2012 International Conference on Networks and Information (ICNI 2012)
IPCSIT vol. 57 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V57.04

Ethical Issues in Online Social Networks

Adnan Ahmad and Brian Whitworth
Institute of Information and Mathematical Sciences
Massey University, Auckland, New Zealand

Abstract. A community is a social entity that by norms, laws or ethics grants its citizens rights - social permissions to act. Online social networks are computer based communities whose social requirements are not too different from any other. Access control in these networks requires some logical foundation to build upon. Without an agreed logical basis to distribute social rights, current access control models are based on intuition, experience or trial and error. This paper identifies some ethical issues in online social networks and suggests their solutions by socio-technical approach – use the knowledge of physical society as the basis of information rights model for online communities. Social axioms provide a theoretical base for rights analysis that could not only satisfy technical but also social and ethical requirements.

Keywords: Access control, Ethics, Online Social Networks

1. Introduction

In the last decade, we have seen extreme multi-user systems emerge – online social networks (OSN) where millions of users share billions of resources on daily basis and manage each other access rights [1]. Access control systems for OSN are based on the concept of ownership. It is Locke's idea that one should own what one creates, whether a book, a painting or an online photo [2]. If so, everything posted on an OSN should be owned, and conversely if people own their posts, they should manage their access. Essentially, if people don't own the resources they contribute, why bother to add them at all? Why do work for someone else to get the result? If people don't contribute to a social system there is no user community and it fails socially. Ownership of newly created online objects is critical to OSN success for social reasons.

This research was motivated by a questionnaire provided at a recent conference, one of the authors attended. The questionnaire was designed around some basic ownership concepts, related to some of the current issues in OSN. The results of that survey was curious as there was no consensus among the research community over questions like if we don’t have any mechanism to remove dead person’s profile, what will happen in the next 50 years, when Facebook will have more than 500 million dead profiles. This research is first of its kind, to suggest solutions to the common ethical issues of OSN based on socio-technical design.

Our previous works [3 – 6] discuss how online rights can be legitimately incorporated in access control. This paper now outlines the ownership semantics and suggests answers to some ethical issues in OSN based on the socio-technical design – follow the physical community rules to suggest online solutions. This ensures that technical design doesn't impede social needs, i.e. it avoids a socio-technical gap. The technical design may also support or enhance social rules and needs [7]. The rest of the paper is organized as follows: section 2 will discuss the ownership framework for OSN, followed by the access control model based on the framework in section 3. Section 4 outlines some ethical issues and suggests their solutions, acceptable to the ownership theories and access control practices in industry, while section 5 summarizes the presented work.

2. Ownership Framework

To create an information object from nothing is as impossible in an online space as it is in a physical one. Creation *cannot* be an act upon the object created, as it by definition doesn't exist before it is created.

Likewise, an actor cannot request an access control permission to create for an object that does not exist yet. Also, to create an information object its attribute structure must already be known, i.e. exist within the system. To be consistent, creation is an act upon the system, or in general, an act on the space containing the created object. This gives the design principle:

Creation is an act on a space, up to the system space.

This allows an access control system to be initialized with a system administrator (SA) owning a system space with all rights, including create rights, that then evolves into a community as the SA give rights away. To create a community of others, one must give rights away [8].

The logic can generalize to any space - the right to create in the space is initially allocated to the space owner who can allocate it to others who enter the space. So to create a board post, YouTube video, blog comment or conference paper requires the board, video, blog or conference owner's permission. However space owners can vary [9]:

1. *Object type.* The space owner may limit object type, e.g. in a conference, the right to create paper in a track isn't the right to create a mini-track.

2. *Operations*. A comment isn't usually editable once posted but ArXiv lets authors edit publications.

3. *Exclusivity*. Journals give authors exclusive edit rights while Wikipedia lets anyone edit any creation.

4. *Visibility*. Bulletin boards let you see what others submit but conferences don't until the review phase is done.

5. *Defaults*. Space owners set created entity default values.

