Access Control Standards: Towards an Online Bill of Rights

Adnan Ahmad
Department of Computer Science
COMSATS Institute of Information Technology
Pakistan
adnanahmad@ciitlahore.edu.pk

Brian Whitworth
School of Engineering and Advanced Technology
Massey University
New Zealand
b.whitworth@massey.ac.nz

Abstract

Social-technical systems are social systems operating on technological base, e.g. Wikipedia, Facebook and YouTube, and so subject to social and technical requirements. Physical society evolved ideas like freedom and privacy over thousands of years but online communities just spring up, built by designers still defining what "social" means. In online worlds, code is law, so system designers are essentially the lawmakers of an open, free system that began much as the Wild West did, except now social rules are enforced by access control code not guns. Berners-Lee argues that a bill of online rights is needed to protect the open neutrality of the World Wide Web [1], and this paper agrees, but adds that it must be written as an access control model.

Introduction

Social-technical systems like YouTube and Facebook, which are information technologies mediating online communities, have engaged over ninety percent of all internet traffic in the last decade. These technical platforms, where millions of people share billions of resources, now evidence the same social structures as physical communities, as they are essentially still people interacting with people [2]. Just as physical society has privacy, social networks have privacy settings for pictures and posts. The current Facebook profile has about 275 privacy options, more than most people can manage, yet despite this apparent overkill people still find privacy problems, e.g. that a friend who tags you on a photo puts it on your page without consent seems wrong. Interpreting social concepts is hard, so social networks prefer to make their own rules, like that one can't "friend" another unless they also "friend" you, but that's not how people work. In 1999, Sun CEO McNealy declared: "*You have zero privacy anyway. Get over it.*", but online might is not right, and privacy didn't die. Indeed, as long as social appearances matter, privacy will count, as those who commit suicide after online humiliations testify [3]. Freedom, another social concept, is equally perennial, but if you can't delete your

Wikipedia or WordPress profile, do you own your online "self"? Human beings have fought and died for physical freedom, so it is unlikely they will agree to be online subjects.

The need is to translate social ideas like *ownership* into technical specifications. Ownership rules can reduce conflict over digital objects as well as physical objects. Social rights are a high level language for *access control*, to allocate ownership, so why reinvent the social wheel electronically [4]? Do we really need to re-learn online that legitimate societies prosper and illegitimate ones don't?

Current access control rules for social networks based on intuitions not standards differ between applications and over time, and are often only checked by public outrage. That no global standards exist for the rights to view, edit, create or delete online entities is a design failure, as people expect the social conventions they know to apply online as well. Social-technical systems package the old wine of society in the new bottle of technology, so they need to get the wine right.

Socio-technical design

In 1950's, the Tavistock Institute introduced the term socio-technical to oppose Taylor's attempt to reduce factory workers to machine parts, introducing human factors like [5]:

a) *Congruence*. A process should fulfill its own objective, so democracy needs democratic methods.

b) *Delegate control*. Provide employees with objectives and let them choose how to achieve them.

c) *Flexibility*. Give workers "extra" skills to handle change, lest specialization lead to extinction.

d) *Coal-face change*. Empower those experiencing a problem to solve it, not absent managers.

e) *Innovation*. Encourage innovation at the boundaries, where work passes between groups.

f) *Transparency*. Give information to those it affects first, e.g. to workers.

g) *Evolution*. Work systems evolve in an ongoing iterative process that never stops.

h) *Example*. Leaders should lead by example, as if a General takes an egg his army may loot a village.

i) *Mutuality*. Staff who can choose, feel, learn and belong in return give back to the company.

It proposed the ethical use of technology, but its credo *just because you can doesn't mean you should,* also applies to technology design. Computing already recognizes human factors, but the new "user" is *the online community*. Computing must now satisfy social as well as human, software and hardware needs (Figure 1). Community needs are a new computing requirement [6].

In the industrial revolution, factories enslaved people so technology was the villain, but in today's information revolution, Twitter, Facebook and YouTube help against oppression, so technology is the hero. By *allowing freedom online,* the Internet itself is the revolution manifesto, as people ask: "Why can't my community be so free?" For the first time in human history, political revolutions are based not on a few great heroes, but the many *"small heroes"* plus technology [7].

