Challenges to Privacy in Social Networking Mashups

Social TV as a Case Study

By Karen R. Sollins
Principal Research Scientist
MIT Computer Science and Artificial Intelligence Lab (CSAIL)

MIT Communications Futures Program

A white paper based on discussion in the Privacy & Security Working Group
within the **MIT Communications Futures Program (CFP)**
Authored by Karen R. Sollins, MIT
Presented on August 4, 2011

Participating CFP Companies:

BT
Cisco
Comcast
Nokia Siemens Networks
Telecom Italia

Social networking provides opportunities to expand the nature of existing applications and user activities in cyberspace. Consider the idea of "social TV". Along with these opportunities to combine activities such as social networking and TV or entertainment, comes an interesting set of challenges to the privacy of identity information. In this paper we will examine a key set of these challenges. These include issues of merged identities, inference across identities, merged privacy policies, and flow of information among the composition identity management systems involved in a new composite application service. We conclude with a set of observations to keep in mind when designing such a composition or mashup of existing services, especially with respect to identity and privacy. These observations include

- Identity information is derived from a number of different kinds of sources, with differing kinds of provenance and trustworthiness. It is worthwhile to retain and expose these differences in creating composite identities.

- There is increasing business pressure to discover and take advantage of identity information, either for individuals or in aggregate. We face a new challenge in finding an economic or business model that honors the individual's privacy.

- Although it is tempting and probably wise to consider the composition of privacy policies when identifying information is being merged from different sources, those original policies or elements of policies may not be meaningful in new and different contexts.

This paper was originally presented at The IEEE ICCCN Workshop on Social Interactive Media Networking and Applications (SIMNA), Maui, Hawaii, Aug. 4, 2011 and published in the proceedings of the workshop. The work was funded by the MIT Communications Futures Program.

Challenges to Privacy in Social Networking Mashups: Social TV as a Case Study

Karen R. Sollins
MIT Computer Science and Artificial Intelligence Laboratory
Cambridge, MA, USA
sollins@csail.mit.edu

***Abstract*—Social networking provides opportunities to expand the nature of existing applications and user activities in cyberspace. Consider the idea of "social TV". Along with these opportunities to combine activities such as social networking and TV or entertainment, comes an interesting set of challenges to the privacy of identity information. In this paper we will examine a key set of these challenges. These include issues of merged identities, inference across identities, merged privacy policies, and flow of information among the composition identity management systems involved in a new composite application service. We conclude with a set of observations to keep in mind when designing such a composition or mashup of existing services, especially with respect to identity and privacy.**

Keywords-component; *social networking, mashups, identity management, privacy*

I. INTRODUCTION

In this paper we examine challenges to privacy in the context of the convergence of two key kinds of functionality: social networking and entertainment, for which we use the term "TV". The objective of the paper is to identify these challenges. The challenges to privacy derive not only from each of those contexts, but are made more complicated in the convergence of the two; the challenge to privacy is about the convergence of identity information.

In reviewing the development of social networking over the last few years, it has evolved from a small community wishing to communicate with each other and share information about themselves, to a broad and increasing set of services and functionality. Originally, social networking sites were developed for college students at a particular college to communicate and "socialize" with each other electronically. The audience was limited and known, the content was limited to text, photos, and perhaps video, and the kinds of information collected about the participants was restricted to finding each other and exchanging or "posting" information. With Facebook in the lead at present, these sites have evolved into increasingly rich, broad, and commercial capabilities. In part this may have been driven by demands or requests of the users, but more likely they have been driven by business opportunities. In the commercial social networking world, as is well understood, the business model is that of advertising, and for that to be most effective, the best targets of advertising are those that are best understood or profiled. Hence, the social network business model is to collect, collate, and analyze as much information about the user as possible, in order to sell the best advertising opportunities.