Object creation is a simple technical act but a complex social one, as a newly created entity's rights are initially unallocated. Locke argued that creators owning their creations is fair and increases prosperity, whether it is a farmer's crop, a painter's painting or a hunter's catch [2]. A community that grants producers the right to their products produces more, while there is no incentive to create by effort for others to own. This gives the design principle:

The creator of new entity should immediately gain all rights to it.

This conveniently resolves the issue of how to allocate the rights to newly created object - they are allocated to its creator, including meta-rights. Yet it isn't what must happen - a technical program can create an information object however it likes, e.g. give its ownership to the system administrator as in traditional applications. Creator ownership is a requirement for social success not a technical necessity.

3. Distributed Access Control Model

Based on the ownership framework illustrated in the previous section, this section will now outline a distributed access control model for OSN. Details of the model can be found in [3]. Table 1 defines the constructs of the core model.

TABLE 1. ABBREVIATIONS AND THEIR DEFINITIONS

	Definition
SH	*Stakeholder:* A user who posts online resource objects, e.g. papers, reviews, comments or votes.
NS	*Namespace:* The set of objects a stakeholder creates.
VU	*Virtual user:* A user, from the social circle of stakeholder, seeking a NS resource access.
LR	*Local role:* A VU group with defined access to NS resources.
OC	*Object class:* An object group, based on security clearance, whose access is mapped to LRs.
AC	*Attestation certificates:* Permission objects encapsulated various access rights and map LR to OC objects.

These components are used to define an access control model independent of the policy. Each *SH* manages its own policy by allocating *VU*s to *LR*s with predefine access to *OC*s. No global administration is required, as *SH*s administer their *NS* resources.

The *VU*s are not mapped to the resources rather the entry point to a *NS* is the abstraction of local roles. All the *VU*s in *SH NS* are assigned some *LR* and access is managed on the basis of *LR* membership. Likewise, objects *O* in *SH NS* are categorized in security labeled *OC* with respect to their clearance level. Additionally, attestation certificates *(AC)* are introduced to add another protection layer [10] and are assigned to every *LR*. The access is granted on the encapsulation of requested right in *AC* for the requested *OC* label.

The access control model can be described as a state transition system $\{\delta, \gamma, \sigma, \Lambda\}$ where δ is a set of states, γ is a set of rights that include privileged requests considered by the system, σ is the entailment relation that determines whether a given right request is true or not in a given state, and Λ is the set of state-transition rules. The implementation computes a function σ_i: $\delta_i \times \gamma \rightarrow$ *{true, false}*, where δ_i is the set of local states of domain *i*, and γ is the set of specific access requests. In general, δ comprises of five different states namely, *Virtual users* (*VU*), *Member (M)*, *Non-Member (Nm)*, *Allow (a)* and *Deny (d)*. σ has four set of functions, including mapping of *VU* to *M* or *Nm*, mapping of *objects* to *OC*, allocation of *AC* to *M* and *OC*, and mapping of *LR* to *OC* to decide the outcome of request Υ_i. Λ comprises of the following access rules for every namespace request:

- If a *VUid* is in NS_i and maps to some LR_j, the *VU* state changes to M_i, else it becomes Nm_i.
- Object belongs to an object class under some label (default $L_1(\tau)$), i.e. $O \rightarrow OC_\tau$, where, τ is the set of all security labels used for confidentiality levels. These labels are hierarchical and form a lattice under a partial order > such that $L_1 > L_2$ if and only if $L_2 \in L_1$.
- If *VU* is in *M* state and requests some object *O* from *OC*, and there is a mapping of LR_i to OC_i then the request Υ_i is granted, else it is denied.
- If *VU* is in *Nm* state and requests some object *O*, then the request Υ_i is always denied.

4. Ethical Issues

This section presents some ethical issues for access control in OSN. It highlights some questions and suggests their solutions based on socio-technical design.

4.1. Who owns the persona?

If every person is represented by some online persona in OSN then who really owns that persona?