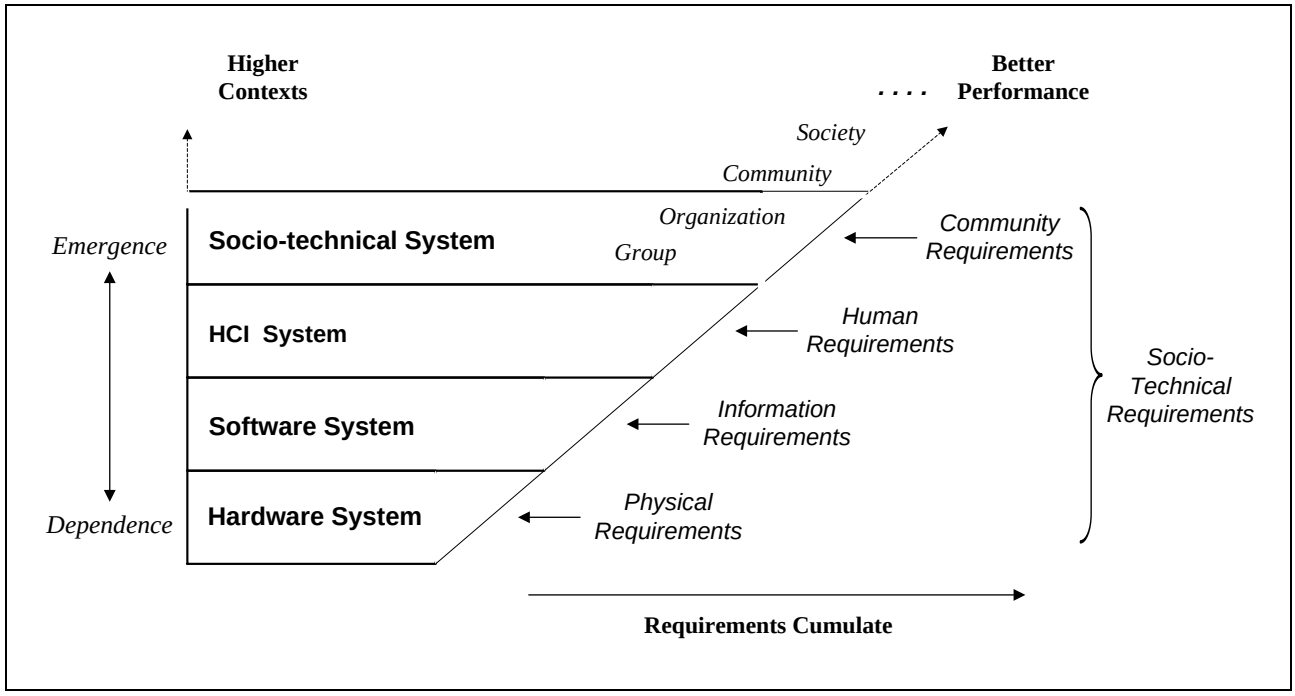

Figure 1. Social and technical requirements cumulate

Social inventions like the road code are less obvious that technical inventions like the car, but both are important, e.g. the Knights Templar *invented credit* by giving pilgrims a chit to redeem in Jerusalem instead of carrying cash, and it is critical to business. Likewise without the invention of the United Nations, nuclear conflict could have destroyed humanity last century. Today, traders give billions of dollars to online people they haven't met, for things they haven't seen, to arrive at some unidentified future time, which a medieval trader would see as pure folly, yet almost all online business works this way. Modern markets have *confidence*; the willingness to transport goods to unknown people or to fund risky projects, because if the other party cheats, the community will step in [7].

