A Model of Visual Privacy Concerns for PIM Systems

Kirstie Hawkey
Dept. of Electrical and Computer Engineering, University of British Columbia
4044-2332 Main Mall, Vancouver, BC, V6T 1Z4
hawkey@ece.ubc.ca

ABSTRACT
Information management is done for both personal and work-related purposes. As devices increasingly move between usage contexts and the line between work and home blurs, the same computer and the same PIM systems are often used for both personal and work purposes. Visual privacy issues can arise when these devices are used during times of collaboration; information associated with personal activities may be visible when the PIM system is used for group purposes. We developed a model of visual privacy concerns for the information that may become visible in web browser convenience features. The dispositional and situational factors that comprise this model will likely apply to privacy concerns for other PIM systems.

Author Keywords
Privacy, personal information management,

ACM Classification Keywords
H.5.3 [**Information Interfaces and Presentation**]: Group and Organization Interfaces – *Collaborative Computing, Web-based Interaction.*

INTRODUCTION

Visual privacy can be an issue when people gather in an ad hoc basis around a personal computer to collaborate on a project or share information. As they do so, a great deal of incidental information (i.e., information that is incidental to the current task) about an individual's past activities on the computer may be visible with casual inspection. This information may or may not be appropriate for the current viewing context [6]. Visual privacy concerns are usually mitigated by social norms (i.e., relying on others from openly staring at information on a display within someone's personal zone [1]). However, when viewing of the display is explicitly invited (i.e., during co-located collaboration, when giving a presentation), normative privacy does not apply. In this case, the display itself acts as an object in the collaboration. Any incidental information displayed will not only be visible, but will likely be viewed.

Presented at PIM 2008, a 2-day CHI workshop

Florence, Italy. April 5-6, 2008.

Note: This position paper summarizes work done as part of my dissertation research [3]– a full version of this work is currently under consideration for journal publication.

Visual privacy concerns may occur in personal information management (PIM) systems. Essential PIM activities include storing information, finding and re-finding information, and maintaining and managing that information [9]. Many PIM systems include advanced features to improve recognition of desired information for the end user (i.e. text snippets, thumbnails). These features can be a privacy concern as they increase the visibility of incidental information making it easier for others to see traces of previous activities with casual inspection. The use of search as a method of re-finding information may introduce additional privacy concerns. It can be difficult for users to know precisely what information will appear (as opposed to when navigating through a user defined hierarchy). This problem can be exacerbated in PIM systems that incorporate results across tasks or applications. For example, if email is included in the searched documents, personal emails about difficulties working with another person on a project may be inappropriately revealed when searching for information about the project.

One PIM system often used during co-located collaboration is a web browser. Web browsers are typically used for a wide variety of tasks, both personal and work related [6]. Web browsers have many convenience features (i.e., History, Auto Complete, Favorites/Bookmarks) that have been developed to allow users to more easily revisit content. Incidental information can be generated both through explicit user action (e.g., when information is saved in Favorites) and by the web browser itself (e.g., text stored for use in Auto Complete functions). This information may be displayed later in response to user interactions (e.g., when entering a search term, Auto Complete shows other recently entered terms). It is this display of information, incidental to the task at hand, that causes visual privacy concerns.

We have developed a contextual model of visual privacy concerns during web browsing [3,6]. Before briefly presenting this model, we first present related work examining contextual privacy concerns. We conclude with a discussion of the model's applicability to PIM systems in general.

CONTEXTUAL PRIVACY CONCERNS

Privacy concerns have been found to differ according to the viewer of the information [12]. Goffman [2] first introduced the need to project different personas or faces during social

interactions. The face presented in a given situation depends not only on the current audience but also on the current conditions. The combination of audience and situation determines how much and what information will be disclosed. Furthermore, people can have many roles between which they fluidly move and can act in multiple capacities, often simultaneously [14]. How an individual balances privacy depends on his personal situation including family life, education, social class, and psychological composition; furthermore, his needs are highly contextual and continually shift depending on situational events [15].

The impact of privacy violations depends in part on the content of what has been revealed [11]. Activities convey the essence of a persona; knowledge of an individual's prior activities is more sensitive when their identity is known as the activities can reveal hidden personae [10]. Traces of activity that are in character with the persona a user is trying to maintain [2] and are appropriate for the setting where the traces are viewed should cause little concern (e.g., non-confidential, work-related, browsing activity in the workplace). However, activities that reveal information that is not part of the persona presented (e.g., political affiliation) or that are perceived as transgressions (e.g., personal browsing if company policy does not allow it) may cause great discomfort [12].

