Issues in
Informing Science +
Information Technology

*An Official Publication
of the Informing Science Institute
InformingScience.org*

IISIT.org

Volume 15, 2018

PLACE DETERMINANTS FOR THE PERSONALIZATION-PRIVACY TRADEOFF AMONG STUDENTS

Maor Weinberger*	Bar-Ilan University, Ramat-Gan, Israel	maor89@gmail.com
Dan Bouhnik	Jerusalem College of Technology, Jerusalem, Israel	bouhnik@jct.ac.il

* Corresponding author

ABSTRACT

Aim/Purpose
This exploratory study investigates the influential factors of users' decisions in the dilemma of whether to agree to online personalization or to protect their online privacy.

Background
Various factors related to online privacy and anonymity were considered, such as user's privacy concern on the Web in general and particularly on social networks, user online privacy literacy, and field of study.

Methodology
To this end, 155 students from different fields of study in the Israeli academia were administered closed-ended questionnaires.

Findings
The multivariate linear regression analysis showed that as the participants' privacy concern increases, they tend to prefer privacy protection over online personalization. In addition, there were significant differences between men and women, as men tended to favor privacy protection more than women did.

Impact on Society
This research has social implications for the academia and general public as they show it is possible to influence the personalization-privacy tradeoff and encourage users to prefer privacy protection by raising their concern for the preservation of their online privacy. Furthermore, the users' preference to protect their privacy even at the expense of their online malleability may lead to the reduction of online privacy-paradox behavior.

Keywords
online privacy behavior, online personalization, privacy paradox, privacy concern, online privacy literacy, online privacy self-efficacy

Accepting Editor: Eli Cohen │ Received: December 13, 2017 │ Revised: March 12, 2018 │
Accepted: March 26, 2018.
Cite as: Weinberger, M., & Bouhnik, D. (2018). Place determinants for the personalization-privacy tradeoff among students. *Issues in Informing Science and Information Technology, 15,* 79-95. https://doi.org/10.28945/4019

INTRODUCTION

Information privacy is defined as users' right "to keep information about themselves from being disclosed to others [marketers and other unknown people]" (Rognehaugh, 1999). Privacy has always been a major concern associated with the commercial information technology and particularly with regard to the issue of personalization (Sutanto, Palme, Tan, & Phang, 2013) - "the ability to provide content and services that are tailored to individuals based on knowledge about their preferences and behaviors" (Adomavicius & Tuzhilin, 2005). It seems that the Internet has created a conflict regarding the concept of privacy, since personalization technologies offer beneficial tools for enhancing users' online experience, but at the same time allows service providers and other users to collect their personal information, and in many cases without their consent (Toch, Wang & Cranor, 2012). Thus, users are constantly faced with the dilemma – whether to agree to online personalization or to protect their personal privacy.

The tradeoff between online privacy and self-disclosure was investigated in numerous studies (Fogel & Nehmad, 2009; Graeff & Harmon, 2002; Hoy & Milne, 2010; Milne, Rohm & Bahl, 2004; O'Neill, 2001; Paine, Reips, Steiger, Joinson, & Buchanan, 2007; Sheehan, 1999; Taddicken, 2014; Wills & Zeljkovic, 2011). Many of them showed that users are concerned with their online privacy and wish to protect it (e.g. Paine et al., 2007; Wills & Zeljkovic, 2011). Nevertheless, the conclusions regarding actual behavior and its correlation with users' attitudes and intents reported in the previous research were inconclusive. Some studies showed consistency between users' behavior and attitudes, as they preferred to protect their online privacy, even at the expense of their convenience (Akhter, 2014; Awad & Krishnan, 2006; Castañeda & Montoro, 2007; Heirman, Walrave, & Ponnet, 2013; Hoffman, Novak, & Peralta, 1999; J. K. Lee & Letho, 2010; Phelps, D'Souza, & Nowak, 2001; Phelps, Nowak, & Ferrell, 2000; Potoglou, Palacios, & Feijóo, 2015; Taylor, Davis, & Jillapalli, 2009; Weinberger, Bouhnik, & Zhitormirsky-Geffet, 2017). However, other studies found a miscorrelation between users' reported desire to protect their privacy and their actual behavior which reflected the opposite - a voluntary disclosure of personal information over the Internet (Acquisti & Gross, 2006; Bronstein, 2012; Debatin, Lovejoy, Horn, & Hughes, 2009; Dienlin & Trepte, 2015; Gross & Acquisti, 2005; Guo, Zhang, & Sun, 2016; Jensen, Potts, & Jensen, 2005; H. Lee, Park, & Kim, 2013; Norberg, Horne, & Horne, 2007; Taddicken, 2014; Tufekci, 2008; Zafeiropoulou, Millard, Webber, & O'Hara, 2013; Zhitomirsky-Geffet & Bratspiess, 2014). This discrepancy between users' online privacy attitudes and their actual behavior, when they prefer to utilize the malleability of the cyberspace at the expense of privacy and anonymity protection, was termed "privacy paradox" (Barnes, 2006; Norberg et al., 2007).

Past research has raised several hypotheses to explain users' online self-disclosing behavior, i.e., "providing others with personal information about oneself" (Jacobs, Hyman, & McQuitty, 2001), for example, on social networks and e-commerce websites.

