Interface Application Comprehensive Analysis of Ghostery

Dan Bouhnik, Golan Carmi
Jerusalem College of Technology, Israel
bouhnik@jct.ac.il, carmi@jct.ac.il

Abstract

The object of this study is to analyze the Ghostery extension's interface. This app is a browser extension, which allows users to block tracking mechanisms found on web pages. The interface analysis will be performed in two parts: At first, a general overview of the extension's implementation and usage. The second level will be a heuristic analysis according to Shneiderman's 'Eight Golden Rules of Interface Design'. The overall analysis will show that despite having a high level of aesthetics and minimalism, the app is not accessible to the end user and contains too many options to choose from. Moreover, the analysis shows that without prior knowledge or an ardent desire to learn using the app may cause frustration for the end user and possibly lead to errors.

Keywords: Ghostery, Interface Application.

I. INTRODUCTION AND RELATED WORK

Many tracking measures exist on the internet, which violate user privacy by collecting data regarding user browsing habits as well as personal information. These measures offer advertising and marketing body's broad access to personal data, storage and distribution. (Shwartz-Altshuler, 2012). Website owners can assimilate data collection technologies which document surfer's activity on their sites. Similarly, advertisers are able to reach wide, specific and segmented audiences, thus increasing their profits. Frequently the average internet user is not aware of the data collection regarding his usage patterns, and so he unknowingly actually waives his privacy rights. The publication and advertising mechanisms are aware of this ignorance and take advantage of it. The most popular data collection method uses cookies. A cookie is a text file which is saved by the server on the user's hard disc on the internet. Cookies perform management activities which assist internet sites to maintain data regarding the user's status or to document his actions.

Originally, cookies were intended for user identification purposes and to notify the site server when a user returned to the site. The identification process takes place when the server identifies the user by accessing the data stored previously in the cookie. Initially, the user identification process focused on the users benefit and was meant to help him save data regarding the items chosen by him when making online purchases. In other words, the cookies were first developed to serve as a 'shopping cart' which save the users' data on shopping sites, a usage which is still widespread today (Hormozi, 2005).

Cookies and other tracking measures are received by the browser during the session between the browser and the server in Hypertext Transfer Protocol (HTTP). The communication process between the browser and the server in HTTP includes requests sent by the browser and replies sent by the server. During an HTTP session the browser requests the server to send it the internet page with all its components. If the internet page includes links to different sources which include tracking measures, such as cookies, those sources will also be sent (Grysiuk, 2015). Over time, the use of cookies expanded beyond the original intent. The use of cookies now deviates from personal adaption which benefits the user and are stored on the users' computers without their consent or awareness. Cookies have become quite controversial as they arise many privacy concerns. They are currently used by advertisers and marketers to collect personal data regarding the user and for tracking his surfing activity on the net, which may even include the route through which he visits the site and the time he spent in the site. Third party cookies allow the combination of cookies from several sites in order to create specific user profiles and to facilitate data base storage.

Whilst violating the users' privacy, cookies grant various parties - the user, the site developer, the advertiser and the publisher - many advantages. Some internet site activities, such as on-line ordering, internet site tracking and identification of user, depend on cookies. In addition, cookies allow personal customization of the internet site. As cookies 'remember' the user's data, future visits to the site can be made more efficient and pleasant. When the site 'remembers' the user's preferences, there is no need to ask the user again for all the data required for a specific operation, thus saving the user time and energy. (Birnhak, 2009).

Cookies are used by internet developers for statistical analysis of the site usage data such as: number of visitors, frequency of visits and the ratio of returning visitors and new visitors. Storing and analyzing the data which has been collected in the data base, enables the developer to an efficient website. Upon his first visit to a website, the user is assigned an identifier, which is stored in the cookie file. When the user returns, the site identifies it as a return visit. This process repeats itself for every site visitor. Besides identification of users, cookies are also used for tracing the user's route during his visit to the site. Knowledge of the sites visited by the user, allows the developers to focus on
Several studies have found that the browser applications for control over his exposure to advertising firms and tracking applications increase the user's awareness level and his what data he would like to protect. In addition, the surfing sessions. Some applications activate default tracking measures and advertisements during internet protection and personal data security by blocking unwanted protection are included in the definitions of the browser in designated to preventing tracking.

