Functional Analysis of Applications for Data Security and for Surfing Privacy Protection in the Internet

Article · July 2016

CITATION
1

READS
103

2 authors:

Golan Carmi
Jerusalem College of Technology
29 PUBLICATIONS **29** CITATIONS
SEE PROFILE

Dan Bouhnik
Jerusalem College of Technology
37 PUBLICATIONS **597** CITATIONS
SEE PROFILE

International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 7 201 - 208

Functional Analysis of Applications for Data Security and for Surfing Privacy Protection in the Internet

Golan Carmi[1] and Dan Bouhnik[1,2]
[1]Faculty of Management, Jerusalem College of Technology, Jerusalem, Israel
[2]Department of Information Sciences, Bar-Ilan University, Ramat Gan, Israel
Email [1]carmi@jct.ac.il, [2]bouhnik@jct.ac.il

Abstract:-Browser applications for the purpose of data security and surfing privacy allow the blockage of tracking measures and data collection regarding the user activity on the Internet. This article analyses the function of four common data security and privacy applications in the internet: Privacy Badger; Disconnect; Ghostery; and Privdog. The content analysis includes three aspects: functional activity, user interface design and economic-financial sources. The results show that in spite of the functional similarity between the applications, each application has its own unique approach for maintaining privacy and each acts in a different way and on different levels to secure the user data on the internet.

Keywords: *data security; user privacy; cookies; internet tracking; internet advertizing blocking*

*****

Introduction

There are currently many tracking measures on the internet which collect data and penetrate user privacy on the internet. These measures offer advertising and marketing bodies broad access to personal data, storage and distribution. The broader the internet activity becomes, the more intense the involvement of the site owners, as well as third parties who can make money by sharing information collected by them regarding the users (Shwartz-Altshuler, 2012). Site owners can assimilate data collection technologies which document the surfers 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 the ignorance of some of the users and take advantage of it. Different organizations have developed applications for browsers which are designated for increasing data security and user privacy on the internet.

The main collection technology today is the cookie. The cookie allows the internet site to save data on the user's computer and to retrieve it later. The source of the word 'cookie' is the phrase 'Magic Cookie' which is used in programming languages to describe data shared by software components which work together. A cookie is a text file which is saved by the server on the user's hard disc on the internet. Cookies perform situation management activities which assist internet sites to maintain data regarding the user's status or to document his actions. Cookies include fields which define the use which can be made of the cookie files by the server. The cookie includes mandatory fields which serve as a measure for providing data for the server (Mayer, 2011). For instance, a name field which contains the cookie name, and a value field which contains the data to be kept by the server on the hard disc.

Besides the mandatory fields the cookie includes optional fields which include data which limits the server usage of the cookie. The limiting optional fields include for instance: expiration date, route and domain. The expiration date field specifies when the cookie will be deleted. If no date is specified, the cookie will be deleted upon termination of communication between the browser and the server. The route field includes the URL in which the cookie is valid for use by the site, so that the internet pages which are not included in this route cannot read or use the cookie. The domain field includes a full or a partial domain name which indicates the cookie validity. The browser will return the cookie to every computer which is compatible with part of the domain name. When the domain name is not specified, the cookie is returned to the server in which it was created. In addition to these fields, a field exists which specifies whether the cookie is protected, an option which indicates that the cookie can be used only if the server is protected (Hormozi, 2005).

When cookies were first developed they were not intended to be used as a surveillance means to track user activity on the internet for advertising and marketing purposes. They were originally 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 in his online purchases on the internet. 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 HTTP protocol (Hypertext Transfer Protocol). The communication process between the browser and the server in HTTP includes requests sent by the browser and replies sent by the server. Thus, 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. There are various types of cookies:

* Session Cookies – are saved in a temporary memory and are deleted when the browser is shut down by the user. They include a session identification field and serve to preserve the connection between the user and the site.
* Persistent Cookies - are saved over time and are not deleted when the user closes the browser. Their termination

is determined by their expiration date, defined by the server or by the user, who may manually delete them.

* First-Party Cookies – are saved on the user's hard disc by the site he has visited.

* Third-Party Cookies – are saved on the user's hard disc after clicking on an advertisement or upon entering content which is stored in a third party's site.