These hypotheses include the following: 1) the knowledge gap hypothesis – a lack of awareness of the risks posed by information disclosure (Barnes, 2006; Debatin et al, 2009) or a lack of knowledge regarding privacy-enhancing tools and techniques (Trepte et al., 2015); 2) the uses and gratification theory – a lack of willingness to forfeit the benefits of information disclosure, e.g., social benefits (Debatin et al., 2009; Trepte et al., 2015); 3) the optimistic bias theory, also known as unrealistic optimism or comparative risk judgments (Weinstein, 1989) – self-perception of Internet users to be less vulnerable to privacy and information security risks than their peers (Baek, Kim, & Bae, 2014; Cho, 2012; Cho, Lee, & Chung, 2010).

Inspired by the above theories, our primary objective in this study is to examine predictive factors affecting users' decisions in the dilemma of whether to agree to online personalization or to protect their personal privacy. This may help us reach extensive conclusions on the matter of users' online privacy paradox behavior. As opposed to previous research that examined only a few specific predictors for this type of behavior and mostly in the context of social network sites, this research suggests a wide variety of factors, both at the individual level and among predefined groups (e.g., online literacy level and field of study).

For the purposes of this research, a user survey was conducted with 155 students from the Israeli academia, who were administered a closed-ended questionnaire examining their online privacy attitudes and behavior. Further, the questionnaire was analyzed using multivariate linear regression models in order to determine the predictive factors of users' decisions in the personalization-privacy tradeoff.

Related Work

Personalization and Customization in a Privacy Threat Perspective

Online users encounter various privacy and information security threats (Mayer, 2009). Some of these threats are related to the exposure of the users' anonymous identity. Many popular web browsers (e.g., Google Chrome and Mozilla Firefox) provide the user with the ability to exclusively shape their browser interface, by settings alteration or add-ons installation, enriching the user experience. As a result, every user has his/her own unique web browsing environment, compatible with his/her personal preferences and different from the setting of any other user. Proactive specification of the user's products and services is called customization (Li & Unger, 2012). This uniquely-shaped online environment is effectually a digital fingerprint that might also be used by external parties for exposing the user's identity (Eckersley, 2010; Mayer, 2009). However, exposure of one's online identity can also occur without the user's proactive measures. One of the most common methods for online surveillance is the tracking cookie. Cookies were initially developed to allow users to re-visit websites without the need to identify themselves and their preferences each time. However, in subsequent years cookies have been used in other ways, including in personalization processes (Millett, Friedman, & Felten, 2001). Personalization is initiated by a commercial entity, aiming to offer the customer products and services that best suited him/her, based on previously collected data (Li & Unger, 2012). This may bear different benefits for both the consumer and the vendor, however cookies that enable personalization might also be used in ways that invade users' privacy, for example third party websites use cookies to create user profiles without their knowledge and track users' online activities (Millett et al., 2001; Milne, 2000).

As customization and personalization are closely related terms and particularly in relation to privacy issues, in this work, both will be referred to as "personalization".

Consumers' Willingness to Partake in Online Personalization

Personalization is dependent on two key factors: 1) vendor's ability to collect and apply consumer information; 2) consumers' willingness to disclose personal information and use personalized services (Chellappa & Sin, 2005). The vendor has obvious strategic benefits gained from personalization, as it allows vendors to predict product demand and thus effectively manage their inventory. In addition, establishment of individual and specific customer profiles provides the vendor with the capability to offer dedicated products adjusted to the customer's needs. This may bear significant contribution in increasing customer satisfaction and loyalty (Chellappa & Sin, 2005; J. K. Lee & Letho, 2010; Li & Unger, 2012). However, personalization may also be beneficial for the consumers. First, it offers them accurate and timely information about products they desire (Senecal & Nantel, 2004). Second, it allows them to save their personal details (e.g., name and address) and shipping preferences to conveniently take use of in the future purchases. In addition, personalization may have an economical advantage for the consumers, as they can predefine an instant alert to be sent for them in case of a price drop of their desired product (Chellappa & Sin, 2005). However, these aforementioned advantages do not come without costs. Previous studies showed that even though personalization has a positive effect, privacy concerns negatively affect users' intention to use it (Awad & Krishnan, 2006; Chellappa & Sin, 2005; Li & Unger, 2012; Sheng, Nah, & Siau, 2008; Sutanto et al., 2013). However, it seems that the impact of these concerns may be limited, as users may relinquish their personal privacy, in return for the various benefits gained from using personalized services (Hann, Hui, Lee, & Png, 2002). The tradeoff between online personalization and privacy protection is a widely explored topic in the context of electronic commerce for many years (Awad & Krishnan, 2006; Chellappa & Sin, 2005; Goodwin, 1991; J. K. Lee & Letho, 2010; J. M. Lee & Rha, 2016; Li & Unger, 2012; Milne & Gordon, 1993; Sheng, et al., 2008; Sutanto et al., 2013; Xu, Lou, Carroll, & Rosson, 2011). Most of the studies explored this issue came to the conclusion that in order for the users to agree to online personalization, its benefits must overweigh the potential risks to their privacy (e.g., Awad & Krishnan, 2006; Chellappa & Sin, 2005; Sheng et al., 2008). However, findings regarding users' preference in this dilemma remains inconsistent. For example, Awad and Krishnan (2006) found that privacy concerns significantly affect users' agreement to personalized advertising. Likewise, Turow, King, Hoofnagle, Bleakley, & Hennessy (2009) found that two thirds of Americans do not want marketers to personalize their advertisements according to their interests. Conversely, Xu et al. (2011), who studied user attitudes towards location-aware marketing, found that personalization could, in some cases, overcome users' privacy concerns. Accordingly, Li & Unger (2012) found that personalization can outweigh the impact of privacy concerns as long as it is perceived by the user as qualitative. They also found that users may be willing to pay for personalization of quality.