Let us now briefly turn to the TV industry. Here, the original model was the provision of a single and then multiple streams or channels, paid for with advertising as well, but the target was the broadest audience, rather than the individual. This evolved into selling packages of channels through either cable or satellite delivery and hence to the addition of pay-per-view. With this evolution, the target might be the

This work was supported by the MIT Communications Futures Program.

individual household. There are the beginnings of profiling individuals[1] from a number of providers in different countries. As we will discuss further below, we are starting to see a merging of TV provision and online social networking.

In addition to the evolutionary merging of these two kinds of services into what one might call "social TV", simultaneously there is increasing interest both in the business of "identity management" (such as the Liberty Alliance [8], now subsumed by the Kantara Initiative [9], the OpenID effort [10], and the multipronged effort of the Telco 2.0 effort [15]) in part as a result of the apparent increase in the number and diversity of "identities" that the individual user is asked to utilize and manage. Shibboleth [12] and InCommon [6]are two broad based approaches to federation of identity management in order to provide more seamless single sign-on. Shibbleth provides single sign-on across an extremely large number of academic institutions, while InCommon is providing federation for local community-based organizations. This increasing pressure to provide over-arching or single sign-on approaches to identity management leads to an attendant increasing number of questions about privacy of that identity information.

Privacy is being given increasing attention ranging from governmental efforts [1], [4], [3] but also civil rights groups, such as the American Civil Liberties Union (ACLU), the Electronic Privacy Information Center (EPIC), the Electronic Frontier Foundation (EFF), and the Center for American Progress. Attention to privacy dates from as early as 1890 by Warren and Brandeis [16], when they raised issues of conflict or tussle, whether because of how it exhibits conflicts between constitutional rights, as discussed by Swire [14] and Strandburg [13] or other governmental responsibilities[2] to business model conflicts. Warren and Brandeis examined the constitutional and legal basis for privacy. Swire and Strandburg examine the relationship between the right to privacy and the right to freedom of assembly. The FTC and Dept. of Commerce examine the tradeoff space between individual privacy and effectiveness of businesses to operate.

In the following sections, we will first elaborate on the idea of social TV and then identity management and identity information. That will provide the basis for a discussion about a number of key challenges to privacy in this evolving context. Possible technical solutions must be addressed in a different context.

II. SOCIAL TV

The concept of "Social TV" is a return to the social nature of the television experience at its origins.[7][5] The early model of TV watching was that it was done in a family or community group and thus was a shared experience within a social group. With increasing penetration, another form of interaction evolved, "the coffee-machine conversation", which increasingly focused on what the participants at work saw on TV the previous evening. This latter experience separates the watching experience from the communicating experience, but extends the social model.

With the increase in what is now being called Social TV, we are currently seeing a merging of new forms of communication with new forms of TV or entertainment watching. An extremely simple form of this may be watching video content, whether network TV productions, content from a Hulu kind of service, or content from a site such as YouTube with some reasonably independent communication model, often a social networking capability, such as Facebook, MySpace, or Twitter. Increasingly we find that these media are being merged. A very early version of this was music TV available about five years ago in Europe. Viewers could send premium SMS messages to the TV station, which would then be scrolled across the bottom of the screen, running. More advanced forms solicit SMS messages on specific "topics". In both forms, the identity information, such as the phone number, is discarded with only a voluntary "identity" included. More recently, during the Obama inauguration, cnn.com had both live video and a stream of comments from Facebook on a single screen. This is occurring increasingly frequently, more often with

[1] Examples include products from Sky TV, Kabel Deutschland, and DirecTV, each of which provides the option of some form of identifying information, often a smart card, for identifying and authorizing individual viewers within a household.

[2] In private conversation with the author, a commercial social networking company n Germany reported that they are required by privacy laws to delete personal information within a month, but required by law enforcement agencies to keep communication for at least 6 months. As a result, they are considering relocating to another country.