* Flash Cookies – are called 'locally stored object' and their goal is to improve the functioning of Adobe Flash. They can perform any activity executed by a standard cookie, but include a wider range of information and, in comparison with other cookies which are stored in a different file for each browser, they are not controlled or limited by the browser and thus are accessible by different browsers in the user's computer. The data which is saved on them is application-based, so very diverse information can be received. These characteristics are the reason for treating Flash Cookies as Super Cookies.

* Evercookies - are based on a technology named Persistent Identification Element, which was developed by United Virtualties. This technology is used for creating or transferring the cookie to a different location than that which is usually used to store cookies in the user's computer. In fact, the cookies are stored in several locations on the user's hard disc along with a unique identifier which connects the locations. If a user deletes the cookie in one location, the Evercookies mechanism detects the deletion and creates the cookie anew. Thus, the average user is not able to delete the cookies and their removal can be frustrating even to more sophisticated users. The Evercookies use a combination of JavaScript, Flash and other technologies in order to achieve their goal (Mayer & Mitchell, 2012).

In addition to cookies, there are other measures which are designated for tracking user activity on the internet, such as:

* Web Bug – a small image file which is assimilated in HTML code. When the user enters an internet page which includes Web Bug, an HTTP request is sent to the server, which documents the request and stores it. Web Bugs are mainly used by third party advertisers for analysis of traffic to their site and for improving their advertising quality. When a Web Bug is combined with cookies, it helps the advertiser to build a unique profile of the user.

* Device Finger Printing – is used for collecting online data in real time from cellular phones, tablets and other portable devices. Through identification of the devices unique characteristics are collected, such as: the operating system type, screen resolution, mouse location on the screen, domain server, stored cookie type and more (Grysiuk, 2015).

As aforesaid, with the advancement of the internet, the use of cookies expanded beyond the original intent and became controversial regarding the protection of personal data and the privacy limits of the users on the internet. The use of cookies deviates from personal adaption which benefits the user and are stored on the users' computers without their consent or awareness. 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.

Despite the violation of user privacy, cookies grant the user, the site developer, the advertiser and the publisher diversified advantages. Some of the internet site operations are not possible without cookies, such as: on line ordering, internet site tracking and identification of user. In addition, cookies allow personal customization of the internet site. The user's name may appear upon entering the site or one may define what one would like to have appear or not appear in the site. Since cookies 'remember' the user's data for future use, they can save him precious time. 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. As a consequence, future visits to the site are more efficient (Birnhak, 2007).

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, enable the developer to plan and update the site content efficiently. Each user is assigned an identifier when he first visits the internet site. This identifier is stored in the cookie file which is stored with the user. 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 in the site. This procedure does not take place in order to spy on the user, but rather in order to supply data to the site developers. Knowing where the user visited, allows the developers to focus on those pages and to present them to the user in a shorter or a more friendly way. Similarly, data regarding those pages in which the user does not visit can also be traced in order to determine whether there is a problem with the content or the design of those pages. Tracking a user can also note the last page which was visited by the user or the time of his departure. Tracking users' locations and times of surfing in the site can assist to make modifications in order to improve the user's experience and modify contents, thus increasing the probability of the return of the user (Gafni & Nissim, 2014).

Advertisers 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 through tracing the sites in which the user visited, the ads that were clicked on for further information, items purchased and forms filled over the internet. Thus, the user actively supplies data by filling out forms, or the data is received passively by tracking his activity in several sites. 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 track 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, allowing to expose him in the future to customized ads (Abdulhayoglu, 2008, Mansfield-Devine, 2014).

The increasing concern regarding privacy and the wish to protect data, as well as the concern regarding revealing the user's 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 respondents were not interested in ads which are based on tracking (Mayer & Mitchell, 2012). In a study which took place in Israel, the respondents stated that they avoid using a single connection measure due to privacy and data security concerns (Gafni & Nissim, 2014). Users' resistance to tracking bodies is expressed both in avoidance of tools which can lead data to security damage and in actively using tools which are designated for preventing tracking.

Active measures for data security and privacy protection already exist in the definitions of the browser. Browsers include 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. Yet, the decision whether to respect the 'Do Not Track 'message is subject to the decision of the site operator rather than of the user. Another active measure includes browser applications. This is software which the user can install as an addition to the browser. The software provides the browser other capabilities for privacy protection and personal data security by blocking unwanted tracking measures and advertisements during internet surfing. Some applications activate default security definitions, while others allow definition by the user allowing him 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 surfing privacy protection applications among average users, found that not all the applications which were examined were accessible to the user. Even when the users had a chance to customize the blockage according to their needs, they didn't have enough information in order to make informed decisions. In addition, the users were not able to identify the differences between the different tracking measures. Even when they received information regarding the tracking measure, they didn't have the knowledge to understand the meaning of such information. The users also expressed their dissatisfaction regarding the distraction caused by the applications while surfing the internet, their inability to give feedback to the application and stated that the user's interface was confusing and inconvenient (Constantin, 2015, Leon et al, 2011).