Advertisements and marketers use cookies to collect data related to the user and accordingly determine the advertisements to be presented to a specific user. When users see an ad from a specific server for the first time, the internet browser receives a unique identifier which is saved together with the other cookie files. When the user visits a site which contains advertisements from that server, the cookie is used for presenting the most suitable advertisement, based on the interest of the user. This data can be collected both actively and passively, by tracing the sites which the user visited, the ads that were clicked on for further information, items purchased and forms completed over the internet. Cookies also enable to determine the efficiency of the advertisements on internet sites. When a user clicks on an ad which collects data through cookies, the advertisement operator tracks the user to the site to which he has been directed. Clicking on a specific advertisement also helps to map and establish the interest realms of the user. With this information, the advertiser may decide upon the best choice of advertisements to present to the user (Abdulhayoglu, 2008, Mansfield-Devine, 2014).

The increasing concern regarding privacy and the wish to protect data and ones' personal identity raises resistance to organizations which collect data and use it for marketing and advertising purposes without the users' consent. A study held in the U.S. in 2009 showed that 87% of the participants do not want to receive ads which are based on tracking (Mayer & Mitchell, 2012). In an Israeli based study, the participants stated that they avoid using a single connection measure due to privacy and data security concerns (Gafni & Nissim, 2014). Users' objection to tracking bodies is expressed both in avoidance of tools which may have security issues and in actively using tools designated to preventing tracking.

Simple measures for data security and privacy protection are included in the definitions of the browser in the form of a ‘Do Not Track’ mechanism, which sends the internet servers of the sites visited by the user a message that the user is not interested in tracking. However, the site operator does not have to acknowledge the request. Other active measures include browser applications, which may be installed by the user as an extension to the browser. The software provides enhanced capabilities for privacy protection and personal data security by blocking unwanted tracking measures and advertisements during internet surfing sessions. Some applications activate default security definitions, while others allow the user to decide what data he would like to protect. In addition, the applications increase the user's awareness level and his control over his exposure to advertising firms and tracking. Several studies have found that the browser applications for user privacy protection and data security improve the user experience, both in terms of loading speed of internet pages and the user's sense of security sense while surfing, as well (Ajdari et al, 2013; Marella et al, 2014).

A study which examined the usefulness of privacy protection applications among average users, found that many applications are automated and not open to personal adaptation. Even those which enable customization do not always provide enough information in order to allow informed decisions. Differences between various tracking measures are not always clear, either because of a lack of information or the inability to understand relevant information. The users also expressed their dissatisfaction regarding the distraction caused by the applications while surfing the internet and stated that the user's interface was confusing and inconvenient (Constantin, 2015, Leon et al, 2011).

Carmi & Bouhnik (2016) analyzed and compared the performance of four common security applications – Privacy Badger, Disconnect, Ghostery and Privdog. Of the four, Ghostery was found to offer the most control over the process of tracking and blocking cookies, the others relying heavily, if not completely, on atomization, i.e. automatic blocking of all cookies. Ghostery allows the user complete control over the process, allowing him to decide for himself which tracking measures he wishes to block. In view of Ghostery's unique approach, we wish to make an in-depth analysis of Ghostery's interface.

II. GENERAL OVERVIEW

Ghostery presents the user with the tracking and monitoring mechanisms detected on every web page visited. Based on this information, the user can decide which of those mechanisms to block or to permit. In addition, the user can decide in advance to block all types of tracking mechanisms sweeping, or to block just a part of them based on specific categories.

After installing the extension, an initial settings screen pops up. This screen consists of several slides, which the user can browse through. The first slide is an introduction slide, providing background information about the extension, clarifies the menu and provides an email address for support. The second slide offers the user to send anonymous information to Ghostery Company, regarding tracking mechanisms detected during use. The third slide allows the user to enable the Purple Boxwindow
display, which contains the tracking mechanisms detected by the extension on a specific page. In that Purple Box, the end user will be able to select the different categories of tracking mechanisms to be blocked or to be permitted. There are 5 categories: Advertising, Analytics, Beacons, Privacy, and Widgets. An explanatory bubble appears when hovering above each category’s name. The last slide notifies the user that the initial setting process has been completed, and the extension is now ready to be used. An advanced user may skip this entire initial setup, and configure the settings directly at the extension's options menu.

