Assessing Privacy Awareness from Browser Plugins

Aditya Marella, Chao Pan, Ziwei Hu, Florian Schaub, Blase Ur, Lorrie Faith Cranor
School of Computer Science
Carnegie Mellon University
{amarella, chaop, ziweih, fschaub, bur, lorrie}@cmu.edu

1. MOTIVATION

The rise of social networking platforms and Internet connected smartphones has increasingly exposed user's personal information. People generate and disclose vast amounts of personal information without being aware about what is being collected or who is collecting it. While previous study [2] has examined the usability aspects of browser privacy plugins; in this preliminary study, we explore the effectiveness three browser privacy plugins – Ghostery, Disconnect and DoNotTrackMe – and a placebo tool in communicating awareness about privacy risks. Malandrino et al. [3] have shown that making people aware of privacy risks could lead them to take steps to protect their privacy; Balebako et al. [1] studied the effectiveness of privacy tools for limiting behavioral advertising.

2. METHODOLOGY

We performed a between-subjects lab study with twelve participants in an interview setting. Each participant was randomly assigned one of four tools: Ghostery, DoNotTrackMe, Disconnect, and PrivacyGuard. The first three are existing privacy plugins available for Firefox and Chrome and PrivacyGuard is a placebo tool without any functionality included as a control group.

A fourth of the participants were assigned to a placebo tool in order to understand whether changes of rating are due to a psychological feeling of safety caused by the plugin. We developed a plugin (PrivacyGuard) which claims to protect user privacy but really did not have any functionality. The PrivacyGuard UI is shown in the right-most image in Figure 1. The plugin's UI has been designed to state nothing about tracking or targeted advertising. In fact it does not give any information about the plugin, beyond stating that it protects the user's privacy online.

Our lab sessions consisted of the following four phases:

1. In the first phase, participants completed searching and viewing tasks on four websites – amazon.com, nytimes.com, veoh.com and shop.com without the privacy plugin. They were asked to rate the websites on a 7-point Likert scale based on how concerned or unconcerned they were about their privacy. They were also asked to explain why they chose that rating.

2. Next, participants were asked to install the assigned privacy plugin. They were not provided with additional information beyond the plugin description. We instructed participants to familiarize themselves with the plugin in order to test the best case scenario where the user attempts to read and understand how the plugin works.

3. In the third phase, participants were asked to perform similar tasks on the same four websites. After each task, they rated the website again based on how concerned or unconcerned they were about their privacy. If they changed their rating they were asked to explain their reasons. By observing the change in the rating before and after installation of the plugin, we hope to understand the awareness gained by using the tool.

4. After completion of the tasks, participants were asked general (non-task specific) questions to understand whether the plugin was effective in changing their privacy perception on the four websites.

3. RESULTS

We observed that Ghostery was most effective (100% changed rating) in making the participants change their rating. Interestingly, PrivacyGuard did better (83% changed rating) than both DNTMe(66% changed rating) and Disconnect(66% changed rating) in making the participants change their rating. Note that Ghostery is the only plugin which shows alert notifications when it finds trackers; DNTMe shows alerts only once for a website and Disconnect does not show alerts. PrivacyGuard does not show alerts but has a short and simple description "PrivacyGuard helps protect your privacy online".

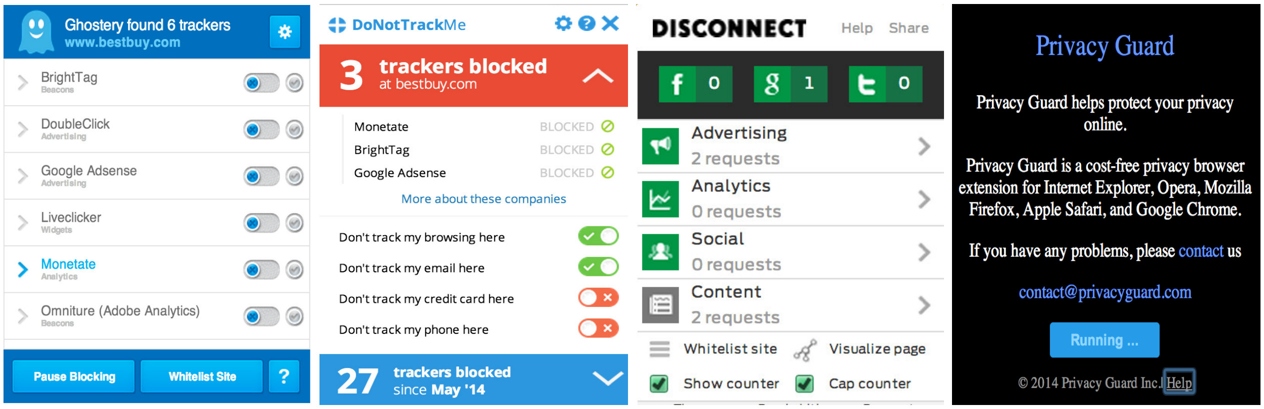
We also observed that participants using Ghostery became more concerned about their privacy while participants using DNTMe, Disconnect and PG became less concerned. This could be because Ghostery does not block the trackers by default unlike DNTMe and Disconnect. Moreover, DNTMe and Disconnect explicitly state that they block trackers in the plugin description which is reason for participants becoming less concerned after plugin installation.