In light of the results of that study, we wish to examine the characteristics of a number of other common browser security applications. We executed content analysis on four applications: Privacy Badger; Ghostery; Disconnect Private Browsing Extension; and Privdog in three realms: the functioning of the application, the user's interface design and the economic-financial source of its operator.

Rationale

The function and activation system of applications reflect the developers idealogic-economic outlook of information security and privacy preservation. The choices of the Images, icons, command symbols, and colors which illustrate functions are not coincidental, but have meaning and are meant to deliver messages.

Research Question

How do applications function from a visual-functional standpoint in order to secure information and protect the user's privacy whilst surfing the net?

Theoretical Basis

Functional analysis and visual-semiotic analysis.

Research Population

Four leading internet security applications.

Research Process

Systematic examination of each application individually. Identification of outstanding characteristics. Documentation and encoding of findings.

Methodology

The research carried out a systematic examination of the visible content of each application on 2 levels - functional and visual. On the functional level we examined each applications' system, checked the information security measures, we described the decision mechanisms for identification, removal and blockage of tracking measures. Also, we examined the user interface, checked the ease of use of each application and the level of detail which is provided to the user. On the visual level of the interface, we examined the semiotic use of the symbols, images and colors which characterize each application. Furthermore, in order to understand the ideology of the application developers, we examined the economic-financial model of the bodies which sponsor the development and management of the applications.

Results

Privacy Badger Application Performance

Privacy Badger is an open code application, with a code which is accessible to all. In fact, Badger is based on a code of other applications, including AdBlockPlus which is designed to block advertisements. It does not require special definitions by the user and adopts different study and analysis tools in order to reach its goal. Badger tracks and analyzes the data sources which are linked to each internet page. The data source can be, for instance, a content service and the site can load its articles from one source and its users' replies from another. If it finds that a certain source tracks the user's surfing in several sites, it defines that source as a tracking source and blocks its activity. The blockage is based on several principles. First, Badger analyzes the cookies saved by the data source. If the cookie includes essential, harmless data, for instance, the user's

interface language, Badger will allow the cookie to be saved on the computer. Yet, if it finds that the cookie is designated for tracking the user's activity, Badger will block it and the data source that sent it. According to the second principle, if the browser sends a 'Do Not Track' message and the data source respects such message, Badger does not block the source. Yet, if the source does not comply with the request, the source will be blocked. The third principle is related to its capabilities in the realm of social networks controls (such as the 'Like' function in Facebook or the 'Twitting' function in Twitter). Different internet pages assimilate social network codes which are used for tracking the user's activity, even when he does not use them. That is, the mere existence of the social network control in a certain site, allows tracking of the user's activity. As a security measure, through a mechanism of another application, ShareMeNot, Badger replaces the social network code with an alternate code with a similar function yet without the tracking measure. As of 2015, Badger is at the beta stage and is currently being examined, modified and improved.

Design of User Interface

Badger operates as an addendum to the browser. After installation, an icon of the application appears on the ruler, an icon of a badger on the background of a red hexagon. In sites in where no tracking measures are found, the icon appears as is. Yet, when such measures are found, a number will appear on the icon which represents the number of tracking measures which were found in the site. When the user surfs in different sites, the number on the icon changes, in accordance with the number of the tracking measures indentified in each site. For information regarding the tracking measures which were found, the user has to click on the icon. First, a message indicating that the application protects against tracking in the site appears and then, beneath the message, a list of the tracking measures which were found. Beside each tracking measure an interactive ruler appears, which allows the user to define the protection level against each tracking means specifically. When the ruler key is on the left, its color will be red with a 'No Entrance' sign above it, which means that this tracking measure is completely blocked from tracking the user. When the ruler key appears in the center of the ruler, its color will be yellow with a cookie icon marked by a red X, which means that Badger has found a tracking measure, yet it is necessary for the ordinary activity of the site. That is, Badger allows tracking, yet blocks the possibility to create a cookie. When the ruler key appears on the right, its color will be green and a green circle will appear above it with the letter V. This sign indicates that Badger has found that this source is not a tracking measure. Information regarding the different keys can be found on the Badger internet site or by maneuvering the mouse above the 'No Entrance', cookie and confirmation icons. The colors for the different options, red, yellow and green, are used as they are customarily used in society, and allow clear and comfortable access to the application. Below the tracking measures list there are two more keys: one allows a temporary cessation of the application in the site and the other allows termination of the Badger operation completely. In addition, below these keys there is a link which refers to the FAQ page. No information regarding the tracking measures found by Badger can be found in the application or in the Badger site, except its name.