The extension options menu consists of three tabs: General, Advanced and About. The General tab contains an option to choose whether or not to send anonymous information collected by the extension to Ghostery Company; an option to enable automatic updates of the Ghostery trackers library; and a blocking option, which can be done in two ways: by category, or by adding sites (or pages) to a 'white list' which Ghostery extension won't block any tracking mechanisms detected within. The Advanced tab contains displaying options for: the popped-up Purple Box, the tracker URL patterns, the Ghostery extension icon on the browser’s toolbar, and the extension’s notifications on the browser. Other options included in the Advanced tab are: blocking first party tracking mechanisms (meaning allow trackers created by site owners); blocking by default newly added trackers by the Ghostery library (while notifying the end user about the changes that were made); replacing blocked content by a button that enables the user to temporarily allow that content; replacing blocked social media buttons (such as Facebook’s Like and Share buttons or Twitter’s Tweet button) with a Ghostery icon. Also on that tab, the user can set the interface language and export/import settings (for backup).

The main user interface of this extension is a browser toolbar menu. This menu acts as a findings panel, where the user can view and control the blocked trackers. When shifting the sliding button to the right, it changes to red, meaning that this tracker is blocked from now on that specific site (shifting left- blued- permits it). A tracker can be permanently permitted, by clicking the checkbox on the right of the sliding button (making it a green check). It is possible to temporarily pause blocking by clicking the “Pause Blocking” button at the bottom of the panel (making the sliding buttons yellow). In addition, the user can add the current site to the ‘white list’ (making the sliding buttons green). The settings button located on the upper right corner of the findings panel opens up a menu with four options: switching to the options menu; browsing to the extension’s support forum; answering up a satisfaction survey; and online sharing of the extension with several social networks. The help button at the lower right corner, will direct the user to a tutorial.

There are many other browser extensions aiming for the same objective as Ghostery. The Privacy Badger extension can also block tracking and monitoring mechanisms. Privacy Badger is based on much higher automation than Ghostery. It studies the trackers code snippets’ behavior and makes decisions accordingly on behalf of the user. Another similar extension is Disconnect, which has a stricter policy than Ghostery. Disconnect blocks all categories by default and then allows the user to enable specific trackers.

**Figure 2- Options Menu Tabs**

**Figure 3- Findings Panel**

Ghostery is basically an extension for securing the user’s personal information. The way Ghostery chose to do so is by educating the user about the vast monitoring and tracking mechanisms on web pages. The Ghostery approach can be described as: "Knowledge combined with Control means Privacy". This way, a user browsing a web page will be presented with all of the page’s monitoring and tracking elements, alongside the option to block them. Ghostery provides the essential knowledge required to the user in order to "Take Control of the Digital Experience" (from the company slogan).

In terms of the user’s needs, Ghostery is actually trying to preform two somewhat contradicting actions: On the one hand, it is trying to protect the surfer’s privacy without to much bother, while on the other hand it is trying to educate about privacy issues. Within that contradiction Ghostery operates in a few different ways: temporarily pausing blockage of trackers; permanently stopping blockage of trackers; and blocking trackers by category. For further explanation, we will use the following example: a commonly used tracker is the Disqus commenting system.
This commenting system allows site owners to easily add an area on the web page, containing a text box where the users can post their comments. On a back panel, this system collects all of those comments (from wherever the system operates) and groups them together by the individual users while creating a profile for each. In fact, the system serves the user's needs, whereas one can claim that it also violates the user's privacy at the same time. When this commenting system appears on a page and Ghostery blocks it, it actually replaces that area on the web page (containing the system), with a caption: 'Ghostery blocked comments powered by Disqus'. Two triangular buttons are added next to the Ghostery logo: the first button is marked with a rounded circle containing the digit '1', and the second button is marked with two arrows compounding a round circle. An explanatory bubble appears when hovering overeach button. The first button will unblock and permit the use of the system only for this instance. The second button will permit the use of this system permanently. By enabling the system's operation, the user's browsing experience is not impaired. Moreover, the user can decide to permit 'useful tools' category (which consists of tracking systems such as this). Just a reminder, the user can also permit all of the trackers on a specific page, by adding it to the 'white list'.

