

# The TV Is Watching You

Gunnar Harboe

Motorola

1295 East Algonquin Road  
Schaumburg, IL 60196, USA

847-576-1207

gunnar.harboe@motorola.com

## ABSTRACT

There are serious privacy concerns around social television. Users' privacy may be threatened by the government, corporations, illicit intruders, and strangers. However, the most urgent privacy issues relate to people's friends and family. Users worry about how others will judge their TV viewing, and want to maintain confidence in and confidentiality of their conversations through the system. Designing for these issues involves giving users control over their self-presentation, support for multiple users, and employing constructive ambiguity.

## Categories and Subject Descriptors

H5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

## General Terms

Design, Security, Human Factors.

## Keywords

social television, privacy, TV presence, communication, porn, big brother, impersonation, ambiguity, persistence, multi-user.

## 1. INTRODUCTION

Social television, a combination of technologies that enable social experiences around TV content, is positively received by many potential users [3][10]. However, the concept also raises grave privacy concerns. In a focus group study by Motorola Labs [6], many participants sum up their privacy concerns in the term "Big Brother" and other references to *Nineteen Eighty-Four* [9]. Orwell's novel indeed features an example of social television, in the form of a combination TV set and video camera:

*The instrument (the telescreen, it was called) could be dimmed, but there was no way of shutting it off completely. [...] The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it, moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard.*

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Conference'04, Month 1–2, 2004, City, State, Country.  
Copyright 2004 ACM 1-58113-000-0/00/0004...\$5.00.

## 2. WHO WATCHES THE VIEWERS?

For users of social television, threats to their privacy come from a number of sources: government and law-enforcement, corporations, strangers, people in their social networks, and people who share the home and TV.

The government surveillance issues for Social TV are in many respects similar to those for other telecommunications technologies, such as email or telephone. In addition to the communication dimension, many social television concepts involve TV presence, which implies the ability to monitor content consumption. This can be seen as analogous to accessing library records. The conditions under which the government can legitimately monitor this information must be settled by law, but the decision is influenced by technological choices, such as where the data is stored.

Corporations are interested in the information generated by Social TV use mainly for the purpose of analytics. Sharing TV presence with a social network provides a convenient alibi for tracking TV viewing in unprecedented detail, which is valuable information for advertisers. One of the companies exploring Social TV analytics is Google [5], and its and other web companies' businesses have shown that users are willing to share their personal information in exchange for a free service, and as long as the information is used anonymously or in aggregate form.

Another consideration is that both government and corporate databases are vulnerable to leaks and intrusion. Hackers are just one example of how unknown, private individuals can pose a threat to users' privacy. Some focus group participants were worried about spammers, online stalkers, and of strangers contacting their children. There was a strong preference for limiting all communication to people already in their social network.

However, these people, the very friends and family that Social TV systems would allow users to communicate with, are also the people that participants have the most privacy concerns about. I will discuss these concerns in more detail.

## 3. WE KNOW WHAT YOU WATCH

In our focus groups, as in other studies [1],[8], the feature that caused the most unease was *television presence*, the ability to tell what others are watching on TV. The participants worried about others being able to see what they were watching at any given time. Most argued that this social transparency overstepped the boundaries of acceptability: "Would I want someone to know what I was watching? Really. It's kind of private."

Many articulated their discomfort in variations of, “I don’t watch porn, but if I did...” The more general point is that people worry about being embarrassed about their TV viewing. After all, many popular TV shows, as well as television viewing in general, are held in low regard critically and culturally. These “guilty pleasures” may therefore not reflect well on the viewer: “If someone was watching stupid shows all the time, I would think, ‘God, what a moron are *they!*’ to be watching these dumb shows.” People are also concerned that on occasion, their TV watching will be viewed as excessive: “They’d be like, ‘All you did was watch TV. Look at that! Ten hours...’”

In later field studies [6][7][12], the live television presence did not prove to be particularly problematic, perhaps because participants were able to log off if they wished to watch something in private. However, many felt that a *viewing history* feature, logging all the TV programs watched, was too intrusive: “It’s not really personal information, but it’s not information required for anyone else to know. [...] I don’t think people would feel comfortable knowing what other people have watched.”