Technology is the *proximate* cause of financial exchanges but the social system is the *distal* cause, i.e. why it occurs at all. Without confidence, the global financial system would collapse, as the recent credit crunch illustrated, but this doesn't make it a house of cards. Just as a physical system is stable given its requirements are met, so a social system is stable if requirements like fairness are met. The error is to ignore the social system and its requirements. Today, technology mediates society and society limits technology, but one can't "stretch" physical laws into cyberspace because they:

a) *Don't transfer:* What is online "trespass"?
b) *Are too slow:* Constitutional laws take years to change but online code changes every month.
c) *Don't apply:* What law applies to online "cookies"?
d) *Have no power:* How can the law punish online users who are anonymous?

e) *Have no jurisdiction*, e.g. American law applies on its but cyber-space isn't "in" America.

We must reinvent the social principles behind physical laws in online code.

Definitions

Communities, by laws, norms and rules, give people *rights* - social permissions to act. As physical rights express physical ownership, so online rights express information ownership [9]. They don't automate interactions as by definition they are choices not compulsions. The right to delete a file doesn't make one delete it, any more than the right to sue forces one to sue. Rights are what we *can* do online, not what we *must* do. The goal is *legitimate* rights, accepted as both fair and in the public good. The data model proposed is:

1) ***Entities****:* Represent static system information.
    - *Actor*. An active entity that can socially interact.
        - *Persona*. An online avatar, profile or mail account.
        - *Agent*. Represents a persona.
        - *Group*. Multiple personae acting as one.
    - *Object*. A passive entity that conveys information.
        - *Item*. An object with no dependents, e.g. a post.
        - *Space*. A complex object with dependents, e.g. an email thread.
        - *Namespace:* A set of objects owned by a persona, e.g. a wall.
    - *Right*. An access control permission for an act.
        - *Simple right*. The right to act on an actor or object.
        - *Meta-right*. The right to act on a right, to transfer or delegate it.
        - *Role*. A variable right.
2) ***Operations***. Actions upon entities.
    - *Null operations*. Don't change the target, e.g. view.
    - *Use operations*. Change the target, e.g. edit.
    - *Communications*. Transfer data from sender to receiver, e.g. send.
    - *Meta-right operations*. Modify a right or role, e.g. unfriend.

An *actor* entity can socially interact and an *object* entity conveys meaning to an actor. An *item* is an object without dependents, like a photo, while a *space* is an object with dependent objects, e.g. a wall. Every entity needs a parent space to contain it, so the spaces above it, up to the system itself, are its *ancestors*. Conversely, every space has *offspring* - the entities it ultimately contains.

In access control, a right (R) permits an actor (A) to apply an operation (O) to an entity (E):

$$R = (A, E, O)$$

Such triplets can define an access control system [9]. A *meta-right,* the right to change a right, works the same way, except the target entity is a right. An object *owner* has its meta-right, i.e. the authority to allocate its rights, e.g. to post a video on YouTube an *actor* must register*,* create a personal *space*, submit a video *entity*, and grant YouTube the *right* to display it, which is a *meta-right* operation.

Social standards

Social systems, whether mediated technically or physically, implement social standards to succeed, whether by law or code.

1) Accountability

The elements of a social system are people accountable for their actions. No program currently has a "self" to be a social actor, so an access control system must allocate all its rights:

The accountability principle. *All rights must be allocated to persona representing actors at all times.*

An access control system can ban a person and delete their rights, but it can't take them itself.

2) Freedom

If I create a persona, whether a Hotmail identity or game avatar, it should belong to me:

The freedom principle. *Every active online persona should own itself.*

This rule simplifies access control and denies online slavery, that one persona can control another. I should be able to delete any online account I created, yet some systems don't allow this.

3) View

Operationally view as a null act doesn't alter anything, but being viewed socially energizes the viewee, e.g. a viral video excites its author. This *social facilitation* arises because social success depends on how others see you. People are accountable for their effect on other *viewers*, so have to remove offensive posts. One can't be accountable for what one can't see, giving:

The view principle**:** *To be accountable for an object one owns, in any way, implies the right to view it.*

What we post "in private" on Facebook is visible to moderators accountable for what it contains. Any space owner has the right to view all its contents, e.g. a track chair should be notified of new track papers as ancestor space owner are responsible for all their offspring.