The Privacy Paradox and the Factors that Affect Self-Disclosure

The personalization-privacy tradeoff was also examined in a wider perspective by studies which investigated the discrepancy between users' online privacy attitudes and their actual behavior reflected the opposite - the "privacy paradox" (Barnes, 2006; Norberg et al., 2007). These studies (e.g., Acquisti & Gross, 2006; Debatin et al., 2009; Dienlin & Trepte, 2015; Gross & Acquisti, 2005; Taddicken, 2014; Tufekci, 2008; Weinberger et al., 2017) explored the dichotomy between privacy concerns and self-disclosure. This dichotomy was most apparent in the setting of social networks. Social networks encourage self-disclosure by their very nature, as one of their most important benefits for the user is probably the social capital gained from maintaining interpersonal relationships and friendships (Ellison, Steinfield, & Lampe, 2007). This might be achieved more easily when the privacy settings are less strict and the profile information is more exposed (Acquisti & Gross, 2006; Debatin et al., 2009; Gross & Acquisti, 2005). Taddicken (2014) found that about 75% of the participants revealed factual information, such as surname, birth date and occupation. Sensitive information was found to be less frequently disclosed, but was still revealed in great extent – about 67% posted personal pictures and about half of the participants shared personal experiences. Similarly, H. Lee et al. (2013) found that users actively share personal information albeit their concerns, due to the expected benefits of information sharing.

Other studies explored the factors that affect self-disclosure on the e-commerce and social network sites. Many factors were revealed as influential, such as socio-demographic factors – gender and age (Baddeley, 2011; Castañeda & Montoro, 2007; Milne & Boza, 1999; Phelps et al., 2001); users' online privacy literacy (OPL) (Trepte et al., 2015), i.e., their knowledge of the tools available to protect their information online and Internet experience (Hoffman et al., 1999; Park, 2013) and online privacy self-efficacy (OPSE), i.e., users' belief in their ability to protect their identity when surfing the Internet (Chen & Chen, 2015); Website-related variables, such as firm's reputation (Andrade, Kaltcheva, & Weitz, 2002; Costante, den Hartog, & Petkovic, 2011), the detail level of the website's privacy policy (Andrade et al, 2002; Metzger, 2006); and the type and scope of information requested (Andrade et al., 2002; Joinson, Reips, Buchanan, & Schofield, 2010; Leon et al., 2013; Metzger, 2006; Phelps et al., 2001; Sheehan & Hoy, 2000); general perceptions and attitudes on online self-disclosure in e-commerce and social network sites (Acquisti, Brandimarte, & Lowenstein, 2015; Baddeley, 2011; Chellappa & Sin, 2005; Culnan, 1993; Culnan & Armstrong, 1999; Joinson et al., 2010; Milne & Boza, 1999; Phelps et al., 2000; Phelps et al., 2001; Yoon, 2002), such as users' unawareness of the information they are sharing or the ways it can be used (Acquisti et al., 2015).

The current research aims to address the aforementioned factors and apply them on the personalization-privacy trade-off. In addition, we explore additional factors that were not examined by previous research. Thus, the main research questions examined in this study were:

1) Whether and to what extent do users choose to agree to online personalization at the expense of personal privacy protection?
2) What are the main predictive factors of the tendency of embracing online personalization at the expense of privacy protection?
3) What demographic factors are related to the personalization-privacy trade-off?

The above works explored factors affecting online self-disclosure. However, to the best of our knowledge, no previous work directly assessed and determined the main influential factors that are decisive in the personalization vs. privacy dilemma. In this study, a variety of factors were tested, such as gender, the users' OPL level, field of study, and online privacy attitudes (e.g., OPSE and privacy concern). In addition, as opposed to previous research that examined online privacy behavior in particular settings (e.g., social network sites), our research examined this issue from a wider perspective, with no thematic limitation.

METHODOLOGY

SAMPLE POPULATION

This study was conducted among 155 students from four different Israeli academic departments: 1) Computer Science and Programming at the Jerusalem College of Technology; 2) Industrial Engineering at the Jerusalem College of Technology; 3) Information Science at Bar-Ilan University; 4) Accounting and Business Management at the Jerusalem College of Technology. The questionnaires were handed out throughout the academic courses of the 2016/17 school year, to be filled in class. Notably, all four departments are considered somewhat technologically oriented, but differ in the level and number of Internet and computer system courses.

This study received ethics approval from the Institutional Review Board of the Faculty of Humanities at Bar-Ilan University and was conducted in accordance with the American Psychology Association (APA) ethical requirements. It was also made clear that no personal information would be collected by the researchers and their responses would be used solely for the purposes of the study.

Table 1 presents the demographic characteristics of the sample.

Table 1: Demographic Characteristics of the sample (N = 155)

	Variable	Percentage %	N
Gender	Male	41.29%	64
	Female	58.71%	91
Age	<26	70.3%	109
	>26	29.7%	46
Birthplace	Israel	88.39%	137
	Other	11.61%	18
Field of Study	Computer Science and Engineering	34.84%	54
	Industrial Engineering	24.52%	38
	Information Science	21.94%	34
	Accounting and Business Management	18.71%	29

Research Variables and Validation Method

For the purposes of the study, a questionnaire of 44 items on online privacy behavior and its affecting factors was composed (see Appendix). The questionnaire was based on Weinberger et al.'s (2017) privacy paradox study. The use of a questionnaire allows data gathering and analysis in a short period of time, and its distribution among the chosen sample population permits us to investigate the subject matter among those who are proficient in Web applications and engaged with to the online world.