Twitter feeds. Comcast has new entry into this market with Tunerfish, an online social networking site specifically tuned to complement their TV and entertainment products. We can expect this to be a growing market.

There are several directions that this may expand. The first and simplest is to provide a continuous and somewhat richer social networking feed in conjunction with content selected in the context of a social networking group, collection of friends, or other self-selecting community that is smaller than the universe of possibly participants. This reflects a truer merging of the entertainment video and social networking application domains.

A second, more sophisticated development is the possibility of integrating additional kinds of application domains or services. A primary target is online merchandising and shopping, or in the US, fundraising for public television. It is likely that this direction of extensibility should and will be extensible to include qualitatively different kinds of capability, thus enriching the Social TV experience in new dimensions.

One of the reasons that Social TV is an interesting case study is that it demonstrates an interesting set of tussles. The business opportunities may be enormous and without them it will not evolve or thrive. Regulation and social mores may dictate certain kinds of constraints. Individual privacy concerns may further complicate the tussle between increasing participation and perceived threats and risks. In this context, we focus in this paper on concerns of management and use of personal information in the context of tussles between users and service providers.

The idea of social TV is not new, but was reviewed deeply by Klym and Montpetit in 2008 [7] and recently was mentioned in Technology Review by Hof in considering the future of TV.[5]

III. IDENTITY INFORMATION

Since our focus in this paper is on issues surrounding merging identities from multiple domains, we will begin with a simplistic example from the social TV space. We start with a group of friends from work, who before heading home, decide to share a TV experience during the evening, a sports event. Each member of the group has at least one online social networking identity and each is part of a household that has traditional TV service of some kind. To do this, they will all use a social TV service. In the simplest case, they will all use the same online social network and TV service, but it is to the social TV service provider's advantage to allow for use of as many different online social networks and TV services as possible to increase their potential customer base. Within this group, Bobby is a "Trekky", and has joined a group to discuss "Star Trek" alien languages, but considers out of bounds with work colleagues. Sandy has previously expressed a liking (used the "like" button) for certain brands of clothing, thinking it would simply be pooled information that would improve the reputation of the manufacturers with other potential customers. Alex has chosen a TV service package that is heavily loaded with children's programming. Alex has kept the fact of having children from people at work.[3] The online social network considers Sandy a good target for similar kinds of clothing, and similarly, the TV service provider considers Alex a good target for children's toys. Bobby is also an advertising target for science fiction conventions.

Up front the social TV service has a dilemma. It is building a service utilizing supporting services, in this case online social networks and TV services and is adding additional value to that. The question it must address is how much control of the user experience remains with the supporting services and how much it controls. For example, will all the participants in the evening's sports viewing party see the same ads or not? If one of their group is interrupted by a friend outside the group through the online social network, will the others see that? The list of possibilities is endless. This is about both control of the experience and the information that can potentially be collected in the process, opening up additional business opportunities, which, as we discussed earlier, has been the progress of online social networks. As we will see below this composition is in fact at the heart of many issues with respect to privacy as well.

[3] The author knew a student who kept his child private from everyone at his university for a number of years, in order that having a child not be considered a factor in his progress on his dissertation.

We next consider examples of identity information that the social TV service might access from the supporting services. From the online social network, the social TV service may learn the name provided by the user, email address, home town, high school, a sampling of "friends", groups that the individual has joined and some profiling of "likes" as indicated by the user pushing the "like" button at other sites. If the user was not logged into the online social network at the time of using the "like" button, generally the IP address of the user's machine, but if the user happened to be logged in to the online social network, the user's ID is then annotated with that choice. [4] Furthermore, some set of credentials or other authorization provided by the online social network may be available to the social TV service.

From the TV service provider, the subscriber's name, home community (e.g. for access to community TV programming), billing address, email address, and information about the subscription and pay-per-view programs watched. Again, the social TV service may acquire credentials or other authorization in order to ascertain whether the user has legitimate access to the content.