#### 4. WE KNOW WHAT YOU SAY

The field studies also exposed another problem: the confidentiality of (and the confidence participants could have in) communications via the system. There were numerous instances of participants being impersonated by other members of their households. In some cases they were quickly found out (“it was the way [her husband] said ‘Hey dude,’ and my sister doesn’t talk to me that way”), while in other instances the other person never realized the deception. Once people recognized this potential, reactions were strong: “Oh wow, that’s scary... Heavens no! I’d be, like, angry if I knew that that happened. [...] That’s just, like, a violation of just, like, normal goodness.” “If she just pries a little bit, [...] [my girlfriend] might find out something she doesn’t necessarily need to know.”

Everyone did not share this reaction. One participant was generally unconcerned about divulging information to the wrong person, because he felt that the conversations generally centered on topics that were not particularly sensitive: “What I was saying, even if it wasn’t the person I [thought I] was talking to, I didn’t feel like it was going to hurt anything. It wasn’t anything that was sensitive information... so I wasn’t too concerned about that.” “I wasn’t giving out my social security number.”

#### 5. CONCLUSION

Although study participants have expressed worry about government surveillance (“Can you imagine, like, back in the fifties, if they were Big Brother watching what we were watching? I would hope the government now doesn’t want to come and... I mean, we don’t have anything on our TV that’s so...”), spammers and hackers, the possibility of strangers stalking them through the system, and the safety implications for their children, these are not the Social TV privacy risks that keep people up at night.

The information available through Social TV is really only meaningful to, and therefore sensitive for, people already in their social network. The threat to privacy is not Big Brother, but people’s own big brothers/sisters, significant others, and other close kin.

Addressing the privacy concerns of Social TV is an ongoing challenge. An important principle is to give the user control: for example, television presence does not appear to be too intrusive as long as users can choose to turn it off. The persistence of information is also important: while live, transient TV presence is acceptable, users object when it is available in log form as a viewing history. To provide users control of their self-presentation, ambiguity can be a useful design tool, giving users the opportunity to tell stories the way they wish [2]. Several social television systems deliberately provide presence information in a more ambiguous form, making it either less specific or more abstract and aggregated [7][11]. Finally, the fact that the television is not a single-user device, but is “public within the home” raises a number of privacy issues. Multi-user support [10] and user-identification [4] are important components of a future solution to these problems.

#### 6. ACKNOWLEDGMENTS

I’d like to thank my teammates on Motorola’s Social TV project for all their help, and for being so great to work with.

#### 7. REFERENCES

- [1] Ali-Hasan, N.F. 2008. Exploring Social Media Scenarios for the Television. In *Proc. ICWSM 2008*.
- [2] Aoki, P. M. and Woodruff, A. 2005. Making space for stories: ambiguity in the design of personal communication systems. In *Proc. CHI 2005*. ACM, New York, 181–190.
- [3] Baillie, L., Fröhlich, P., Schatz, R. 2007. Exploring Social TV. In *Proc. ITI 2007*. 215–220.
- [4] Farré, D.G. 2006. Presence-Induced Implicit Interaction and Audience Measurement in Interactive Television. In *Proc. EuroITV 2006*. ELTRUN, Athens, 105–109.
- [5] Fink, M., Covell, M., and Baluja, S. 2006. Social – and Interactive – Television: Applications Based on Real-Time Ambient Audio Identification. *Proc. EuroITV 2006*. ELTRUN, Athens, 138–146.
- [6] Harboe, G., Massey, N., Metcalf, C.J., Wheatley, D., Romano, G. 2008. The Uses of Social Television. In *Comput. Entertain.* 6, 1 (Jan 2008).
- [7] Harboe, G., Metcalf, C. J., Bentley, F., Tullio, J., Massey, N., Romano, G. 2008. Ambient Social TV: Drawing People Into a Shared Experience. In *Proc. CHI’08*. ACM, New York, 1–10.
- [8] Hess, J. 2007. Supporting Community Building in iTV Environments. In *Adjunct Proc. EuroITV 2007*. TICSP, Tampere, 129–130.
- [9] Orwell, G. 1990. *Nineteen Eighty-Four*. Penguin, London.
- [10] Regan, T. and Todd, I. 2004. Media Center Buddies: Instant Messaging around a Media Center. In *Proc. NordiCHI 2004*. 141–144.
- [11] Sokoler, T., and Svensson, M.S. 2008. PresenceRemote: Embracing Ambiguity in the Design of Social TV for Senior Citizens. In *Proc. EuroITV 2008*. Springer, Berlin, 158–162.
- [12] Tullio, J., Harboe, G, and Massey, N. 2008 Investigating the Use of Voice and Text Chat in a Social Television System. In *Proc. EuroITV 2008*. Springer, Berlin, 163–167.