Economic-Financial Source

The body behind Badger is the Electronic Frontier Foundation (EFF), a non-profit organization which is financed by donations. The organization was established in 1990 and acts to protect civil freedom in the digital world. EFF acts to protect the users' right for privacy and their freedom of expression on the internet. The organization uses legal measures, policy analysis, ground activities and technological developments to obtain its goals. Besides Badger, the organization has developed other applications such as NSA Spying, which scans the user's computer and verifies that the American Intelligence organization does not track the communications which are sent from it.

Ghostery Application Performance

Ghostery is based on the principle that personal knowledge combined with personal control gives the user the maximal privacy protection. The application blocks the tracking measures of the user's activity by scanning code sections of advertisement bodies which are found on the internet page visited by the user. Ghostery locates the code section by checking them against a data base which is maintained by its operators. When an unfamiliar code which belongs to a tracking network is detected by Ghostery, it adds it to its' data base. This way, the Ghostery operating organization builds an accessible data base regarding the tracking networks which track users' activities.

Design of User Interface

Like Badger, Ghostery is installed on the browser. It appears as an icon of a blue smiling ghost on the ruler of the browser. Clicking on the icon opens a new window which offers information regarding the tracking measures and the customization options for blocking. In addition, there are several keys for the postponement of blockage, a key which leads to a White List created by the user, a support key, an options key, an 'about' key and a key for sharing the application. During surfing, a list of tracking measures found in the site will appear at the bottom of the page in a purple bubble. The tracking measures which were blocked will appear with a delete line through the name. Those not blocked will appear without such a line. A number will appear on the icon in the ruler representing the number of tracking measures found by Ghostery on a given internet page. Clicking on the application icon in the ruler will open a list of all the existing tracking measures in that internet page. Beside each tracking measure name, a ruler with a key which allows the user to control the blockage will appear. Moving the key to the left will turn it blue and a message will appear indicating that this tracking measure is approved for tracking at this time. Another message will appear, instructing the user to refresh the page in order for the change to be executed. Moving the key to the right will turn it red and a message indicating that this measure is blocked will appear. On the right side of the ruler there is a round grey key with the letter V for location verification. Clicking on this key will turn it green with a message indicating that this tracking measure is now approved permanently for

tracking on the specific page which the user is currently visiting. In addition, the user can click on the tracking measure name in order to obtain a description of the measure.

The description of the measure includes information regarding:

1. The icon of the company which operates the tracking measure, the names of all tracking measures operated by it, a description of the company, a link to the internet site of the company, affiliates and tags which describe the nature of the tracking measures.
2. The privacy policy of the tracking measures, the information gathered by the tracking measure, details regarding the sharing policy of the tracking measure and storage data policy of the tracking measure.
3. Details for contacting the privacy officer in the company which operates the tracking measure.
4. User options for blocking the tracking measure.
5. The number of locations in which the tracking measure was found and a link to the full list which is supplied by the business application of Ghostery.
6. The 'Learn More' option which includes links to the Ghostery blog, Ghostery Facebook page and Ghostery Twitter account.

Ghostery operators claim that with this detailed information the user is able to decide for himself when to block a tracking measure. He can decide whether to block each tracking measure separately; to block according to the categorization made by Ghostery; or to block all tracking measures. Another option offered by Ghostery is an explicit consent mechanism for cookies (Cookie Consent) – an option of the site owner to voluntarily present the information gathered by Ghostery. This mechanism is part of a self-regulation process regarding data security and user privacy in international organizations with advertisement networks.