4) Privacy

Privacy, the right to control the display of one's personal data, is about choice not secrecy, as one can *choose* to publicly reveal personal data, e.g. if everyone in a company agrees to say display their salaries to each other, there are no privacy issues:

The privacy principle: *Every person has the inalienable right to control the display of their personal information.*

One shouldn't use a telephoto lens to spy on people at home but what about in public? To photograph a crowd does one need everyone's permission? The acceptance of CCT surveillance in Britain surprised privacy advocates, but socially, people *mutually agree to be viewed* when in public. So I can photograph you in public without your consent, but can't *display* it on my magazine cover without consent, because the right to view is not the right to display (see #9).

5) The public domain

When Disney copyrighted public domain stories like Snow White, which they didn't create, many felt it was neither fair nor in the public interest, i.e. illegitimate. What people have given into the public domain shouldn't be appropriated. Open-source advocates like GNU and SourceForge now use Creative Commons contracts to ensure that no-one steals public domain items, giving:

The public domain principle: *Non-personal information validly made public cannot be taken back.*

If a photo is put in the public domain, how is this reversible? Can online journals rewrite history by "unpublishing" articles? Yet personal data as an inalienable right can't be permanently given, so a European Union court recently ruled that Google must honor user requests to not *link* to personal data made public. Yet surely the solution is to remove the data, as Google argues.

6) Creation rights

Creating an object can't be an act on that object that doesn't exist yet, so it is an act on the space that contains it:

The right to create principle. *The right to create an entity originally belongs to the space owner.*

To add a video, blog comment or board post requires the video, blog or board owner's consent.

7) Creation ownership

By Locke, creator(s) owning their creation(s), whether a painter's painting, a hunter's catch or a farmer's crop, is fair and increases prosperity [10]:

The creation ownership principle. *The creator immediately gets all the rights over the created object.*

This simplifies access control, as new items can be allocated to their creators. If I create a video I *initially* own it, but the space may also impose *creation conditions*.

8) Creation conditions

The delegation of the right to create by a space owner may include *conditions* the creator agrees to beforehand, e.g. a university gives staff a space to create in, so a condition of employment can be

that it owns all its faculty's ideas. By Locke this reduces creativity, but Facebook could likewise claim every post and YouTube every video, if these *creation conditions* are known in advance:

The creation conditions principle. *The conditions of a delegated creation in a space must be clear in advance.*

A person creating an object in a space should know if they can delete it, as ArXiv lets authors delete submissions but some boards don't. Indeed an access control system's rules could be automatically translated into clear text, to allow *social transparency*.

For a Hotmail or Gmail account, the creation condition is that if one doesn't use it for some time it