In the physical world, freedom is the right to control one's body, to not be a slave to another. If freedom online is the right to control one's online body, or persona, one should be able to edit or delete it, yet many systems don't permit this [9]. A system offers freedom if actors can remove themself from it, e.g. delete a Facebook wall or YouTube channel with nothing left behind. The social logic is that one *owns* oneself online, i.e. an online persona does *not* belong to the system administrator (SA). It gives the design principle:

P1. A persona should be owned by itself.

4.2. Who owns the relationship?

OSN is a combination of users, their relationships with each other, and objects shared by them. Currently, Facebook claims to have more than 955 million users, 67 billion online objects and more than 125 billion relationships among users. If everything in OSN is owned by some user, who owns the relationship? If relationship exists between two users, are both of them the owners of it?

In physical communities, relationship between two users, Alice and Bob can be represented differently based on their personal will and experience. It is possible that Alice considers Bob just as colleague but Bob considers her as a friend. Based on STS design, relationship in online communities are also two unidirectional information objects rather than one bidirectional. The relationship of Alice with Bob is its one aspect – owned by Alice, while the relationship of Bob with Alice is the second aspect – owned by Bob. It gives the design principle:

P2. A relationship is a combination of two unidirectional objects, one side owned by each user.

The concept of unidirectional relationship objects also solves the problem of heterogeneous individual traversal policies and allows every user to formulate their policy according to their own discretion.

4.3. Who can display the information?

If an object is created by user A in a space owned by user B, who has the right to display/ban the object?

The right to display is not the right to view, e.g. viewing a video online doesn't let you display it on your web site. Display grants another the right to view an entity, so it is the meta-right to view, i.e. the right to give the view right over an object to others. Privacy – the meta-right to display the persona, gives the design principle:

P3 (a). Displaying a persona requires its consent.

However, as the SA owns the public list, to put a persona on a public view list needs the permission of both its owner and the list owner, jointly allocated. Table 2 summarizes these persona access rights.

TABLE 2: PERSONA ACCESS RIGHTS.

	View	Delete	Edit	Display	Ban	Allocate
SA	√			½√	√	
Owner	√	√	√	½√		√
SA refers to System Administrator ½ shows that both SA and owner need to be agreed to perform the operation.						

It gives the following design principle:

P3 (b). Displaying an entity in a space requires both persona and space owner consent.

For example, to put a physical notice on shopkeeper notice board involves these steps:
Creation: Create a notice. You own it and can still change it, or even rip it up.
Permission: Ask the board owner if it can be posted on the notice board.
Post: The board owner either vets notices in advance or lets people post themselves.
Removal: As the notice is displayed by mutual consent, either can remove it.

This gives the design principle:

P3 (c). A space owner can ban a persona without their consent.

4.4. Who decides the access policy if two users are tagged in a photo?

In current systems, one can tag their friends in some photo and display it without their permission. Is this approach fair?

Socio-technical design suggests that a person has the rights over his created objects. However, the creator's rights should not contradict others freedom and reputation, i.e., the right to free speech is not the right to defame. As tagging shows that the person is present in the photo, it suggests that they too own it and thus should be asked before being tagged. It also reduces the risks of sharing indecent information about someone. This gives the design principle:

P4 (a). The consent of users should be taken into account before tagging anything in their name.

Another approach in the same vein suggests that the intersection of the two access policies may apply on it. So, the tagged photo can be accessed only by users who are allowed by both tagged users. This phenomenon puts some responsibility on the user tagging photos of others, and also allows both the users to define who can see them. This gives the design principle:

P4 (b). The intersection of access policies of the tagged users applies on tagged objects.

4.5. Are two friends equal?

Current friend based access control models are coarse in nature and treat every user in the social circle at same hierarchical level. However, a user is normally associated with 3 – 6 close friends, 5 – 15 friends, and about1000 acquaintances [11]. Considering this, should two friends be treated at equal disclosure level?