Finally, the social TV service may want to provide the appearance and experience of a unified and enriched environment. So, they may provide their own single sign-on approach, that underneath provides the login to the supporting services, manages and collects information in order to provide the service it is offering more effectively, and possibly to enable future services and business opportunities.

To summarize, identity information, with or without the original privacy policies associated with it may be provided from each of the supporting services to the mashup or composite application of social TV, which may also collect its own identity information. The social TV service is likely to "compose" those supporting identities with its own, possibly make inferences, and combine information that was never intended to be combined. In addition, there are well understood cases, in which identity information can flow back from the composite, such as the social TV service, to the supporting services, with little control over whether that information originated with the final receiver or the other supporting service. In other words, once the links have been made across the identity information in the originally independent domains, it may be further mixed and distributed.[5]

IV. KEY CHALLENGES

We identify five key challenges that arise from expectations of privacy and discuss each briefly. The five are:

(1) composition of identities and privacy policies,

(2) inference across domains,

(3) unintended exposure,

(4) reverse flow of information,

(5) secondary leakage of information.

These all arise because of misunderstandings, confusions, or lack of clarity in the context of composition of multiple domains, each with its own model of identity information and privacy. This work assumes that the service providers intentions are to preserve privacy, but we must acknowledge here that there may be a tension, between the user's privacy intentions and possible business opportunities for the service providers. That would be the subject of a different paper.

A. Composition of identities and privacy policies

The most obvious privacy problem with our social TV scenario is the set of opportunities that derive from the composite nature of the application domain. Even in this simplest of social TV scenarios, there are three domains involved, with three distinct models of identity and privacy of that information. The social

[4] This is how Facebook functions.

[5] Although they are not alone in this, Facebook is an example of this information flow, not only through the use of "like" buttons, but also as an identity service provider that, in turn often provides all the code to bring up new web services, using Facebook as the supporting structure.

TV identity is composed of identity information from each of the supporting domains, in addition to its own information. Each online social network user will have some model of privacy settings and controls in the online social network domain. Each TV subscriber will have different privacy settings and controls supported by the TV service provider for its domain. Finally, the social TV identity may be not only a composite of a subset of the identity information derived from the supporting domains, but also some of its own. Each domain will have both distinct identity information and applicable privacy policies over that information. This may lead to either a very complex and perhaps non-intuitive composition of privacy policies or more likely one that is irreconcilable. In order to avoid this complexity, it is likely that the third party application will reduce the privacy constraints unilaterally, perhaps simply in order to provide feasibility.[6] It is important to note, that the user may be left without a clear understanding of which privacy policies apply to which information, especially once it is made available to the social TV service.

Furthermore, increasing the heterogeneity by adding more supporting services for a richer "social TV" experience will make the problem multiplicatively more complex. If the users are not all using the same online social network or TV provider, the issues become more complicated, because different users, or the same users using different online social networks may find different privacy policies enforced or not. If a Social TV application evolves to include something such as public TV and radio membership profiles, customer relationships with merchants, credit card profiles, and on and on, the complexity of profile information flow and privacy policies, especially when not codified in any formal way, becomes unmanageably complex.

B. Inference across domains

A further dimension to this problem arises from the fact that personal information that may originally have been kept separate in the separate domains may now flow among them. Some of this information flow is at the heart of enabling composite applications with composite identities, but consider the following. If the online social network is providing the communication substrate and if the participants on the social TV scenario above share URLs for the program or related material, the online social network will now have information that all of the group is interested in various topics related to the sports event, and may use that to infer information about all the participants, some of whom had carefully not joined particular groups, to avoid having their interest in the subject known by the online social network. This is one example of leakage of information across the boundaries. For example, a member of the group may have alcohol related issues, but may want to keep that private, although an inference might now be made about all members of the group, if adequate care is not taken, such as with respect to the advertising that they all see. It is possible that information can and will flow back from the social TV domain to the supporting domains. The sources of that information may be the social TV domain itself, or it may have originated in the other supporting domain. This implies that there may be porous boundaries among the domains, at best leading to a confusion for the users, and at worst a violation of privacy policies (and possibly laws, in those places where privacy regulation exists). Furthermore information may leak back into the other application domain.