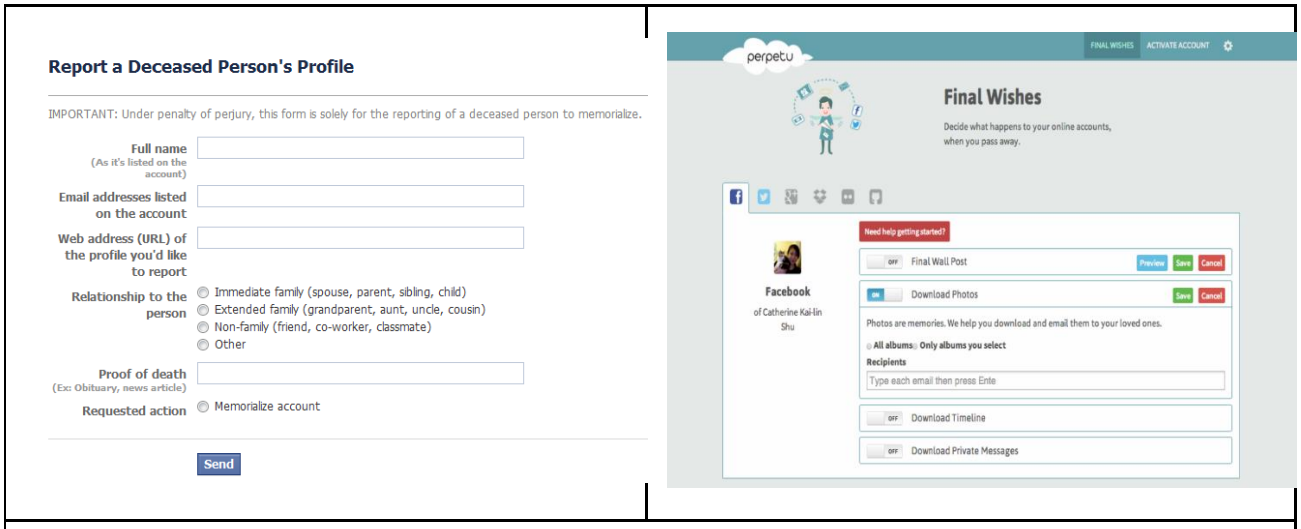

Figure 2. a. *Facebook's deceased profile page,* b. *Perpetu online wills*

can be deleted. In contrast, if a Facebook user passes away their wall may be a memoriam for loving comments and virtual flowers, which it allows (Figure 2a). As people have physical wills and next of kin, systems like Perpetu let people manage their online accounts when they dies (Figure 2b).

9) Display rights

The right to display isn't the right to view - *viewing* a video doesn't let you *display* it on your site. *Display is the view meta-right*, the right to assign the right to view an object, and privacy is that meta-right for personal data. Displaying a video on YouTube is a video owner letting the space owner display it, just as posting a notice on a shop noticeboard is letting the shopkeeper display it. To put a text, photo or video in a space requires the consent of both its owner and the space owner:

The display principle. *Displaying an object in a space requires the consent of the displayer and the space owner.*

Displaying a notice on a physical notice board involves these steps:

1) *Entry*. Physically enter the shop.
2) *Introduction*. Introduce yourself to the shopkeeper, if not known already.

3) *Produce*. Give them your notice.
4) *Edit*. Amend as necessary to their requirements.
5) *Post*. The shopkeeper may vet and post it or let you post it yourself.
6) *Display*. The public sees it.
7) *Removal*. The notice can be removed by you or the shopkeeper.

Likewise, displaying a YouTube video involves:

1) *Entry*. Enter YouTube.
2) *Registration*. Create a YouTube persona.
3) *Produce*. Upload your video.
4) *Edit*. Add YouTube properties like title.
5) *Submit*. Submit to YouTube to display.
6) *Display*. The public sees it.
7) *Removal*. Again, the displayer or YouTube can remove it.

The same logic applies both cases because the social system works the same in both mediums. The video creator initially owns it, by Locke, then delegates the right to display it to YouTube, who can choose not to if it fails decency or copyright rules, but they can't alter (deface) it as *they don't own it*. A public phone book is the same, as it can give people private listings and reject offensive listings. Computing technology will soon allow *private views*, i.e. displays private to a group.

10) Consistency

Social consistency is that social rules always apply, e.g. just as YouTube takes the right to allow videos in its space, or not, so it gives its users the right to have comments or not, as a commented video is a space within a space. Social consistency increases access control efficiency and is a key feature of legitimacy, giving:

The legitimacy principle. *Legitimate access control rules apply on all social levels and in all cases.*

The Mafia illustrates social inconsistency, as it demands loyalty from its members but gives no loyalty to the community of which it is part. Consistency lets one system space, owned by one person (the system administrator), evolve into an online community by the delegation of rights.

11) Roles

In access control, a *role is a variable right,* based on a set, so instead of letting one person view my home page, I can let my "friends" role view it. Local roles can be locally defined, so as well as the 15 friends and 1000 acquaintances most people have, they could have 3-6 close friends or 10-50 family as well. To add someone to your friend set is an act on *your* local role that doesn't need *their* consent:

The role principle. *A role owner can add or remove persona from their role without others consent.*

If I unfriend you, the system needn't tell you, as it changes nothing you own. Currently, social networks say "*Bob wishes to be your friend*", making friendship a social tit-for-tat, but people don't trade friendship, they give it. I can love you even if you don't love me. Programmers trying to rewrite social rules by software fiat often fail, as the attempt to ignore privacy illustrates. If a bi-directional friendship combines two unidirectional roles, owned by each party, the message should be:

"*Bob has befriended you, do you want to befriend him?*"

12) Reallocating rights

Socio-technical systems can evolve dynamically by reallocating rights as follows:

1) *Transfer*. Transfers rights and meta-rights to a new owner, so selling a car transfers all rights and the old owner has no rights over it afterwards.
2) *Delegated*. Transfers use rights but not meta-rights so is reversible, e.g. a rentor renting a house to a rentee delegates it for a time, but later gets the house back.
3) *Merge*. Divides rights among actors who must merge rights to act. Any actor in a merged right can stop it; e.g. couples who jointly own a house must both sign to sell it.
4) *Share*. Copies a right among actors, so each acts as if they owned it exclusively; e.g. couples who severally share a bank account can each take out all the money.