Economic-Financial Source

In contrast to the home user version, there is a fee for the business application which serves to finance the company. The application allows site owners to safely run their data in conjunction with the marketing networks and prevents the transfer of unencoded data between their internet site servers and the marketing networks servers. Furthermore, the site owners can track the advertising networks they work with in order to improve the loading speed of the internet pages and to ensure that the data collected about the user does not deviate from the privacy regulations of the site.

Ghostery users can use a tool named Ghostrank which gathers data regarding the tracking measures scanned by the application. The gathered data includes the following: the tracking measure which was located by Ghostery; the internet page in which the tracking measure was found; the protocol used on the page; information regarding the blockage of the tracking measure; the internet address of the tracking measure; the loading time of the internet page with the tracking measure; the location of the tracking measure on the page; the browser in which the application is installed; the user's country; the application version; and data regarding the server recordings such as IP address and HTTP headline. The gathered information is transferred to the Ghostery database and is used for business needs in conjunction with corporations, for instance Cloud Marketing Management.

It should be noted that Ghostery operates additional tools to educate about privacy protection. The Ghostery AreWePrivateYet.com site includes, among other things, specification of the protection levels supplied by the different privacy protection tools, comparisons of surfing test performances with privacy protection applications, and surfing without such applications. The tests and their results are published frequently and the tools which are used for the tests are accessible in an open code. Another tool operated by Ghostery is The Purple Box blog. The blog serves as a community site for the application users and includes news regarding the product, competitions for programmers who build protection measures against the tracking measures, and graphic illustrations of data regarding user privacy and tracking measures.

Disconnect Private Application Performance

Another application is the Disconnect Private Browsing browser extension. When the application detects that the browser is trying to communicate with a different server than that which the user has entered, it categorizes the communication as a third party communication, or, as Disconnect defines it, a network request. Network requests are categorized by the application into seven groups according to their business model: Google, Facebook, Twitter, Social, Content, Advertising and Analysis. The default definitions of the application establish that every network request which is not categorized as content will be blocked and will not be presented to the user, because if a network request of content is blocked, the site will not be displayed at all. The privacy application continuously communicates with Disconnect servers for the purpose of updates so it may categorize the network application to the suitable group. Like Badger, Disconnect allows the user to view the source code of the application, not only to make sure that he is protected, but also to make sure that the code itself does not constitute a tracking measure.

Design of User Interface

Like the applications described above, the icon of Disconnect , the letter D, appears on the browser ruler with the number of tracking measures which were found on the current internet page. Clicking on the icon opens a window with additional information regarding the tracking measures which were blocked by Disconnect, each measure categorized to one of the seven categories mentioned above. Clicking on the category will display a list of the tracking measures which were categorized and blocked. A green V sign appears beside every tracking measure which was blocked. If the user is interested in cancelling the blockage, he can click on the green symbol, which will turn grey. The grey color means that this tracking measure is not blocked. Unlike other applications which require refreshing of the internet page while modifying blockage definitions, in Disconnect, when the user makes such modifications, the internet page is refreshed automatically. Clicking on the tracking measure will open a new internet window which directs the user to the tracking measure which was traced. This enables the user to receive additional information

regarding the tracking measure and to make an informed decision regarding its blockage. One may also view graphic data which shows the site in the middle of a circle connected to various data sources. Sources which are recognized as tracking measures are immediately blocked and represented by a red 'No Entrance' sign. Measures which are suspected to be tracking measures are marked in grey and are not blocked. Maneuvering the mouse over each source presents additional information regarding that source and an option for modifying the blockage definitions. In addition, the user can create lists of exceptional sites which are not be blocked and view statistical data regarding the application operations which are also presented graphically. Referrals to a help page and an option for sharing the application also exist.

Economic-Financial Source

Disconnect operates according to the business model which is called Free – Freemium and Premium. That is, for free and with an additional payment. This is a pricing method by which the company offers free applications, alongside applications which include extra features and entail a fee. Besides the browser privacy application, Disconnect offers other applications for personal data and privacy protection:

1. Protection from advertising damages application through blockage of harmful advertisements. Is applicable to Android smart phones.
2. Wireless network protection application through a private virtual communication network. Is applicable to Android smart phones.
3. Private browser search application, which sends the query via a proxy server, thus preventing tracking.
4. Privacy browser icon application which presents aspects related to the user's privacy for each page: use of gathered data, collection of data regarding surfing session, an option to locate the user's location, the time span during which the surfing data was gathered, children's data privacy security certificate on behalf of TRUSTe, respect of' Do Not Track' requests, use of encoding in SSL protocol, vulnerability to security crack Heartbleed.
5. Educational application for children which allows them access to data regarding their privacy and which filters their tracking measures. The application is applicable to iOS smart phones.
6. Privacy application for smart phones which acts similarly to the surfing privacy application for the browser.

