PrivateBits: Managing Visual Privacy in the Web Browser

Kirstie Hawkey and Kori M. Inkpen
Faculty of Computer Science, Dalhousie University
6050 University Ave.
Halifax, NS B3H 1W5
{hawkey, inkpen} @ cs.dal.ca

ABSTRACT
Privacy can be an issue during collaboration around a personal display when previous browsing activities are visible within web browser convenience features (e.g., Auto Complete). Users currently lack means to present contextually appropriate content. This demo introduces PrivateBits, a web browser designed to help users manage their visual privacy within the web browser.

Keywords
Privacy, incidental information, web browser, collaboration.

1. INTRODUCTION
Web browsers are used in a variety of contexts, including during collaboration around a personal computer. Web browsers have several convenience features (e.g. History, Auto Complete, Favorites) that assist with page revisitation by storing traces of activity. However the information visible within these convenience features may be problematic in a group setting because the traces may reveal incidental information (i.e. information unrelated to the task at hand) that is inappropriate for the current viewing context. For example, previous search terms (personal bankruptcy laws, presentation anxiety) may be revealed to a collaborator in a Google search field when the user begins to type in their current search (privacy research).

Users lack the means to present contextually appropriate content when their displays are visible by others. To maintain privacy of their prior activities, users must currently opt to turn the convenience features off within their web browsers or clear the stored information periodically. However, those traces may be valuable for future transactions and their removal may decrease productivity. Commercial products typically allow users to clear a class of traces (e.g. Auto Complete) rather than allow selective deletion. Some tools allow users to partition their browsing into private and public activities; however, the underlying assumption is that the vast majority of items are public in nature with only a small subset needing to be password protected (i.e. pornography), and that sites of both types are never viewed concurrently.

There has been little research investigating tools for managing privacy in this domain. COLLABCLIO was developed to support automated sharing of web browsing histories [6] and provided users with a binary classification scheme (public/private) to indicate which visited URLs should be shared. Users indicated a desire for a more nuanced approach than public/private. Berry et al. [1] took a role-based approach to enable privacy in shared views of applications such as Internet Explorer (IE) and allow protection of objects within documents. For example, in the public view of an IE window, the Auto Complete options for URLs can be masked, while the presenter retains full functionality of this feature in the private view.

Copyright is held by the author/owner(s)
CSCW '06, November 4-8, 2006, Banff, Alberta, Canada

We have used a mixed methodology approach to study the visual privacy of incidental information found in web browsers. A survey examined participants' self-reported privacy concerns [5]; two week-long field studies examined participants' application of privacy levels (public, semi-public, private, don't save) to their actual web browsing [3,4]. Results from these studies provided design requirements for a privacy management system and suggested an approach for semi-automatically classifying the privacy of traces of browsing activity. As we developed our solution to this problem, we followed design principles that have emerged for privacy management systems (e.g., [6,2]) with respect to ease of creation, inspection, and modification of privacy policies, application of the privacy levels as items are encountered, and the visualization of the settings.

2. PRIVATEBITS WEB BROWSER
PrivateBits is our privacy management solution to allow users to manage their visual privacy within the browser's convenience features. PrivateBits allows the user to open browser windows of different privacy modes and to change the privacy mode of a window when the sensitivity of the visited pages changes (Figure 1). Windows in the PrivateBits browser filter previous activity appropriately and enable the automatic tagging of visited pages with the current privacy level of the window. We implemented the prototype in C# as a custom web browser that utilizes an IE browser control object.

We anticipate that the ability to have concurrent windows open with varying privacy levels will allow users to easily classify

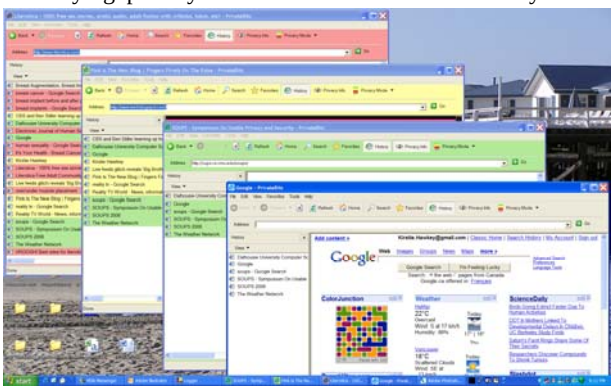

Figure 1. Screenshot of four PrivateBits browser windows open, each in a different privacy mode: (from back to front) the private (red), semi-public (yellow), and public (green) modes, as well as the public mode with no privacy feedback.

visited pages with the appropriate privacy level. Our approach capitalizes upon patterns inherent during web activity as revealed during our field studies. Participants tended to partition their activities between browser windows, with private browsing often occurring in a single window. Within each browser window, there also tended to be streaks of browsing at a given privacy level with relatively few transitions between levels [3]. While a more simple approach might have users classify each trace of new browsing manually, the rapid bursts of activity and the sheer magnitude of pages visited would make this task overly burdensome [3,4].