Based on the questionnaire the following factors of the privacy paradox and privacy protection behavior as independent research variables were considered:

1) Gender (Part A, item 1);
2) Age (Part A, item 2);
3) Birthplace (Part A, item 3);
4) Students' field of study (Part A, item 5);
5) The level of users' online literacy introduced by Park (2013) was measured as follows: The participants were classified into three different online literacy groups, according to their academic and occupational background (Part A, item 6) and level of proficiency in the fields of computers and the Internet (Part A, item 7), based on their self-reports: low; moderate; high.
6) The level of users' OPL was measured via two different indicators based on Park's (2013) technical skills' parameter: i) The level of knowledge of privacy-enhancing tools (Part C, items 1-8); ii) The level of use of privacy-enhancing tools (Part C, items 9-16). The participants were questioned about eight different privacy-enhancing tools examined in Rainie, Kiesler, Kang, and Madden (2013): i) Logging-out from the online accounts; ii) Clearing of history and other browsing details; iii) Blocking cookies; iv) Browsing via Incognito Mode; v) IP spoofing; vi) Using proxy servers; vii) Using VPN; viii) Using TOR.

Each subject's responses was coded on a 1-5 Likert scale (1= no knowledge of / no usage at all, 5=very high level of knowledge/usage) and then averaged over all the tools. A test of internal consistency reliability (Cronbach's α coefficient values) showed that the reliability of the indicator measuring the level of knowledge of privacy-enhancing tools in the present sample was $\alpha = 0.74$ and for the indicator measuring the level of usage of privacy-enhancing tools was $\alpha = 0.72$.

7) The level of privacy and anonymity threat awareness was measured via three different indicators: i) The awareness of the social threat as the sense of exposure to other users (Part B, item 3); ii) The general awareness of privacy threats as users' sense of privacy protection while visiting a website (Part B, item 2); iii) The awareness of the technological threats as users' knowledge of concrete parameters that are prone to online surveillance (Part B, item 4). The subjects were questioned regarding seven personal details that can be monitored while visiting a website: 1) Operating system; 2) Computer type; 3) Web-browser; 4) IP address; 5) Browsing history; 6) Location; 7) Name.

Responses were coded as follows: 0 = no, 1 = yes. Lastly, a single value, summing up the number of personal details that were marked by the participant, was calculated.

8) Users' OPSE level was measured through one indicator that examined the belief in one's ability to browse anonymously (Part B, item 7). The responses were coded on a 1-7 Likert scale (7 - high level of belief, 1 - no belief at all,) and then were averaged.
9) The level of privacy concern was measured via two indicators: 1) The level of concern for the protection of privacy on the Web (Part B, item 5) - 1-5 Likert scale (5 - very highly concerned, 1 - not concerned at all); and 2) The level of concern for the protection of privacy on social networks (Part B, item 6) - 1-5 Likert scale (5 - very highly concerned, 1 - not concerned at all).

The dependent research variable was the embracing of online personalization at the expense of personal privacy protection (Part D, items 1-15), based on Chellappa and Sin (2005) and information security surveys, such as Aydin and Chouseinoglou (2013) and Talib, Clarke, and Furnell (2010). Each item in this part comprised a certain privacy behavior. Based on the uses and gratification theory (Trepte et al., 2015), these items implicitly present the risks and benefits of the suggested behavior (e.g., "I tend to download software and services aiming to improve the performance of my computer / Web browser, even from seemingly unprotected websites."). The behavior could be either privacy protection behavior or self-disclosing behavior, i.e., agreeing to online personalization despite the awareness of the privacy threats. This group of items constitutes a direct scale of 15 items for assessing user decisions regarding the personalization-privacy tradeoff. The users' tendency towards embracing online personalization at the expense of privacy protection was measured by this scale. In order to create a single variable, the values of three items that reflected the opposite tendency (items 1, 13, 15) were reversed. The values were coded on a 1-5 Likert scale (5 – a strong tendency towards online personalization, 1 – a strong tendency towards privacy protection) and then averaged.

We conclude that the internal consistencies of the above measures assessed by means of the Cronbach's alpha coefficient were at least 0.70 or higher and thus can be considered acceptable (Nunnally & Bernstein, 1994).

To predict the users' tendency of embracing online personalization, a multiple linear regression analysis was performed using the above factors as independent variables.

Results

This section presents the results of the statistical analysis conducted to examine the research questions presented in the Introduction section. First, we analyzed the respondents' concern for the protection of their personal information on the Web, in general, and on social networks, in particular. The respondents were found to be moderately concerned with privacy threats posed on their personal information on the Web (M = 3.43, SD = 1.05) and in the setting of social networks (M = 3.45, SD = 1.12). Furthermore, the levels of OPL and OPSE were measured among the general sample and distributed by field of study. Both the OPL and OPSE levels of the sample were medium, M = 2.46, SD = 0.72 (in the range of 1-5) and M = 3.15, SD = 1.65 (in the range of 1-7), respectively.