![Ghostery blocked comments powered by Disqus](image)

**Figure 4 - A blocked Disqus commenting system**

This example reveals the main issue for Ghostery in terms of user's needs. On the one hand, the extension enables the user extensive control over blocking trackers mechanisms: temporary blockage, permanent blockage, blockage by category and the use of a 'white list'; On the other hand, the user must be well-versed in all the extension available options and understand the implications of each of them. Also, the user must fully understand the contents of each category or mechanism, to make the right decision in a given situation. In Ghostery's defense it should be noted that it provides all of the information needed, however most users won't bother to thoroughly read the detailed instructions.

Therefore, it can be argued that the Ghostery target audience are users who want to expand their knowledge about privacy, are willing to thoroughly explore every option this extension has to offer, and would read every piece of information within it. Perhaps this target audience is not what Ghostery Company aims for; rather than the mere outcome of Ghostery developers' way of thinking. We believe that the developers had in mind advanced users who want to expand their knowledge about privacy.

III. HEURISTIC ANALYSIS

Beyond the general analysis presented above, we would like to analyze Ghostery using Shneiderman's 'Eight Golden Rules of Interface Design', which are: Strive for consistency; Offer informative feedback; Prevent errors; Support internal locus of control; Cater to universal usability; Reduce short-term memory load; Enable frequent users to use shortcuts; and Aesthetic and slim design.

'Striving for consistency'- Ghostery displays three different menus: the findings panel; the Purple Box that pops-up when the extension detects a tracker; and the Options menu. In terms of trackers' blockage, the findings panel contains settings that overlap with those of the Options menu. Whereas the findings panel also lists all of the trackers detected in the current web page, the Options menu, on the other hand, displays more advanced options, which donot appear on the findings panel. The Purple Box also shows the same results listed on the findings panel. In our opinion, the multi-menus, each with a different design and displaying slightly different information, contravenes the principle of striving for consistency.

'Informative Feedback' is carried out properly in Ghostery. Each user's action at the findings panel will lead to a corresponding interface gesture, such as changing the button's color and/or changing its position, so the user is well aware that the demanded action has occurred. In addition, when accessing a web page, there are two indicators that the extension is functioning properly: the first indicator is the Ghostery logo icon, displayed at the browser's toolbar, with a counter representing the numbers of trackers identified on the web page; the second indicator is the popped-up Purple Box, displaying the various tracking or monitoring mechanisms detected on the page. When blocking a tracker, its title will appear at the Purple Box with a strikethrough. This way the user can easily see how many trackers detected on that page, their title and which of them are blocked or permitted. However, it should be noted that the Purple Box window does not contain an explanation about its contents, nor a header which identifies it as a part of the Ghostery extension. The trackers titles are shown (in the Purple Box) without any clarification regarding their behavior.

'Preventing Errors'- the interface designers' efforts in this area are very noticeable. The entire interface input fields are from 'Markup Class', so the user cannot type in any data at all. This prevents entering incorrect input, such as alphabetic characters in numeric entry fields. Moreover, all users' actions are easily reversible by clicking a single button. Nevertheless, the extension lacks notifications to the end user regarding changes that are going to be carried out, and awaiting approval to commit those operations. Thus, any user action is executed immediately. An exception is in the case of cancellation of all of the blockages; such action requires refreshing the web page, which can be done by clicking the corresponding button shown to the user (after choosing this action).