In information terms, merging is an AND and sharing is an OR policy combination. In publishing, one author can edit a paper, or delegate it to another, or authors can share it, so each can do any change, or they can divide it, so every author must confirm every change. Each policy has different social effects, as sharing is risky but invites change while merging is safer but makes change harder.

That delegation doesn't give the meta-right means that a delegatee can't further delegate:

The delegation principle. *Delegating doesn't give the right to delegate.*

Renting an apartment gives no right to sub-let, so when Outlook lets you delegate your email to another party while on holiday, they can't further delegate it without your permission.

13) Democratic action

Merging access control policies allows democratic actions online, given:

The democratic action principle. *Joint actions require the permission of the all the parties involved*

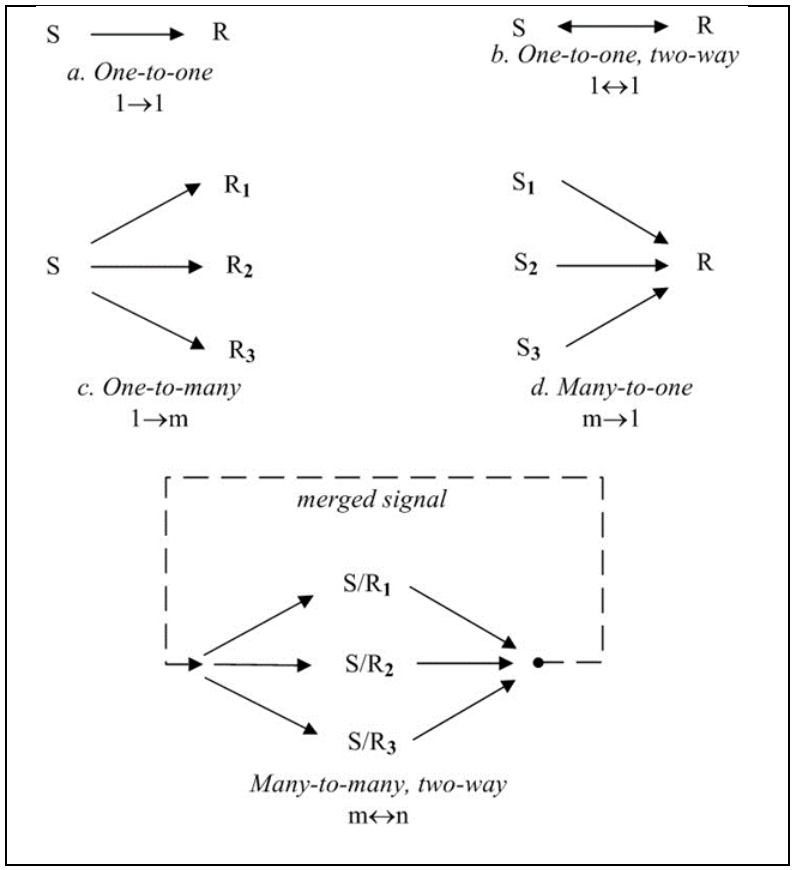

Figure 3 Communication linkage (S = Sender, R = Receiver)

Currently, someone tagging me in a photo puts it on my page without my consent, but they shouldn't be able to post on my wall like that. Access policy merging needs the permission of both parties, so the system should ask: "*You are tagged in this photo, allow it on your page?*"

For a large group like a nation, the traditional options are control by: *dictatorship* (one person), *aristocracy* (a select few) and *democracy* (a majority). So a dictatorship is one persona owning the group, an aristocracy is a persona set, and a democracy is its members owning it.