The premium version includes all the Disconnect applications and offers some extra features for the privacy application, such as: connecting to a private virtual network and a Proxy server. Another economic-financial source includes user contributions. Upon installation of the application, the user is referred to an internet page with explanations regarding the application and which also includes a request for a one-time or an annual donation to the company.

Privdog Application Performance

The last application we examined is Privdog. The application is a product of AdTrustMedia which acts in cooperation with the leading data security company, Comodo. Like the previous three applications, Privdog also scans for tracking measures, statistical tools and third party commands on the internet page and blocks them. The uniqueness of Privdog is that when it scans a code which is identified as a third party advertisement, it does not block it, but rather replaces it with an ad from the advertisement server of AdTrustMedia. If the ad source is the internet page which the user is visiting the ad is not replaced. The ads supplied by AdTrustMedia are scanned by Comodo service and are examined according to the following principles:

1. The site address which the ad leads to is identical to that of the owner of the ad.
2. The site address does not include a link to a damaging source.
3. The ad does not gather personal information regarding the user, such as: name, electronic mail box address or connecting details to the site.
4. The ad does not include a malicious code or a non-efficient code (which requires unnecessary resources from the user's computer).

Design of User Interface

Unlike the previously reviewed applications, Privdog is installed by the user as an application on the computer. Its icon is a watchdog with a neck-chain and a lock, colored in blue, white and black, which appears on the ruler of the browser. Clicking on the icon opens a window with information regarding the tracking measures which were identified by Privdog. First a message is sent which notifies the user that the site he is visiting is not included in the exceptional sites list, thus indicating the user option to create a list of exceptional sites which the application does not apply to. Next, the number of blocked tracking measures in the site appears. These are later categorized into four categories: advertisement networks, tracking measures, third party commands and statistics, with the number of the tracking measures in each category appearing alongside.

Alongside each category there is a sign which indicates that the measure has been blocked or restricted. Clicking on the category opens a list which includes the names of the measures which were found and the number of requests for information which were received from each measure. At the bottom of the window there is a message which specifies the number of threats which were blocked by Privdog in the current browsing session. Clicking on the options key opens a new browser window which allows to customize Privdog. On the threats page, there are two options: blocking the threat, or allowing its activity. It is possible to block ads totally or replace them with those of AdTrustMedia. In the Exceptions page, the user can choose sites which will not be blocked by Privdog, and in the Preferences page the option of 'Do Not Track' maybe activated.

Economic-Financial Source

The economic model of Privdog is based on the AdTrustMedia advertising network. Like any other advertising network, AdTrustMedia is based on three factors: advertisers, site owners and cooperators. The advertisers are the owner of the ads which are published by the advertising network; the site owners supply the advertising space for the ads; and the cooperators are the marketing factors of the advertising network. In Privdog the cooperators are agents who distribute the application. An example for such an agent is the Comodo Dragon browser

which includes Privdog. The application replaces the harmful ads with secured ads from the AdTrustMedia advertisement network and the advertisers pay the advertising network for publishing their ads. The economic-financial model is based on a win-win situation: the users receive secured ads, the advertisers receive advertising space and the marketing network benefits from its mediation between the users and the advertisers.

Discussion

Data security and privacy protection applications have similar goals – to protect the internet user. Yet, they differ in their view of the data security and user privacy, which is expressed in the functional and applicable level of each of the applications.

In general, all applications operate as an addendum to the browser which has to be installed by the user, except Privdog which has to be installed as an application on the computer. Each application has access to information regarding the tracking measures by clicking on the icon on the ruler of the browser and each presents the number of tracking measures which were found on the internet page. Furthermore, in each application the user is allowed to limit the blockage of the tracking measures. The differences between the applications are defined by the blocking options of the tracking measures, their categorization and the data specification level that each application supplies to the user. A comparison of all the applications studied shows that the Badger defines tracking measure security and privacy according to which partial data may be exposed, while other details remain confidential. This application decides for the user, based on to its own discretion, whether or not to block a tracking measure, depending on its' characteristics. The lack of specification is due to the privacy approach of Badger – decision making regarding blocking as at the discretion of the application, which is able to make decisions while analyzing different factors which cannot be weighed by the user. Like Badger, Disconnect also demonstrates that the privacy right is total and as such, the data should be protected by every means. Thus, the application blocks, as a default, every tracking measure, while the user is unable to neutralize the application temporarily, as he is able to do in the other applications. In addition, in the premium version of the application, Disconnect offers a comprehensive package for protecting the privacy of surfing and for protecting the personal information of the user.