'Supporting Internal Locus of Control' is at the essence of the extension. Ghostery gives the user control over many options: a temporary blockage option; a permanent blockage option; an option to add a page to the 'white list' (permitting all of the trackers on that page); an option to block a category; an option to permit specific trackers on a specific page; and an option to temporarily permit all trackers on a single page. However, as mentioned above, controlling all of those options requires prior knowledge and subject to familiarity with the Ghostery extension.
In terms of 'Catering to Universal Usability', the extension uses familiar and well-known metaphors. There are nine types of buttons, while eight of which use metaphors: check box, sliding button, green check button, question mark (help) button, gear knob (settings) button, blockage sign button, playback button, and a caption button. A checkbox is often used at the Options menu, when the user wishes to apply or change a setting for a tracker. The slider button and the green check button are displayed at the findings panel, where the user can change a definition of a specific tracker. The question mark (help) button and gear knob (settings) button at the findings panel directing the user to other menus: the help button switches the findings panel window with a tutorial window, presenting descriptions regarding this findings panel; the settings button displays a menu with additional captioned buttons, such as switching to the options menu. The playback button and the blockage sign button appear on the web page body, only in case it contains blocked tracker content. The caption buttons appear in various locations throughout the findings panel and on the advanced Options menu. Some buttons use well known metaphors, such as: gear knob (for settings); question mark (for help); and check boxes, whereas other buttons use unique gestures or signs, exclusively with this extension, such as the blockage sign button and the playback button. The last is shown with the digit ‘1’ or with two arrows creating a rounded circle, which without explanatory captions, is difficult to understand their meaning. The most challenging interface involves the color metaphor used on the slider buttons and the green check button. The slider background varies between four different colors: blue, red, green and yellow. Blue marks a permitted tracker; red is for blocked tracker; green means that that tracker is always permitted; and yellow is for a temporarily permitted tracker. On top of all that, there is also the green check button used when enabling a specific tracker on a specific site. Hence, there are confusing colors in use (such as blue and yellow) which are not well-known metaphors, alongside a duplicate use of the green color.

'Reducing Short-Term Memory Load' is not quite accomplished due to the many buttons' classes, with various types of activities. That kind of variation makes it harder for the user to select the correct action, as there is obligatory use of memory. When hovering over each button, there is an explanatory caption bubble that clarifies the meaning of it. Using this kind of clarification indicates that the developers had to compensate the minimalism of their interface and by that actually admitting that it is not intuitive enough.

There is very little 'Use of Shortcuts for Frequent Users'. The only place where there is a use of a shortcut is when a tracker is blocked, which will make the playback button appear over the blocked area. This limited usage of shortcuts is peculiar, since obviously Ghostery is an extension used by experts, who are by definition frequent users that will generally appreciate having shortcuts. Other evidence of this is the lack of automation for decisions making- all of the settings are for the user to decide (rather than being partly determined automatically by the extension).

Regarding the 'Aesthetic and Slim Design', there is a considerable effort on behalf of the interface designers. The blue color dominating the extension is pleasant and its interface is well-designed. In addition, there are very few windows, while more advanced and less common options are on a separate menu. This way, the user is not bombarded with unnecessary information and is able to distinguish between the principal and secondary content over the different menus.

Consolidating all of the options into the findings panel could greatly contribute to improving the interface. In that manner, the Purple Box would be displayed on the browser toolbar, rather than at the bottom corner. The Options menu would be a part of the findings panel, but on a different level of displaying (like an added menu that would be revealed after clicking a dedicated button). This change would also be accompanied with some menu design adjustments. For example, the Purple Box will no longer be purple, but rather designed in the same way as the findings panel. Adding keyboard shortcuts for commonly used actions, such as pause blocking, can contribute significantly to frequent users while working with this extension. Another improvement proposed, is an automated reload of page after pause blocking, which would save the manual reload and decrease the numbers of clicks. Additionally, using more familiar colors for the sliding buttons and more approval notifications after changing an advanced feature, would greatly improve Ghostery's user interface. We are not convinced that adding a layer of automation to Ghostery will contribute to its functionality, since the whole purpose of this extension is to give users control over definitions and educate them about digital privacy. An added automation layer or automated decision-making mechanism to the extension will cause it to lose its uniqueness.

IV. EXPERTS

We set up a heuristic experts group, in order to assess Ghostery user interface. The meeting consisted of four experts, two women and two men, who are well proficient with the heuristics rules. Each expert was asked to install the extension on the PC, pass through the initial settings screen and perform basic tasks using the extension, all without any specific instructions. The basic tasks were to permit or block a specific tracker mechanism; to permit or block a category; to cancel the displaying of the Purple Box; and to browse a news website. The purpose of those tasks was to motivate the experts to use the extension and to explore its possibilities. Browsing a news website was selected, because such websites contain many active trackers and monitoring mechanisms in their pages’ codes, which support their business models. Some of the experts carried out additional tasks after completing the basic ones. At the end, the experts were asked to give feedbacks whilst following the heuristic rules.