14) Voting transparency

In traditional communication *richness* can be defined as the meaning possible as follows:

1. *Position*. A choice, e.g. a raised hand.
2. *Document*. A static pattern, e.g. a text sentence
3. *Streaming*. A dynamic pattern, e.g. audio.
4. *Multi-stream*. Many dynamic streams, e.g. video as audio plus video.

However if meaning is the human response, it also depends on the *communication linkage,* the number people involved in the communication, defined as follows:

1. *Interpersonal:* One-to-one, two-way.
2. *Broadcast:* One-to-many, one-way.
3. *Matrix*: Many-to-many, two-way.

Matrix communication operates when a democratic group wants to act as one, as when a nation votes for a new leader. The vote is the country telling itself what "it thinks". Just as an e-mail is a one-to-one communication from one person to another, so voting is a many-to-many communication from a group to *itself* (Figure 3). Tag clouds illustrate matrix communication, as people clicking on a text link increase its font size, just as people walking in a forest form paths for others to follow.

	Linkage

Richness	***Broadcast***	***Interpersonal***	***Matrix***
Position	Footprint, Flare, Scream,	Posture, Gesture, Salute, *Smiley*	Applause, Election, *Web counter, Karma system, Tag cloud, Reputations, Social bookmarks*
Document	Poster, Book, *Web site, Blog, Online photo, News feed, Instagram, Tweet*	Letter, Note, *Email, Text, Instant messaging, Social networks*	*Chat, Tweet, Wiki, E-market, Bulletin board, Comment system, Advice board, Social media*
Streaming	Radio, Record, CD, *Podcast, Online music*	Telephone, *Cell phone, Skype*	Choir, Radio talk-back, *Conference call, Skype conference call*
Multi-stream	Speech, Show, TV, Movie, DVD, *Online video*	Face-to-face talk, *Chatroulette, Video-phone, Skype video*	Face-to-face meeting, Cocktail party, *Video-conference, MMORPG, Simulated world*

Table 1: Communication performance by richness and linkage

If *communication performance* involves both richness and linkage, the advances of the last computing decade were more about linkage than richness, as chat, Twitter, texting, and karma systems are all lean text (Table 1). By Locke, the voters that create a vote result own it, so should be able to view it:

The vote transparency principle. *Every voter is entitled to see the vote result they helped create.*

Democracies understand that people won't vote if the result is secret, but in online votes this transparency depends on the code. A rights based access control system would automatically allocate a votes ownership jointly to the voters who created it by #7, who can then view it by #3.

15) **Communication**

In communication, a sender creates a message then offers it to a receiver, who may accept it. It is a joint act that requires the consent of both parties:

The communication principle. *Every communication act requires prior mutual consent.*

The "send and forget" design of email enables spam by allowing communication without consent, but systems like Skype and Twitter require consent to communicate [11].