C. Unintended exposure

We next address the privacy issues surrounding what information about individual participants in the shared social TV experience may be exposed to the other participants, perhaps unexpectedly and undesirably. Let us consider what some of the boundaries might be on "sharing" an experience. In its simplest form we can imagine that our group comes together in the social TV environment and when all are gathered, one of them starts the "show". The idea is that they all see the same content simultaneously and can use the online social network component to communicate with each other, although from their perspective they are logged into the social TV application space, rather than the online social network or TV provider space. One might consider, in this context, how exactly they are presented with the same content. One person may live in a household for which even mild violence is to be bleeped out, while another does not and thinks that missing parts of the program corrupts the whole show. As a result of watching this

[6] As an example, with respect to sharing identity information, Facebook does not pass along any information about privacy policies, along with the information it provides to third party services it supports. They are likely not alone in this approach.

particular event, Bobby may be targeted to receive ads for science fiction conventions, while Alex might be targeted to receive ads about children's toys. In these cases, it is easy to understand the sources of those target decisions. In a more complex situation, the information for targeting may be determined by a combination of home location as represented in either the online social network context or the TV provider context, who their friends are in the online social network, and various other behaviors they have exhibited in one or the other of the supporting domains. One then must ask whether they all see only their own ads, because that leads to a less shared experience. If the TV content were the SuperBowl[7], one of the attractions and primary subjects of the shared experience may be the ads. Do they all see all of the ads addressed to each of them? That may be a violation of their supporting privacy policies. At the same time, if they see different ads, they will have had different "SuperBowl" experiences. Furthermore, by sharing ads that have been targeted at one or another of them, they are also sharing information about themselves that may not have been desired or intended. It may be that Bobby and Alex do not wish for that information about outside interests or family situation to be known to these particular friends. Information about them is leaking from either their private TV "customer" identities or their online social network identities in ways that may not be intended.

The "like" button and Sandy's situation is an example of a further extension of this. As mentioned above, if the user is logged into the online social network to which the "like" preference is being reported, that information is generally associated with the particular user. If the user logged in to the online social network directly, at least he or she may be aware of this. If the online social network was providing identity services to a third party service, such as our social TV service, the user may not even know that he or she is logged in to that online social network service. This is more subtle form of unintended exposure of personal information.

D. Reverse flow among services

As mentioned above, one of the hidden challenges to users' intentions to retain certain kinds of privacy may be threatened or violated because the set of services composed to support the intended service may receive information back from the service that the user is interacting with. Thus, for example, in our simplified example the social TV service may, intentionally or not, provide information back to the TV and online social network services, and there is little or no control over where that information originated. Hence information can leak from one domain to another, in contradiction of the user's intentions and wishes. This derives from the challenges of composing privacy policies, in part due to weak tracking of the provenance of identity information, and in part due to lack of carrying privacy policies forward. One of the significant advancements made by the Geopriv [2][11] work in the Internet Engineering Task Force (IETF) was to include privacy policies with the information provided that were not only enforced when information is accessed, but a form of them that is attached to the information as it travels, so that further enforcement is at least possible.

E. Secondary exposure

Finally, we note that privacy may be violated by secondary exposure. If a user is in a situation where non-participants can know about the shared experience of the group, again undesired and unintended exposure of some member's personal information can occur. Examples may include the non-participant being able to see the screen or hear an audio stream of the private social TV group, such as if one of the participants is in a public location. This kind of situation suggests that there may be information about each participant's immediate context that may it important to incorporate into the social TV experience, reflective of some immediate contextual information. This kind of information about context is an example of information that is necessary for and unique to the social TV experience but not derived or collected by either the TV service provider or the online social network.