Regarding 'strive for consistency'- the experts reported that they believe that "there is consistency in design and colors", but one expert reported that the fact that the Option menu can be accessed both from the Purple Box and the findings panel “is problematic, since the user might think that those are different settings for each window” (whereas they’re the same). Three of the four experts used the settings button (which leads to the Options menu) that is placed at the Purple Box window rather than the one within
the findings panel. This caused an error for one of the experts who reported that "I did not know how to return to the options menu, since I blocked the Purple Box". The experts were pleased with the 'Informative feedback' given to them by the extension. The experts were also pleased with the check boxes as well as the sliding buttons, informing them about a successful execution. One expert reported that when she pressed the playback button (for a blocked Facebook recommendation button) within an article, that button gave her no feedback about what will happen, and she ended up recommending an article without any intention to do so. Concerning 'preventing errors', the experts stated that the initial settings window, that appears after installing the extension, may contribute to the users understanding of how to work with the extension, "but it cannot be inferred that this is what an average user will necessarily understand". Also, the experts stated that the extension enables a clear choice between the different kinds of trackers blockage. In that matter, they reported that the lack of prior knowledge regarding the different terms used by the extension, adversely impacted their performance. The experts confirmed that the extension supports internal focus of control by easily allowing control and enables the "undo/redo of any action. If I canceled the blockage, I can simply undo this". Another expert said that the extension is "easy to handle". The experts complained about not 'catering to universal usability', and mentioned the usage of then on-intuitive blue color with the sliding buttons, as an example. Yet another expert considered this to be slightly intuitive, as he associated the blue color to the cold faucet water, and the red to the hot faucet water. The experts reported that the extension is 'reducing short-term memory load', as "it is possible to understand how the extension works, even without reading the instructions". Having said that, one expert attempted to work also with a touch screen PC, and reported that without using the mouse there are no explanatory caption bubbles and therefore he had some difficulties carrying out some of the actions. Regarding 'use of shortcuts for frequent users' - One of the experts reported that the findings panel is a shortcut to the advanced settings menu, and that the use of categories can also be considered as a shortcut. Another expert mentioned that although the extension has 'aesthetic and slim design', it is not minimalistic in terms of the many possibilities and options it offers.

V. DISCUSSION AND CONCLUSIONS

The experts claim that the extension is easy to use, but requires thorough understanding. We tend to agree with this argument, as we believe this is a key issue of Ghostery. The average user, who is unfamiliar with the diverse types of monitoring or tracking mechanisms, won't enjoy the full potential of the many advantages and possibilities this extension has to offer. Moreover, there is a duplication of menus within the extension. This duplication is complicated for the user, who does not take into account that two different menus may serve the same purpose, and that there is an easier way to perform a requested task. An example for that may be found with that expert, who canceled the display of the Purple Box window and then did not understand how to return to the Options menu.

Another issue is the use of explanatory caption bubbles (tool tips). In our opinion, the vast usage of this method is a clear sign that the extension is not intuitive enough, and that the usage of known metaphors has failed. As mentioned before, one of the experts has pointed out that while working with a touch screen (when no mouse is present) those captions are worthless, as the hovering option is not relevant, hence the caption bubbles won't appear. There are two possible ways to improve this matter: the first is to use explanatory text alongside its corresponding icon; the second possibility is to use more obvious and clearer metaphors.

VI. SUMMARY

Ghostery is a menu interfaced extension for blockage of tracking and monitoring mechanisms, intended to keep user privacy and awareness. However, the average end user will probably not be able to fully enjoy its benefits due to its interface design which targets advanced users. As of today, there are many extensions similar to Ghostery, and their number just keeps increasing with time. Therefore, it is crucial that Ghostery improve its interface to accommodate larger audience.

Ghostery developers and designers should focus on creating a more accessible interface to a wider range of audience. In that way the Company will achieve its objective to educate users about privacy issues. Personally, we have been using Ghostery for a long time now, but as an information and data security professional, we don’t experience the average end user’s difficulties. This study, in which we analyzed the Ghostery user interface together with other experts (who are not data security professionals), revealed to us the blind spots it has, and has given us a deeper understanding of the end users.

REFERENCES


