity framework supported by trust recommendations with subjective logic for access control. However, research into a cohesive approach is still needed, with users in mind.

References

Abdul-Rahman, A., & Hailes, S. (2000). Supporting Trust in Virtual Communities. In Hawaii International Conference on System Sciences 33, pp.1769-1777, 2000.

Baden, R., Bender, A., Spring, N., Bhattacharjee, B., & Starin, D. (2009). Persona: an online social network with user-defined privacy. SIGCOMM Comput. Commun. Rev., 39(4), 135-146. doi: 10.1145/1594977.1592585.

Barth, A., Datta, A., Mitchell, J., & Nissenbaum, H. (2006). Privacy and Contextual Integrity: Framework and Applications. 2006 IEEE Symposium on Security and Privacy, 21-24 May 2006, Berkeley, CA, USA.

Besmer, A., & Lipford, H. (2009). Tagged photos: concerns, perceptions, and protections. In Proceedings of the 27th international conference extended abstracts on Human factors in computing systems (pp. 4585-4590). Boston, MA, USA: ACM. doi: 10.1145/1520340.1520704.

Besmer, A., Lipford, H. R., Shehab, M., & Cheek, G. (2009). Social applications: exploring a more secure framework. In Proceedings of the 5th Symposium on Usable Privacy and Security (pp. 1-10). Mountain View, California: ACM. doi: 10.1145/1572532.1572535.

Carminati, B., Ferrari, E., Heatherly, R., Kantarcioglu, M., & Thuraisingham, B. (2009a). A semantic web based framework for social network access control. In Proceedings of the 14th ACM symposium on Access control models and technologies (pp. 177-186). Stresa, Italy: ACM. doi: 10.1145/1542207.1542237.

Carminati, B., Ferrari, E., & Perego, A. (2006). Rule-Based Access Control for Social Networks. In On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops (pp. 1734-1744).

Carminati, B., Ferrari, E., & Perego, A. (2009b). Enforcing access control in Web-based social networks. ACM Trans. Inf. Syst. Secur., 13(1), 1-38. doi: 10.1145/1609956.1609962.

Dwoskin, J. S., & Lee, R. B. (2007). Hardware-rooted trust for secure key management and transient trust. In Proceedings of the 14th ACM Conference on Computer and Communications Security (Alexandria, Virginia, USA, October 28 - 31, 2007). CCS '07. ACM, New York, NY, 389-400. DOI= http://doi.acm.org/10.1145/1315245.1315294

Ellsberg, D. (1961). Risk, ambiguity, and the Savage axioms. Quarterly Journal of Economics, 75:643-669.

Gollu, K. K., Saroiu, S., & Wolman, A. (2007). A Social Networking-Based Access Control Scheme for Personal Content. PROC. 21ST ACM SYMPOSIUM ON

OPERATING SYSTEMS PRINCIPLES (SOSP '07).

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM workshop on Privacy in the electronic society (pp. 71-80). Alexandria, VA, USA: ACM. doi: 10.1145/1102199.1102214.

Guha, S., Tang, K., & Francis, P. (2008). NOYB: privacy in online social networks. In Proceedings of the first workshop on Online social networks (pp. 49-54). Seattle, WA, USA: ACM. doi: 10.1145/1397735.1397747.

Jøsang, A. (2001). A logic for uncertain probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 9(3):279-311, June 2001.

Kwasny, M., Caine, K., Rogers, W. A., & Fisk, A. D. (2008). Privacy and technology: folk definitions and perspectives. In CHI '08 extended abstracts on Human factors in computing systems (pp. 3291-3296). Florence, Italy: ACM. doi: 10.1145/1358628.1358846.

Lipford, H. R., Hull, G., Latulipe, E., Besmer, A., & Watson, J. (2009, August 29). Visible Flows: Contextual Integrity and the Design of Privacy Mechanisms on Social Network Sites. text. Retrieved November 23, 2009, from http://www.computer.org/po ... /doi/10.1109/CSE.2009.241 .

Lipford, H. R., Besmer, A., & Watson, J. (2008). Understanding privacy settings in facebook with an audience view. In Proceedings of the 1st Conference on Usability, Psychology, and Security (pp. 1-8). San Francisco, California: USENIX Association.

Nissenbaum, H. (2004). Privacy as Contextual Integrity. Washington Law Review 79 (2004), 101-39.

Olson, J. S., Grudin, J., & Horvitz, E. (2005). A study of preferences for sharing and privacy. In CHI '05 extended abstracts on Human factors in computing systems (pp. 1985-1988). Portland, OR, USA: ACM. doi: 10.1145/1056808.1057073.

Rasmusson, L., & Jansson, S. (1996). Simulated Social Control for Secure Internet Commerce. In Proceedings of the 1996 New Security Paradigms Workshop, Lake Arrowhead, CA, USA, September 16-19. ACM.

Shand, B., Dimmock, N., & Bacon, J. (2003). Trust for Ubiquitous, Transparent Collaboration. First IEEE International Conference on Pervasive Computing and Communications.

Simpson, A. (2008). On the need for user-defined fine-grained access control policies for social networking applications. In Proceedings of the workshop on Security in Opportunistic and SOCial networks (pp. 1-8). Istanbul, Turkey: ACM. doi: 10.1145/1461469.1461470.

Squicciarini, A. C., Shehab, M., & Paci, F. (2009). Collective privacy management in social networks. In Proceedings of the 18th international conference on World wide web (pp. 521-530). Madrid, Spain: ACM. doi: 10.1145/1526709.1526780.

Strater, K., & Lipford, H. R. (2008). 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 (pp. 111- 119). Liverpool, United Kingdom: British Computer Society.

Tootoonchian, A., Gollu, K. K., Saroiu, S., Ganjali, Y., & Wolman, A. (2008). Lockr: social access control for web 2.0. In Proceedings of the first workshop on Online social networks (pp. 43- 48). Seattle, WA, USA: ACM. doi: 10.1145/1397735.1397746.

Tootoonchian, A., Saroiu, S., Wolman, A., & Ganjali, Y. (2009). Lockr: Better Privacy for Social Networks. To be presented at the ACM CoNEXT '09, Dec 1- 4, 2009, Rome, Italy. Retrieved November 27, 2009, from http://www.lockr.org/papers/lockr- conext2009.pdf

Young, A. L., & Quan- Haase, A. (2009). Information revelation and internet privacy concerns on social network sites: a case study of facebook. In Proceedings of the fourth international conference on Communities and technologies (pp. 265- 274). University Park, PA, USA: ACM. doi: 10.1145/1556460.1556499.