Another example of leakage may be in the form of co-habitation. It may be optional to provide an address to the online social network and two of the participants choose not to, because they prefer to keep

[7] We choose this example because the content comes from a single provider as does the advertising, which is a major part of the shared experience. This is not true of broadcast of the World Cup, but there are probably other examples from other, non-US parts of the world, where a single provider is sourcing mixed content to a huge audience, that could be targeted more individually with the appropriate technology.

their co-habitation private. From observing that the TV service delivery in the social TV application is to the same TV customer location, it is easy to derive that they live together. The users may not have limited access to their home address information in the online social network, because they knew they were not providing it, but the social TV application may have inferred it and either may keep and use that information or supply it back to the online social network.

A third leakage problem has already been mentioned, the "like" button. As reported, this is generally collected with some identifying information. In the simplest case, this may be an IP address.[8] If the user has logged in to the online social network, it is generally going to be the user's id for that online social network. This may have happened at the user's instigation, but as we mentioned above it may happen secondarily because some other application such as our social TV service uses the online social network as its identity management service. So, the user might believe that he or she is logging into the social TV service exclusively, when in fact, this includes logging into the online social network, and hence making any other "like" button activities linked to the user's online social network id.

Finally, we identify a fourth form of leakage or uncontrollable access to information about oneself having to do with profiling information about users' behaviors. This is readily available from at least some online social networks. Many online social networks let the individual set privacy constraints on attributes provided to the online social network by the user, but the online social network may collect continuous behavior information about the user such as targets of communication, frequency of communication, and content of communication. Some such services are prepared to provide or sell that information to third party services, giving the individual little or no control of that. In fact, the user may be able to delete such an account, but is unlikely to be able to delete the profiling information about him or herself to third parties, even after the account has been deleted.

V. DISCUSSION AND CONCLUSIONS

With the ever-increasing presence of the Internet in people's lives, businesses, and governance, we see a natural evolution of a new widely available service, from the originally intended capabilities, to a desire to expand opportunities. This is often driven by discovering increased value in aspects of the service that were originally only a necessary enabler, as in the larger online social networking sites. It is also beginning to happen with TV and entertainment.[9] The collection of phone companies that comprise the Telco 2.0 organization are strong proponents of the telephone companies using the information they already collect to go into the identity management business. As new kinds of service come along, if they are built on a composite of the capabilities of several of these services, we may find ourselves increasingly in the position of this simple social TV example. The challenges will multiply as the social TV service expands to product marketing, affinity organizations such as public television membership, educational services, and many others. With each new added supporting service will come a significant increase in the challenges that we saw with only two such services.

We note here that it was the intention of this paper to identify design challenges, in the simpler case, in a basic Social TV context, and to lead the reader to generalize from that to the evolving Social TV opportunities. Beyond that, the reader should also be able to generalize to the larger domain of mashup or merged application domains with many other objectives and services in mind. There is unlikely to be a single technical solution, even in the simplest case of basic Social TV service. This paper is intended to highlight design issues in order increase the probability service designers and builders will incorporate their approaches to these challenges in their products, rather than being surprised by them after the fact.

[8] If this is an IPv4 address, it will change with time and mobility, but it should be remembered that if it is an IPv6 address, there is at least one proposal on the table to include the machine's MAC address in the IPv6 address, guaranteeing an ability to link facts between different IP addresses based in the inclusion of the unique MAC address.

[9] Comcast now runs an online social networking service, Tunerfish, as well as building a merged identity system for their TV and Internet customers. Tunerfish, built on top of the Plaxo addressbook service, is intended to be a social networking site for their cable service customers.

From the discussion in the previous sections above we call out three key design elements that are worthwhile considering when building new services by adding value on top of more than one existing service: identity information, privacy, and context.