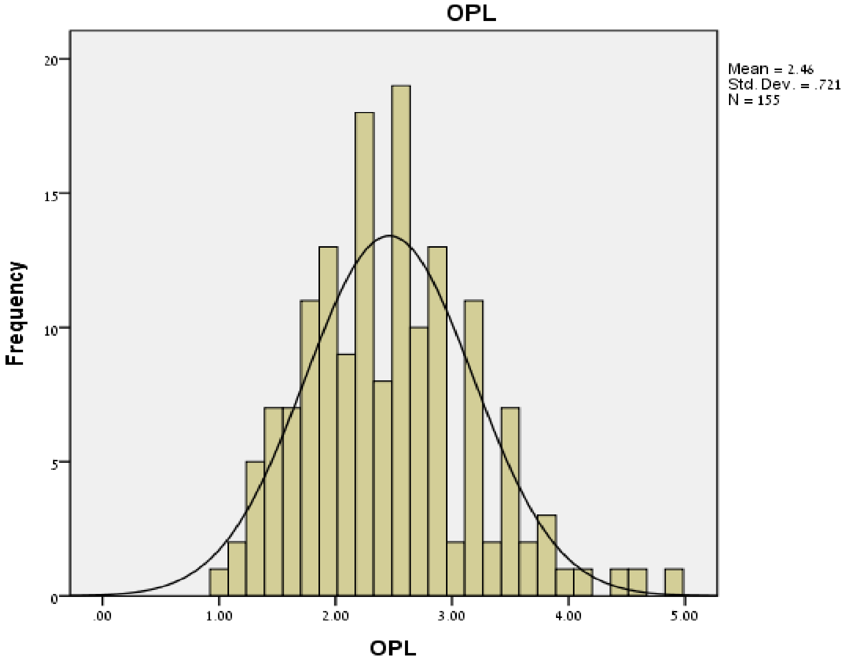

Figure 1: Schematic representation of the OPL distribution across the general sample

Regarding the dependent variable, we found that most respondents chose to protect their personal privacy, at the expense of online personalization (M=2.18, SD=0.51).

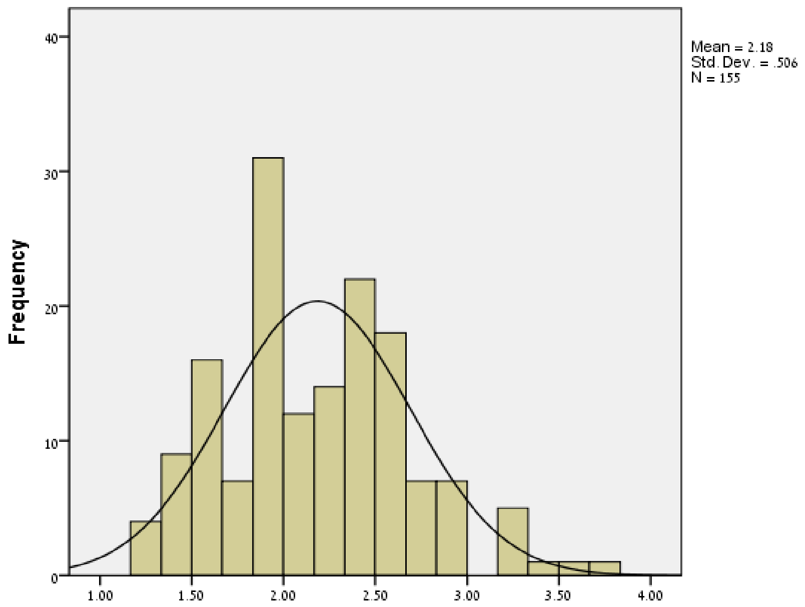

Figure 2: Schematic representation of the dependent variable distribution across the sample (5 - a string tendency towards online personalization, 1 - a strong tendency towards privacy protection)

Subsequently, we examined the role of the aforementioned factors in predicting the dependent variable, namely the users' tendency of embracing online personalization at the expense of personal privacy protection. A multivariate linear regression analysis was therefore performed, using the various independent variables described in the Methods section. The regression was conducted using the stepwise method that takes into account only the variables which were found significant.

Table 2 presents the regression coefficients for predicting users' tendency of embracing online personalization at the expense of personal privacy protection.

Table 2: The Linear Regression Coefficient for Predicting Users' Tendency of Embracing Online Personalization at the Expense of Personal Privacy Protection

Predictors	Dependent variable: Tendency to of embracing online personalization			
	β	SE	B	T
Gender	-0.18	0.81	-0.18	**-2.27***
Privacy Concern on the Web	-0.24	0.04	-1.12	**-3.07***

*** p<0.05**

Table 2 shows that the regression for predicting the users' tendency of embracing online personalization at the expense of personal privacy protection was significant, F(2,148)=7.92, p<0.001, with the predictor variables: gender and privacy concern on the Web, accounting for the explained variance.

As shown in Figure 3, as the students' privacy concern on the Web increases, their tendency of embracing online personalization at the expense of personal privacy protection decreases. Namely, the higher the students' level of privacy concern, the more they tend to protect their personal privacy at the expense of online personalization. In addition, the results indicate a higher tendency of men towards privacy protection, compared to women.