Hutchings and Pierce [7] found that privacy issues were a factor when their participants considered how they might divide an application's interface across devices in private, semi-private, and public multi-display environments; particularly for the semi-public work environment; participants wanted to shield personal activities from their colleagues.

CONTEXTUAL MODEL OF INCIDENTAL INFORMATION PRIVACY IN WEB BROWSERS

We conducted exploratory research consisting of a survey and two field studies in order to learn more about the factors that impact privacy in this specific domain. Through the survey, we investigated how various dispositional and situational variables (potential viewers/users of the device, location, level of control retained over input devices, sensitivity of the visible content) impacted participants' inherent privacy concerns and their reported browsing activities (preliminary results presented in [6]). We also examined their actual activities and privacy levels applied through two field studies [4,5]. Triangulating the results from these studies allowed us to develop a model of incidental information privacy concerns during web browsing (Figure 1, see [3] for a full discussion of the development of this model).

This model of incidental information privacy concerns incorporates both situational and dispositional factors. Privacy comfort in a given situation depends not only on a person's disposition to privacy (i.e., their inherent privacy concerns), but also on the context of the situation. While

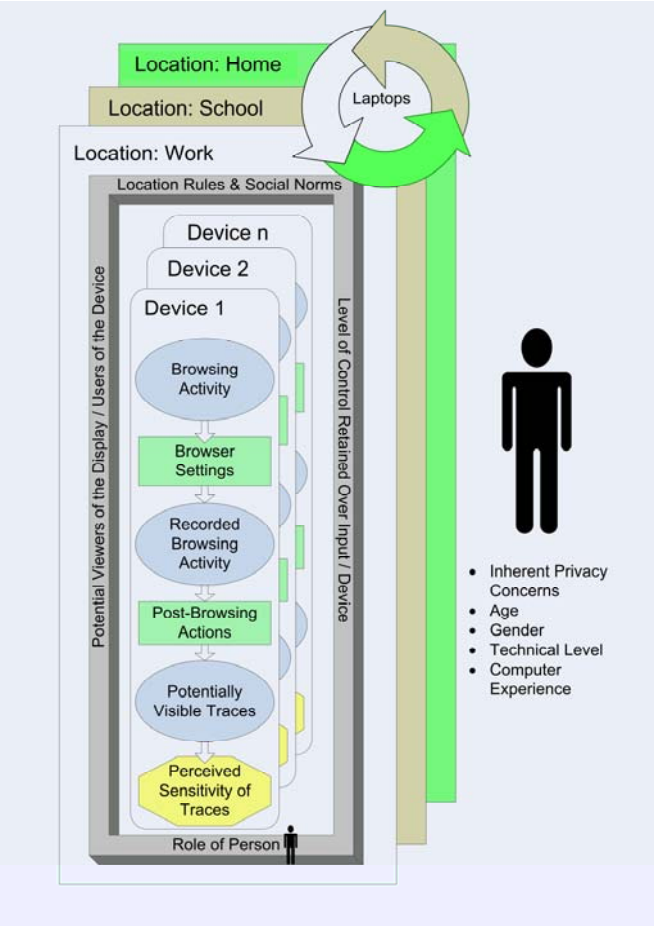

Figure 1. Contextual model of incidental information privacy concerns during web browsing.

inherent privacy concern indicates someone's overall privacy preferences, the situational context will determine what decision is made as to which information is appropriate to reveal [8,15]. The situational context included the device and location where browsing occurred, as well as potential users of the device and viewers of the display, and the level of control retained over the input devices. Furthermore the perceived sensitivity of content depends on which content is potentially visible. Which traces of browsing activities may appear in web browser convenience features depends on the browsing activities conducted, the browser settings, and any preventative actions taken prior to collaboration to safeguard privacy.

Similar to the Westin-Harris [13] privacy segmentation model, we were also able to segment survey participants by their inherent privacy concerns [6]. These segments were determined by participants' level of overall privacy concerns and the magnitude of contextual differences in those privacy concerns across the different viewing contexts (i.e., viewer, level of control, content sensitivity). *Privacy fundamentalists* are those participants with few differences according to context and low overall privacy comfort levels. *Privacy unconcerned* participants are those

with few differences according to context and high overall privacy comfort levels. *Privacy pragmatists* are those participants with high contextual differences. Privacy pragmatists were further subdivided according to their overall privacy comfort level (*wary, circumspect*) or according to which factors impact their privacy concerns (i.e., *viewer, level of control, content sensitivity*). These classifications could be used to determine suitable default settings for a privacy enhanced PIM system based upon a person's responses to a questionnaire during system initialization.