Identity information derives from a number of sources. These may include authoritatively asserted, self-declared, inferred by merging from multiple sources, observation of behaviors and actions. In other words, the provenance can be quite different for different items of identity information. It is best not to obscure the types of sources of identity information or merge them arbitrarily.

Privacy and privacy policies are gaining increasing attention, as information about individuals, especially identifying information becomes more widely collected, and merged across collections. As this information is treated increasingly as a commodity, pressures increase to minimize or violate privacy policies with respect to the information. Even, if that were not true, merging privacy policies across sets of information is much more complex than merging the information itself, and often impossible, because of contradictions among the policies. Furthermore, it is generally the case that as such information moves from one collection into another the privacy policies do not follow and hence are lost. Some form of attached privacy policies would at least make it possible to evaluate and merge policies. Without such inclusion the situation may become chaotic and untenable, as governments take on the role of regulating and enforcing privacy "frameworks".

Finally, the contexts of identity information and privacy policies about them are generally not considered, although they are often central to the definitions of those policies over that information. Even if policies remained associated with identity information as to migrated and even if the policies could be reconciled, their validity may be voided in new and previously unimagined contexts.

We conclude from this that the ramifications of design choices made by such merging and enhancement of identities through composition across multiple service domains are significant and subtle. They require not only careful reasoning about design choices, but also often supporting mechanisms that are not currently provided.

ACKNOWLEDGMENTS

The author is indebted to MIT Communications Futures Program Privacy and Security Working Group, to the corporate members especially involved in it including British Telecom, Cisco, Comcast, NSN, and Telecom Italia, and especially Jim Fenton, Natalie Klym, Jan Kok, Marie-Jose Montpetit, Tony Tauber, Hannes Tschofenig, and Dirk Trossen. This paper is an abbreviated version of a much longer working paper.

REFERENCES

[1] A. Cavoukian, "Privacy by Design: The 7 Foundational Principles", Office of the Information and Privacy Commission Ontario, Canada, Agug. 20, 2009, available from http://www.ipc.on.ca/english/Resources/Discussion-Papers/.

[2] J. Cuellar, J. Morris, D. Mulligan, J. Peterson, and J. Polk, "GEOPRIV Requirements", IETF RFC 3693, Feb. 2004.

[3] Dept. of Commerce Internet Policy Task Force, "Commercial Data Privacy and Innovation in the Internet Eceonomy: A Dynamic Policy Framework", Dec. 16, 2010.

[4] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers: Preliminary FTC Staff Report, Dec. 2010.

[5] R. D. Hof, "Searching for the Future of Television", Technology Review, Jan/Feb, 2011.

[6] InCommon, http://incommonfederation.org.

[7] N. Klym and M-J. Montpetit, “Innovation at the Edge: Social TV and Beyond”, MIT-CFP White Paper, Sept. 1, 2008, available at http://cfp.mit.edu/publications/CFP_Papers.

[8] Liberty Alliance, http://projectliberty.org.

[9] Kantara Initiative, http://kantarainitiative.org.

[10] OpenID Foundation, http://openid.net.

[11] J. Peterson, “A Presence Architecture for the Disribution of GEOPRIV Location Objects”, IETF RFC 4079, July, 2005.

[12] Shibboleth, http://shibboleth.internet2.org.

[13] K. Strandberg, “Freedom of Association in a NetworkedWorld: First Admendment Regulation of Relational Surveillance”, 49 B. C. L. Rev 741, 2009.

[14] P. Swire, “Social Networks, Privacy and Freedom of Association”, Paper from the Center for American Progress, Feb. 28, 2011, available at http://www.americanprogress.org/issues/2011/02/social_networks_privacy.html.

[15] Telco 2.0, “Manifesto”, http://www.telco2.net/manifesto.

[16] S. Warren and L. Brandeis, “The Right to Privacy”, 4 Harvard Law Review 193 (1890).