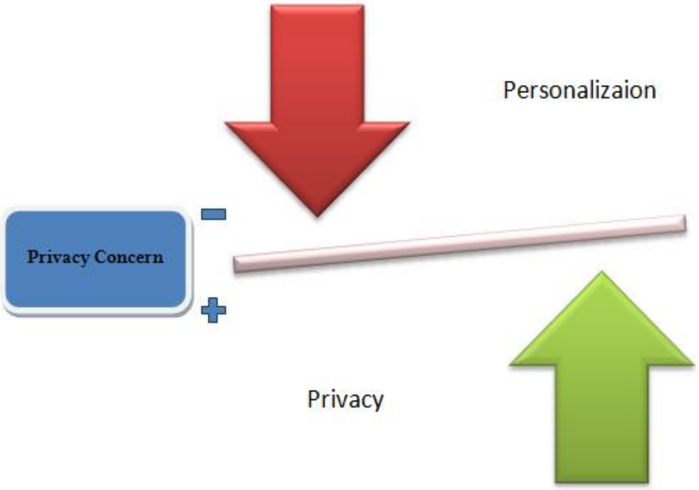

Figure 3: Schematic representation of the research findings which shows the main factor of influence (privacy concern) on the personalization-privacy tradeoff

DISCUSSION AND CONCLUSIONS

This study examined various influencing factors of users' decisions in the dilemma whether to agree to online personalization or to protect their personal privacy. The main conceptual contribution of this study was the creation of a new direct scale for assessing user decisions regarding the personalization-privacy tradeoff. Putting this new scale into practice, we found that users with a higher level of concern for online privacy chose to protect their privacy at the expense of online personalization. In a general outlook, our findings show that users tend to prefer preserving their online privacy, even if it means that their online surfing convenience will be compromised. These results seem to be in accordance with some of the above studies (Akhter, 2014; Awad & Krishnan, 2006; Castañeda & Montoro, 2007; Heirman et al., 2013; Hoffman et al., 1999; J. K. Lee & Letho, 2010; Phelps et al., 2001; Phelps et al., 2000; Potoglou et al., 2015; Taylor et al., 2009; Weinberger et al., 2017).

Another contribution of this study was the investigation of the predictive factors of the personalization-privacy tradeoff. While previous studies (Acquisti & Gross, 2006; Debatin et al., 2009; Gross & Acquisti, 2005) found that users seldom allow their privacy concerns to affect their online behavior, the findings of our research show that as the participants with a higher level of concern for online privacy tended to prefer privacy protection, at the expense of online personalization. This finding may be explained by the fact that most of the previous research that investigated the subject matter did it in the setting of social networks that encourage self-disclosure, while our research also examined privacy concerns on the Web in general. However, they may be other explanations by factors that are beyond the scope of this research.

Unfortunately, the demographic factors that were examined did not have a significant impact on the dependent variable. The only demographic factor that was found significant was gender, as men tended more towards privacy protection than women did. This finding may also be explained by the higher levels of privacy concern among men compared to women.

The social implication of this study is that it shows that by raising the concern for the protection of personal information on the Web, it is possible to influence the personalization-privacy tradeoff and encourage users to prefer privacy protection. This may be done by increasing Internet users' awareness of the online privacy threats and their knowledge of the tools designated to protect online privacy and personal information on the Web. In a broader perspective, the enhancement of users' preference of privacy protection over Web-surfing convenience may be used to mitigate online privacy paradox behavior as it can narrow the gap between users' self-reported desire to protect their online privacy, and their will to preserve the malleability of the cyberspace, including the benefits of online personalization.

Since our results were based on students' self-perceptions, which might be biased, future work should apply qualitative analysis to explore additional types and influencing factors of online privacy behavior. Furthermore, our results are limited by the relatively small study population and reflect Israeli students' behavioral patterns. As most students today are proficient, at least to some extent, in using Web applications, it might have an effect on the obtained results. In future research, an online survey may be in use in order to expand the sample population and allow universalization of the findings. In addition, we assume there are other factors for predicting these behaviors that were not examined in this paper and are subject for further research.

REFERENCES

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514. https://doi.org/10.1126/science.aaa1465

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. *Proceedings of the 6th International Workshop on Privacy Enhancing Technologies,* Cambridge, England. https://doi.org/10.1007/11957454_3

Adomavicius, G., & Tuzhilin, A. (2005). Personalization technologies: A process-oriented perspective. *Communications of the ACM, 48*(10), 83-90. https://doi.org/10.1145/1089107.1089109

Akhter, S. H. (2014). Privacy concern and online transactions: The impact of Internet self-efficacy and Internet involvement. *Journal of Consumer Marketing, 31*(2), 118-125. https://doi.org/10.1108/JCM-06-2013-0606

Andrade, E. B., Kaltcheva, V., & Weitz, B. (2002). Self-disclosure on the Web: The impact of privacy policy, reward, and company reputation. *Advances in Consumer Research, 29*, 350-353.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly, 30*(1), 13-28. https://doi.org/10.2307/25148715

Aydin, O. M., & Chouseinoglou, O. (2013). Fuzzy assessment of health information system users' security awareness. *Journal of Medical Systems, 37*(6). https://doi.org/10.1007/s10916-013-9984-x

Baek, Y. M., Kim, E. M., & Bae, Y. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior, 31,* 48-56. https://doi.org/10.1016/j.chb.2013.10.010

Baddeley, M. (2011). A behavioural analysis of online privacy and security. *Cambridge Working Papers in Economics (CWPE), 1147*, 1-26.