We used three privacy levels (public, semi-public, private) for filtering visible content. The same three levels are available for tagging generated content, along with the option to not record browsing. These multiple privacy levels provide a more nuanced approach than public/private or save/don't save. This need was evident throughout all three of our studies [3,5,4]. At any time, users may change the privacy mode of the window and can toggle between recording and not recording their browsing activity while still filtering which activity traces are visible (Figure 2, b).

A benefit to our approach is that users can specify which pages and search terms should not be saved at the time of the initial activity. During our field studies, participants tended to use the "don't save" category to indicate pages that were either inconsequential or extremely private. Allowing users to stop the recording of their activity for brief periods of time will help users remove some of the most sensitive sites from their convenience features and will also reduce the volume of irrelevant data saved.

To ensure that only contextually appropriate content is displayed, users simply set the privacy mode of the window according to their privacy comfort level in the situation. In a public window, only items classified as public are visible; in a semi-public window, items classified as public and semi-public are visible; and in a private window, all recorded items are visible. Currently items in the History, Favorites, and Auto Complete (address bar and Google search terms) are filtered; in a final version, the back and forward history lists and other form entries will be filtered.

Users can click the Privacy Info button (Figure 2, a) to toggle

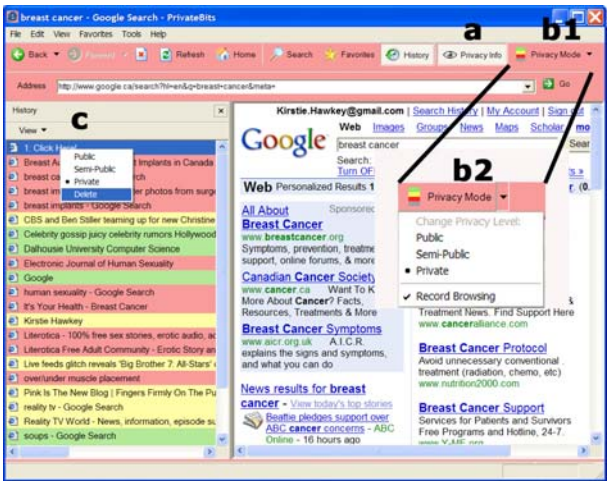

Figure 2. A PrivateBits browser window in private mode showing controls to a) view/hide privacy information visual feedback, b) change privacy mode (b2 shows the menu displayed when b1 is clicked), and c) inspect and adjust the privacy level of previously classified items.

between viewing and concealing visual feedback in the form of colour coding. The feedback indicates the current privacy level of the browser window and of previously generated traces of activity. Colours were selected using a traffic light analogy: green for public (safe), yellow for semi-public (caution), and red for private (danger). When the visual feedback is viewed, the background colour of the toolbar panels is changed as well as the window icon both on the window and in the task bar. When the visual feedback is turned off, the window appears as a normal IE window with the addition of the Privacy Info and Privacy Mode buttons.

Users can open the History panel with visual feedback enabled to check the accuracy of the classified items. The privacy level of entries can be adjusted by right clicking on the entry (Figure 2, c). Items can have their privacy level changed or be deleted entirely. Currently, this is done on a per-item basis; in a final version, the ability to select multiple items would be provided. Items can be sorted within the History panel by privacy level to quickly show which items will appear in a given browser privacy mode.

The demonstration will give conference attendees the opportunity to interact with the PrivateBits browser. Attendees can experiment with the privacy classification and subsequent filtering of the traces of their web browsing activities. We welcome feedback about the design choices made.

3. FUTURE WORK

We are currently evaluating the functionality and usability of PrivateBits with participants in a lab setting. The feedback received on our design choices will be used to refine PrivateBits. Our goal is to implement it as a tool bar with versions for both IE and FireFox. We will then conduct a longitudinal field evaluation.

4. ACKNOWLEDGEMENTS

Thanks to Ryder Ziola for software development and to the members of the EDGE Lab for their continued support. Funding provided by NSERC, NECTAR, and Dalhousie University.

5. REFERENCES

[1] Berry, L., Bartram, L. and Booth, K. S. (2005). Role-Based Policies to Control Shared Application Views. Proc. of UIST, 23-32.

[2] de Paula, R., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D., Ren, J., Rode, J. and Filho, R. S. (2005). Two Experiences Designing for Effective Security. Proc. of SOUPS, 25-34.

[3] 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.

[4] Hawkey, K. and Inkpen, K. M. (2006). Examining the Content and Privacy of Web Browsing Incidental Information Proc. of WWW 2006, 123-132.

[5] Hawkey, K. and Inkpen, K. M. (2006). Keeping up Appearances: Understanding the Dimensions of Incidental Information Privacy. Proc. of CHI 2006, 821-830.

[6] Lau, T., Etzioni, O. and Weld, D. S. (1999). Privacy Interfaces for Information Management. Communications of the ACM 42(10): 89-94.