In physical communities, friends are of different disclosure levels, and they are different from family. A family member may have access to your room, but your friend may not. A close friend may share your car, but an acquaintance may not. The current friend notion is quite coarse to incorporate all the semantics of the friend relations. In physical communities, one can't manage all of his friends at the same level, so socio-technical design suggests that the social circle should be refined to include various levels of friends, family members, colleagues and acquaintances. In general, OSN should support user's defined social circles and local roles, so they can devise more fine grained policies. This gives the design principle:

P5. The social circle should incorporate user defined sub-circles, offering different access control policies.

4.6. What happens to dead personae?

Personae are the online representation of users and act on their behalf. However, as people born and die in offline societies, what happens to personae of dead people?

When a persona is created, a set of rules are singed by the user, which deals with the system rights over the resources and the persona itself. Most of the times, these rules also cover the minimum usage requirement for an account, after which the account is blocked[1]. For personae which are not logged in for a specific time, a notification can be send stating that they need to respond. If they don't respond to the notification or do not activate the persona in another specified time, the system can delete the account and all the information associated with it. Also, as in physical societies, every user can select a "Next of Kin" – another user in the system. If some user is not active and not responding, a notification can be send to the kin, to confirm about the deactivation. This gives the design principle:

P6. Kin can be notified, and his feedback can be acquired for dead users.

5. Summary

Online social networks are user communities and cannot prosper without their participation. If the Internet is to be a global community, it must agree on a consistent logic, and solve the ethical, social as well as technical issues. This research suggests solutions to various current ethical issues in OSN based on socio-technical design to meet social and ethical demands of ownership, local administration and relationship management.

This progress is already happening in OSN but without some common basis, this research proposes that the socio-technical design approach is best suited for these systems as they are built around the social requirements of the community. The technical aspects of OSN have been thoroughly discussed in literature, they are good examples of scalability, distributed architectures and software design, but lack social and ethical values. The values that respect social realities provide OSN legitimacy and systems that are legitimate by design are socially sustainable.

6. Acknowledgements

This work has been sponsored by National Science Foundation (NSF), USA, under award number 0968445. "OKES: An open knowledge exchange system to promote meta-disciplinary collaboration based on socio-technical principles".

7. References

[1] Carminati, B., Ferrari, E. and Perego, A. (2008), "Enforcing access control in web-based social networks" ACM Transactions on Information & System Security.

[2] Locke, J. "An essay concerning human understanding". Oxford University Press, 1975.

[3] Ahmad, A. and Whitworth, B. "Distributed Access Control for Social Networks". International conference of information assurance and security, IAS'11, 2011.

[4] Ahmad, A. and Whitworth, B. "Access Control Taxonomy for Social Networks", Proc. International conference of information assurance and security (IAS'11) 2011.

[5] Whitworth, B., de Moor, A., and Liu, T. "Towards a Theory of Online Social Rights", in R. Meersman, Z. Tari, P. Herrero et al. (Eds.): OTM Workshops LNCS 4277, pp. 247 – 256, Springer-Verlag Berlin Heidelberg, 2006.

[6] Whitworth, B. and deMoor, A. "Legitimate by design: Towards trusted virtual community environments". Behaviour & Information Technology Journal, 22:1, p31-51, 2003.

[7] Patel., N. V. "Theory of Deferred Action: Exploring the Boundaries of and Between Socio-Technical Systems Design", Design Principles & Practices 3(4), 285-296, 2009.

[8] Gaaloul, K., Flegel, U., and Schaad, A. "A secure task delegation model for workflows". International Conference on Emerging Security Information, Systems and Technologies, 2008.

[9] Lessig, L. "Code and other laws of cyberspace". New York: Basic Books, 1999.

[10] Thompson, M., Johnston, W., Mudumbai, S., Hoo, G., Jackson, K., and Essiari, A, "Certificate-based access control for widely distributed resources", Proc. 8th Usenix Security Symposium, pages 215–228, 1999.

[11] Boyd, D. "Friends, Friendsters, and MySpace Top 8: Writing Community Into Being on Social Network Sites." First Monday 11:12, December. 2006

[1] Hotmail account poses the maximum idle duration of 90 days, after which the account is blocked.