In contrast, Ghostery allows the user greater control of his data security. Ghostery is the only application of the four we examined that opens a new window on the internet page which the user is visiting , that includes information regarding the tracking measurers which were found. In addition, Ghostery is the only company which operates a site (AreWePrivateYet.com) and a blog (The Purple Box), which supply information, news and updates for the user regarding familiar and new tracking measures. Thus, Ghostery keeps the user informed at all times regarding its' tracking measures. Furthermore, unlike the other applications, Ghostery not only allows viewing the list of tracking measures which were found, but also directs the user to a page which offers information, supplied by Ghostery, regarding the tracking measures which were located. Therefore, the user is able to make educated decisions regarding blockage of the tracking measures. It should be noted in this regard that the Disconnect application offers the user a similar, yet, not identical option. Clicking on the name of the tracking measure directs the user to the internet site of the tracking measure itself, yet with no details which may help the user make a decision regarding the blockage. The Privdog application operates according to a formula which tries to bridge and to connect between the factors which act in the network: the advertising network, the advertisers and the users. This approach is expressed in the economic-financial model of Privdog, according to which both the advertisers and the users enjoy secured ads under the protection of the technology. Entering the more advanced options allows modifying the blockage of the tracking measures, yet in a very limited way. It is also impossible to cancel the blockage of the ads, but rather only to block ads permanently or to replace them with those of AdTrustMedia. These options are derived directly from the policy of Privdog which wishes to benefit all the involved parties.

Regarding the user interface, the four applications which were examined operate in a similar way, yet each has unique characteristics. We found that the interface of Badger is user friendly. Choosing colors which are used in our society for certain messages (red, yellow and green), as well as using images for illustrating the users' activities, are very convenient for comprehension and operation. Similarly, the colors which were chosen by Ghostery for the different operations (red for blocking a tracking measure and green representing the cancellation of a blockage) is logical. The Privdog interface has been found to be convenient and simple for operation by the user, since Privdog does not allow customization of the interface by the user. In contrast, Disconnect may confuse the user since the green color was chosen for the blockage option, while in society this color commonly represents progression and movement.

Furthermore, we found that half of the applications examined were complicated for use, a fact which makes it harder for the user to make informed use of these applications for data security and privacy protection. This conclusion partly supports the results of Leon et al (2011) according to which all the applications which were examined were inaccessible to users. For instance, according to its view, Ghostery allows the user maximum control and so it presents many definition options, which makes it hard for the user, as well as detailed explanations, which may not all be understood by the user. In addition, the window which pops up while entering each internet page in which the tracking measures are displayed, like pop up ads, disrupts the surfing. Like Ghostery, Disconnect also offers many options, yet they are not accompanied by detailed explanations. The customization process by the user is problematic, but may be intended, since Disconnect uses strict default definitions as part of its strict privacy view.

In addition, our study shows that although the privacy applications define the tracking measures as a negative phenomenon which should be blocked, some of the bodies which operate the applications have business relations with advertising networks in the internet. The payable business

application helps the site owners to safely manage the data against the marketing networks, to track the advertising networks with which they work and to avoid transferring un-coded data between the internet servers and the servers of the advertising network. Another example is AdTrustMedia which operates Privdog, which is in itself an advertising network which uses the application to replace harmful ads with secured ones. In contrast, Disconnect finances its activity by selling the premium version of the application as well as user donations, while Badger is financed only by user donations.

Summary

Users are becoming increasingly aware of the privacy and data protection issue on the internet. Lately, Google has launched an application named My Account which enables privacy control and shows which applications track the user, which personal specifications Google is aware of, including age and sex, voice recognition, languages spoken and interest realms. The new tool of Google enables privacy and security testing. The privacy test shows the data Google has regarding the user who uses its three most popular online services and affect each user: the search engine, YouTube, and the social network Google Plus. The security test shows which backup and restoration tools exist in the user's account in case of password loss or penetration to the account, which devices are connected to it and more. Google also presents all the data gathered by it through the Android devices. Indeed, in the past Google presented data, such as a list of applications which follow the user, platforms which track location and more, but not in such a clear, friendly and relevant way as in My Account. The reform in the privacy control tools of Google points to the realization of the internet firms regarding the increasing significance of the users' privacy.