Implementation

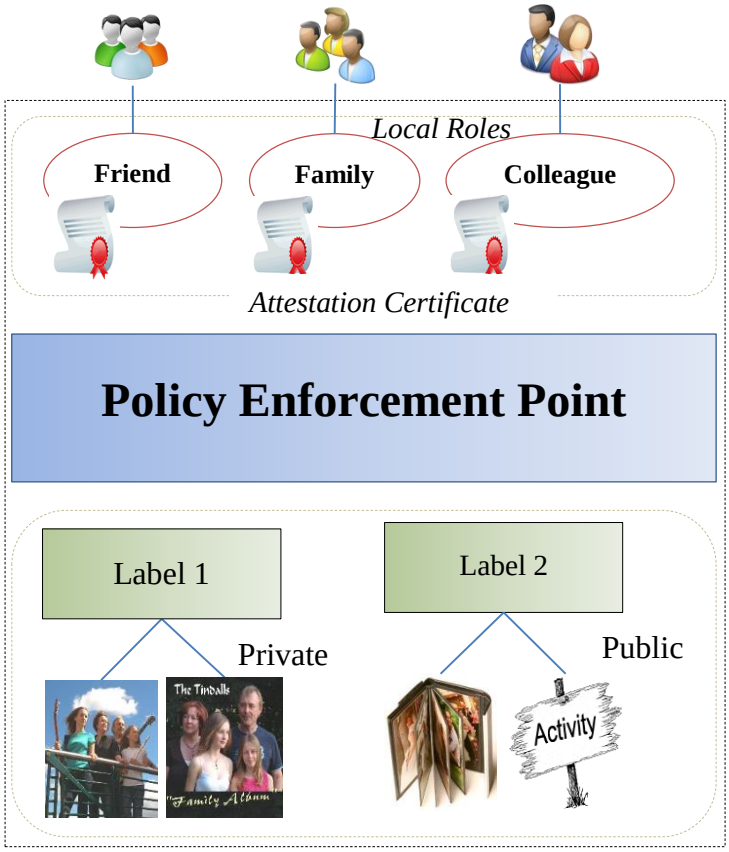

Figure 4. An access control model architecture

Social rights can be supported by an access control system that maps personas to a domain with local roles (Figure 4). Classifying objects into object classes and using attestation certificates allows asymmetric relationships, giving fine-grained access control without global policy overheads. Such models are already in use, but global agreement is needed for user's to trust online social relations. This model is asserted by the following rules:

- All the users who have mapping to at least one of the local roles in a domain become the member of that domain.
- All the objects in a domain having the same confidentiality level are grouped by a label, which forms a hierarchical lattice under the order '>', where $L_1 > L_2$ when $L_2 \in L_1$.
- If a member user requests for an object and (s)he has the lattice clearance, then the request is granted.
- If a member user doesn't have the lattice clearance, then the request is denied.

- If a non-member user requests an object, the request will be denied.

The future

Socio-technical designers could wait until humanity perfects its social logic, but that is still coming and we can't wait. In any community, some legitimacy is better than none. Synergy-based communities like Wikipedia and Kickstarter as a new *social form* must be enabled by technology [6]. In the past, declarations, constitutions and laws preserved advances like democracy, but today, the Internet's social gains, which Berners-Lee says must be preserved or they will be lost, relies on access control code. Only a global access control model can encode an online bill of rights.

References

[1] Kiss, Jemima. (2014, March 12th). The Guardian, Retrieved March 27th, 2014, from http://www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web

[2] Jahnke, I. (2009). Socio-Technical Communities: From Informal to Formal? In B. Whitworth, & A. de Moore (Eds.), Handbook of Research on Socio-Technical Design and Social Networking Systems (pp. 763-778). Hershey, Pennsylvania, USA: IGI Global.

[3] Alvarez, L., (2013, October 15th), The New York Times, Retrieved March 8th, 2014, from: http://www.nytimes.com/2013/10/16/us/felony-charges-for-2-girls-in-suicide-of-bullied-12-year-old-rebecca-sedwick.html?_r=0

[4] Ridley, M. (2010). The Rational Optimist: How Prosperity Evolves. Harper.

[5] Porra, J., & Hirscheim, R. (2007). A lifetime of theory and action on the ethical use of computers. JAIS, vol. 8, no. 9, pp. 467–478.

[6] Whitworth, B.; Whitworth, A. P. The social environment model: Small heroes and the evolution of human society. First Monday, Vol 15, 11-1, Nov. 2010.

[7] Whitworth, B., & Ahmad, A. (2014): The Social Design of Technical Systems: Building technologies for communities. Aarhus, Denmark, Interaction Design Foundation.

[8] Mandelbaum, M. (2002). The Ideas That Conquered the World. New York: Public Affairs.

[9] Freeden, M. (1991). Rights (Concepts in Social Thought). Minnesota, University of Minnesota Press.

[10] Ahmad, A., & Whitworth, B. (2011). Distributed Access Control for Social Networks. International Conference of Information Assurance and Security. Malacca, Malaysia.

[11] Locke, J. (1963). An essay concerning the true original extent and end of civil government. In J. Somerville, & R. Santoni (Eds.), Social and Political Philosophy, pp. 169-204. Anchor.

[12] Whitworth, B. and T. Liu (2009). Channel email: Evaluating social communication efficiency. IEEE Computer, July, vol. 42, no. 7, pp. 63-72.