Table 1 provides an overview of how ratings changed.

	GH	*DNTMe*	*DIS*	*PG*	*Total*
Amazon	3/0/0	0/2/1	0/2/1	0/2/1	3/6/3
Veoh	2/1/0	0/2/1	1/2/0	0/3/0	3/8/1
Nytimes	1/2/0	0/2/1	2/0/1	0/2/1	3/6/3
Shop	2/1/0	1/1/1	0/1/2	2/1/0	5/4/3
Total	8/4/0	1/7/4	3/5/4	2/8/2	14/24/10

Table 1: Number of participants who became (more concerned/less concerned/no change) for each website after using the privacy plugins.

The following are the main reasons for changing concern



Monetate BLOCKED

BrightTag BLOCKED

Google Adsense BLOCKED

Don't track my browsing here

Don't track my email here

Don't track my credit card here

Don't track my phone here

Advertising 2 requests

Analytics 0 requests

Social 0 requests

Content 2 requests

☑ Show counter ☑ Cap counter

Privacy Guard helps protect your privacy online.

Privacy Guard is a cost-free privacy browser extension for Internet Explorer, Opera, Mozilla Firefox, Apple Safari, and Google Chrome.

If you have any problems, please contact us

contact@privacyguard.com

© 2014 Privacy Guard Inc.

Figure 1: The four plugins evaluated in the lab study including existing privacy plugins (Ghostery, DonotTrackMe, Disconnect) and a placebo tool (PrivacyGuard).

ratings. Note that the actual reason could be a combination of multiple categories.

Number of trackers: participants became both less and more concerned when they saw more trackers on the websites. The extent of concern depended on their surprise level and prior knowledge. Some participants were less concerned because the plugin was blocking the trackers while others became more concerned because they did not think that so many trackers would be tracking them on seemingly innocuous and popular websites, such as nytimes.com.

Popularity of website: popularity of the website had a huge negative impact on the rating change. Participants were reluctant to change their rating on the popular websites amazon.com and nytimes.com. Even though veoh.com had less number of trackers than nytimes.com participants expressed less concern for nytimes.com than for veoh.com. Participants were most concerned about shop.com because it had lots of trackers and was not well known.

Placebo effect and control group: interestingly, 66% of the participants became slightly less concerned after installing the placebo plugin, although they were not sure if the tool was doing anything to protect their privacy. One participant noticed lots of advertisements and popups even after installation of the plugin and decided to keep the rating same during the last task.

Nature of task: a couple of participants changed the rating based on the search term or the type of product they were viewing. One participant found the search term 'Obama' to be more sensitive than 'business.' The same participant reported that she was not at all concerned when she searched for 'bottled water.'

4. DISCUSSION

The placebo condition (66% became less concerned) shows that the users feel secure just by installing the plugin. Given these results we cannot make any conclusive statements about the awareness gained. We are planning to expand this study with larger pool of participants to further explore areas that are unanswered from this study. Also, more exposure to the plugin will likely make the users understand the difference between a placebo tool and a real tool.

We found that only 11% of the participants gained any knowledge about the data collection and sharing practices of the trackers from the plugin and none of the participants were clear about the privacy risks associated with the data collection. Ghostery was most effective in improving awareness about data collection and sharing.

The purpose of data collection and sharing was unclear to most of the participants, 60% of participants were not sure about the purpose. The remaining participants stated marketing, advertising, recommendations and political agenda as the purpose. Among them only 11% changed their answer from not sure to advertising after using the tool.

All the plugins were reasonably effective in communicating sharing targets. 30% of the participants changed their answer on sharing targets from 'not sure' to the 'tracking companies' shown by the plugins. Interestingly, participants started speculating about sharing targets based on the search terms or the type of task they were performing.

78% of the participants did not believe they derived any benefit from the data collection. The remaining participants mentioned recommendations as the benefit.

5. CONCLUSION

In summary, our work gives a perspective on privacy awareness gained by using browser privacy plugins. We plan a followup study with more participants that will allow us to probe deeper into what features of browser plugins successfully raise privacy awareness and how these tools may be further improved.

6. REFERENCES

[1] R. Balebako, P. G. Leon, R. Shay, B. Ur, Y. Wang, and L. F. Cranor. Measuring the effectiveness of privacy tools for limiting behavioral advertising. In *Proc. W2SP*, 2012.

[2] P. G. Leon, B. Ur, R. Shay, Y. Wang, R. Balebako, and L. F. Cranor. Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising. In *Proc. CHI*, 2012.

[3] D. Malandrino, V. Scarano, and R. Spinelli. How increased awareness can impact attitudes and behaviors toward online privacy protection. In *Proc. SocialCom*, 2013.