In this paper we carried out a functional analysis of four leading internet security applications: Badger, Ghostery, Disconnect and Privdog. Essentially, all four applications perform the same basic operations: they scan the source code of the internet page before it is presented to the user, remove the parts which are related to tracking the user's activity and present to the user the rest of the page, excluding those parts. Yet, each application operates differently in order to achieve this goal and activates a different decision mechanism regarding the tracking measures to be blocked or removed. In addition, all applications operate to block third party tracking measures. The firms claim that they do have no intention of blocking ads but rather only to protect the privacy and data of the user. Yet, since most of the third party networks are advertising networks, the applications actually function as an ad blocker on the internet pages.

In the analysis of the applications we examined the way each application operates in order to achieve its goal – protecting the user's privacy and securing his personal data against the tracking measures in the internet. We also analyzed the user interface, the convenience level and its practicality. Finally, we examined the economic-financial model of the bodies which sponsor the applications. We found that some of them are financed by donations and others are financed by direct or complementary business activity. We believe that the analysis results point not only to the functionality and practicality of each application, but also to the world view of the application operator regarding privacy and data security of the internet user.

References

[1] Abdulhayoglu, M. (2008). Would have been much easier to build an ad blocker without caring for Publishers. Retrieved from https://www.melih.com/2014/01/05/would-have-been-much-easier-to-build-an-adblocker-without-caring-for-publishers/

[2] Ajdari, D., Hoofnagle, C., Stocksdale, T., & Good, N. (2013) Web Privacy Tools and Their Effect on Tracking and User Experience on the Internet. Retrieved from http://www.truststc.org/education/reu/13/Papers/AjdariD_StocksdaleT_Paper.pdf

[3] Birnhack, M. (2009). Who Owns Bratz? The Integration of Copyright Law and Employment Law, 20 FORDHAM INTELLECTUAL PROPERTY, MEDIA & ENTERTAINMENT LAW JOURNAL 95-163.

[4] Birnhack, M. (2005) Holes in the Net: Pornography, Information and Shaping Policy in the Digital Environment, 13 POLITIKA 101-125 [Hebrew]

[5] Gafni, R., &Nissim, D. (2014).To Social Login or not Login? Exploring Factors Affecting the Decision. Issues in Informing Science and Information Technology, 11, 57-72.

[6] Constantin, L. (2015). Worse than Superfish? Comodo-affiliated PrivDog compromises web security too. PC World. Retrieved from: http://www.pcworld.com/article/2887632/secure-advertising-tool-privdog-compromises-https-security.html

[7] Grysiuk, M., C.I.P. (2015). The cookie trail: Why IG pros must follow the crumbs. Information Management, 49(2), 24-28,47. Retrieved from http://search.proquest.com/docview/1663613520?accountid=14483

[8] Hormozi, A. M. (2005). Cookies and privacy. EDPACS, 32(9), 1-13.

[9] Leon, P., Ur, B., Shay, R., Wang, Y., Balebako, R., &Cranor, L. (2012, May). Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 589-598).ACM.

[10] Mansfield-Devine, S. (2014). The dark side of advertising. Computer Fraud & Security, 2014(11), 5-8.

[11] Marella, A., Pan, C., Hu, Z., Schaub, F., Ur, B., &Cranor, L. F. (2014) Assessing Privacy Awareness from Browser Plugins. Retrieved from http://cups.cs.cmu.edu/soups/2014/posters/soups2014_posters-paper29.pdf

[12] Mayer, J. (2011). Tracking the trackers: Self help tools. The Center for Internet & Society. Retrieved from https://cyberlaw.stanford.edu/blog/2011/09/tracking-trackers-self-help-tools

[13] Mayer, J. R., & Mitchell, J. C. (2012). Third-party web tracking: Policy and technology. In Security and Privacy (SP), 2012 IEEE Symposium on (pp. 413-427). IEEE.

[14] Shwartz-Altshuler, T., Ed. (2012). Privacy In Era of Changes. Jerusalem. Grapus Print [Hebrew].