VISUAL PRIVACY CONCERNS FOR PIM SYSTEMS

The factors (Figure 1) are specific to traces of web browsing activity; however, while the nature of the visible content will change, the impact of sensitivity of the potentially visible content, level of control, viewer, and inherent privacy concerns will likely apply to other personal information management systems. For example, a desktop search PIM system will generate different types of potentially visible information and have different settings and filtering mechanisms for results. However, the sensitivity of the information which may be visible, the level of control retained over what is displayed (e.g. avoiding specific searches), the relationship to the viewer of the incidental information, and the inherent privacy concerns of the user will likely impact the privacy concerns for a given situation.

CONCLUSION

Visual privacy issues can occur when people collaborate around someone's personal computer. Our model of incidental information privacy, which includes both dispositional and situational variables, is unique in its incorporation of multiple factors specific to visual privacy concerns as well as its coverage of both privacy concerns and the activities that generate the information to be protected. Our model can be used as a guide for future study of visual privacy concerns both of incidental information within web browsers and also for other personal information management systems which may give rise to similar incidental information privacy concerns. Researchers investigating other domains, particularly those with mobile users, changing contexts, or changing user roles may find this model useful when considering potential privacy concerns.

ACKNOWLEDGMENTS

This research was conducted under the supervision of Dr. Kori Inkpen, at Dalhousie University and was funded in part by NSERC and NECTAR.

REFERENCES

1. Dourish, P., Grinter, R. E., Delgado de la Flor, J. and Joseph, M. (2004). Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing* 8: 391-401.
2. Goffman, E. (1959). The Presentation of Self in Everyday Life. Garden City, New York, Doubleday Anchor Books.
3. Hawkey, K. (2007). Managing the visual privacy of incidental information in web browsers Faculty of Computer Science. Halifax, Nova Scotia, Dalhousie University. PhD: 337.
4. Hawkey, K. and Inkpen, K. (2005). Privacy Gradients: Exploring ways to manage incidental information during co-located collaboration. Ext. Abstracts CHI 2005, ACM Press: 1431-1434.
5. Hawkey, K. and Inkpen, K. M. (2006). Examining the Content and Privacy of Web Browsing Incidental Information In *Proc. of WWW 2006*, 123-132.
6. Hawkey, K. and Inkpen, K. M. (2006). Keeping Up Appearances: Understanding the Dimensions of Incidental Information Privacy. In *Proc. of CHI 2006*, 821-830.
7. Hutchings, H. M. and Pierce, J. S. (2006). Understanding the whethers, hows, and whys of divisible interfaces. In *Proc. of AVI 2006*, 274-277.
8. Joinson, A. N., Paine, C., Reips, U.-D. and Buchanan, T. (2006). Privacy and Trust: The role of situational and dispositional variables in online disclosure. In *Proc. of Privacy, Trust, and Identity Issues for Ambient Intelligence Workshop, Pervasive 2006*, 1-6.
9. Jones, W. and Bruce, H. (2005). A Report on the NSF-Sponsored Workshop on Personal Information Management, Seattle, WA. Technical Report No.
10. Lederer, S., Mankoff, J. and Dey, A. K. (2003). Towards a Deconstruction of the Privacy Space. Workshop on Ubicomp Communities: Privacy as Boundary Negotiation, UBICOMP 2003, http://guir.berkeley.edu/pubs/ubicomp2003/privacyworkshop/papers/lederer-privacyspace.pdf
11. Margulis, S. T. (2003). Privacy as a Social Issue and Behavioral Concept. *J. Of Social Issues* 2003(59): 2.
12. Olson, J. S., Grudin, J. and Horvitz, E. (2005). A Study of Preferences for Sharing and Privacy. in CHI '05 Extended Abstracts of Human Factors in Computing Systems. Portland, Oregon, ACM: 1985-1988.
13. P&AB (2003). Consumer Privacy Attitudes: A Major Shift Since 2000 and Why. *Privacy & American Business Newsletter* 10(6): 1,3-5.
14. Palen, L. and Dourish, P. (2003). Unpacking "Privacy" for a Networked World. In *Proc. of SIGCHI Conference on Human Factors in Computing Systems*, 129-136.
15. Westin, A. F. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues* 59(2): 431-453.