Barnes, B. S. (2006). A privacy-paradox: Social networking in the United States. *First Monday, 11*(9). https://doi.org/10.5210/fm.v11i9.1394

Bronstein, J. (2012). Blogging motivations for Latin American bloggers: A uses and gratifications approach. In T. Dumova (Ed.), *Blogging in the global society* (pp. 200-215). Hershey, PA: Information Science Reference. https://doi.org/10.4018/978-1-60960-744-9.ch012

Castañeda, J. A., & Montoro, F. J. (2007). The effect of Internet general privacy concern on customer behavior. *Electronic Commerce Research, 7*(2), 117-141. https://doi.org/10.1007/s10660-007-9000-y

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology & Management, 6*(2-3), 181-202. https://doi.org/10.1007/s10799-005-5879-y

Chen, H. T., & Chen, W. H. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology Behavior and Social Networking, 18*(1), 13-19. https://doi.org/10.1089/cyber.2014.0456

Cho, H. (2012). Responses to online privacy risks. In Y. Zheng (Ed.), *Encyclopedia of cyber behavior* (pp. 900-910). Hershey, PA: IGI Global. https://doi.org/10.4018/978-1-4666-0315-8.ch074

Cho, H., Lee, J., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior, 26*(5), 987-995. https://doi.org/10.1016/j.chb.2010.02.012

Costante, E., den Hartog, J., & Petkovic, M. (2012). On-line trust perception: What really matters. *Proceedings of the 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST 2011),* Milan, Italy.

Culnan, M. J. (1993). "How Did They Get My Name?" An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly, 17*(3), 341-361. https://doi.org/10.2307/249775

Culnan, M. J., & Armstrong P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104-115. https://doi.org/10.1287/orsc.10.1.104

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83-108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285-297. https://doi.org/10.1002/ejsp.2049

Eckersley, P. (2010). How unique is your web browser? In M. J. Atallah & N. J. Hopper (Eds.), *Privacy Enhancing Technologies, 10th International Symposium (PETS' 2010): Vol. 6205*. Lecture Notesin Computer Science (pp. 1-18). Berlin, Heidelberg: Springer-Verlag. https://doi.org/10.1007/978-3-642-14527-8_1

Ellison, N., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends": Exploring the relationship between college students' use of online social networks and social capital. *Journal of Computer-Mediated Communication, 12*(4), 1143-1168. https://doi.org/10.1111/j.1083-6101.2007.00367.x

Fogel, J., & Nehmad, E. (2009).Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*(1), 153-160. https://doi.org/10.1016/j.chb.2008.08.006

Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy & Marketing, 10*(1), 149-166.

Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: Consumers' awareness and concerns. *Journal of Consumer Marketing, 19*(4). https://doi.org/10.1108/07363760210433627

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES '05)*, Alexandria, VA. https://doi.org/10.1145/1102199.1102214

Guo, X. T., Zhang, X. F., & Sun, Y. Q. (2016). The privacy-personalization in m Health services acceptance of different age groups. *Electronic Commerce Research and Applications, 16*, 55-65. https://doi.org/10.1016/j.elerap.2015.11.001

Hann, I. H., Hui, K. L., Lee, T. S. Y, & Png, I. P. L. (2002). Online information privacy: Measuring the cost-benefit tradeoff. *Proceedings of the 23rd International Conference on Information Systems (ICIS 2012)*, Barcelona, Spain.

Heirman, W., Walrave, M., & Ponnet, K. (2013). Predicting adolescents' disclosure of personal information exchange for commercial incentives: An application of an extended theory of planned behavior. *Cyberpsychology Behavior and Social Networking, 16*(2), 81-87. https://doi.org/10.1089/cyber.2012.0041

Hoffman, D. L., Novak, T. P., & Peralta, M. A. (1999). Information privacy in the marketplace: Implications for the commercial uses of anonymity on the Web. *The Information Society: An International Journal, 15*(2), 129-139. https://doi.org/10.1080/019722499128583

Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising, 10*(2), 28-45. https://doi.org/10.1080/15252019.2010.10722168

Jacobs, R. S., Hyman, M. R., & McQuitty, S. (2001). Exchange-specific self-disclosure, social self-disclosure, and personal selling. *Journal of Marketing Theory and Practice, 9*(1), 48-62. https://doi.org/10.1080/10696679.2001.11501885

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies, 63*(1-2), 203-227. https://doi.org/10.1016/j.ijhcs.2005.04.019

Joinson, A. N., Reips, U. D., Buchanan, T., & Paine Schofield, C. B. (2010). Privacy, trust, and self-disclosure online. *Human-Computer Interaction, 25*(1), 1-24. https://doi.org/10.1080/07370020903586662

Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on social network services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies, 71*(9), 862-877. https://doi.org/10.1016/j.ijhcs.2013.01.005

Lee, J. K., & Letho, X. (2010). E-personalization and online privacy features: The case with travel websites. *Journal of Management and Marketing Research, 4*(March), 1-14. Retrieved from http://www.aabri.com/manuscripts/09347.pdf

Lee, J. M., & Rha, J. Y. (2016). Personalization-privacy paradox and consumer conflict with the use of location-based mobile commerce. *Computers in Human Behavior, 63*, 453-462. https://doi.org/10.1016/j.chb.2016.05.056

Leon, P. G., Blase, U., Wang, Y., Sleeper, M., Balebako, R., Shay, R., et al. (2013). What matters to users? Factors that affect users' willingness to share information with online advertisers. *Proceedings of the 9th Symposium on Usable Privacy and Security (SOUPS '13),* Newcastle, United Kingdom. https://doi.org/10.1145/2501604.2501611

Li, T., & Unger, T. (2012). Willing to pay for quality personalization? Trade-off between quality and privacy. *European Journal of Information Systems, 21*(6), 621-642. https://doi.org/10.1057/ejis.2012.13

Mayer, J. R. (2009). *"Any person... a pamphleteer:" Internet anonymity in the age of Web 2.0*. Undergraduate Senior Thesis, Princeton University, Princeton, NJ.

Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on Web site trust and disclosure. *Communication Research, 33*(3), 155-179. https://doi.org/10.1177/0093650206287076

Millett, L. I., Friedman, B., & Felten, E. (2001). Cookies and Web browser design: Toward realizing informed consent online. *Proceedings of the SIGCHI conference on Human Factors in Computing Systems (CHI '01)*, Seattle, WA. https://doi.org/10.1145/365024.365034

Milne, G. R. (2000). Privacy and ethical issues in database/interactive marketing and public policy: A research framework and overview of the special issue. *Journal of Public Policy & Marketing, 19* (1), 1-6. https://doi.org/10.1509/jppm.19.1.1.16934

Milne, G. R., & Boza, M. E. (1999). Trust and concern in consumers: Perceptions of marketing information management practices. *Journal of Interactive Marketing, 13*(1), 5-24. https://doi.org/10.1002/(SICI)1520-6653(199924)13:1<5::AID-DIR2>3.0.CO;2-9

Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social-contract framework. *Journal of Public Policy & Marketing, 12*(2), 206-215.

Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers' protection of online privacy and identity. *Journal of Consumer Affairs, 38*(2), 217-232. https://doi.org/10.1111/j.1745-6606.2004.tb00865.x

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100-126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Nunnally, J., & Bernstein, I. (1994). *Psychometric theory* (3rd ed.). New York: McGraw-Hill.

O'Neill, D. (2001). Analysis of Internet users' level of online privacy concerns. *Social Science Computer Review, 19*(1), 17-31. https://doi.org/10.1177/089443930101900103

Paine, C., Reips, U. D., Steiger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies, 65*(6), 526-536. https://doi.org/10.1016/j.ijhcs.2006.12.001

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215-236. https://doi.org/10.1177/0093650211418338

Phelps, J., D'Souza, G., & Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing, 15*(4), 2-17. https://doi.org/10.1002/dir.1019

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy and Marketing, 19*(1), 27-41. https://doi.org/10.1509/jppm.19.1.27.16941

Potoglou, D., Palacios, J. F., & Feijóo, C. (2015). An integrated latent variable and choice model to explore the role of privacy concern on stated behavioral intentions in e-commerce. *Journal of Choice Modelling, 17*, 10-27. https://doi.org/10.1016/j.jocm.2015.12.002

Rainie, L., Kiesler, S., Kang, R. & Madden, M. (2013). Anonymity, privacy, and security online. *Pew Research Center's Internet & American Life Project, September 2013*. Retrieved from http://www.pewinternet.org/files/oldmedia//Files/Reports/2013/PIP_AnonymityOnline_090513.pdf

Rognehaugh, R. (1999). *The health information technology dictionary.* Gaithersburg, MD: Aspen.

Senecal, S., & Nantel, J. (2004). The influence of online product recommendations on customers' online choices. *Journal of Retailing, 80*(2), 159-169. https://doi.org/10.1016/j.jretai.2004.04.001

Sheehan, K. B. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing, 18*(4), 24-38. https://doi.org/10.1002/(SICI)1520-6653(199923)13:4<24::AID-DIR3>3.0.CO;2-O

Sheehan, K. B. & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing, 19*(1), 62-73. https://doi.org/10.1509/jppm.19.1.62.16949

Sheng, H., Nah, F., & Siau, K. (2008). An experimental study in U-commerce adoption: The impact of personalization and privacy concerns. *Journal of Associations for Information Systems, 9*(6), 344-376. https://doi.org/10.17705/1jais.00161

Sutanto, J., Palme, E., Tan, C. H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on Smartphone users. *MIS Quarterly, 37*(4), 1141-1164. https://doi.org/10.25300/MISQ/2013/37.4.07

Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication, 19*(2), 248-273. https://doi.org/10.1111/jcc4.12052

Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An analysis of information security awareness within home and work environments. *Proceedings of the 5th International Conference on Availability, Reliability, and Security*, Krakow, Poland. https://doi.org/10.1109/ARES.2010.27

Taylor, D. G., Davis, D. F., & Jillapalli, R. (2009). Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research, 9*(3), 203-223. https://doi.org/10.1007/s10660-009-9036-2

Toch, E., Wang, Y., & Cranor, L. F. (2012). Personalization and privacy: A survey of privacy risks and remedies in personalization-based systems. *User Modeling and User-Adapted Interaction, 22*(1-2), 203-220. https://doi.org/10.1007/s11257-011-9110-z

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., et al. (2015). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In S. Gutwirth, R. Leenes & P. de Hert (Eds.), *Reforming European data protection law* (pp.333-365). Netherlands: Springer. https://doi.org/10.1007/978-94-017-9385-8_14

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science Technology Society, 28*(1), 20-36. https://doi.org/10.1177/0270467607311484

Turow, J., King, J., Hoofnagle, C. J., Bleakley, A., & Hennessy, M. (2009). Americans reject tailored advertising and three activities that enable it. *SSRN eLibrary*, 1-27. https://doi.org/10.2139/ssrn.1478214

Weinberger, M., Bouhnik, D., & Zhitomirsky-Geffet, M. (2017). Factors affecting students' privacy paradox and privacy protection behavior. *Open Information Science, 1*(1), 1-18. https://doi.org/10.1515/opis-2017-0002

Weinstein, N. D. (1989). Optimistic biases about personal risks. *Science, 246*(4935), 1232-1233. https://doi.org/10.1126/science.2686031

Wills, C. E., & Zeljkovic, M. (2011). A personalized approach to web privacy: Awareness, attitudes and actions. *Information Management & Computer Security, 19*(1), 53-73. https://doi.org/10.1108/09685221111115863

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems, 51*(1), 42-52. https://doi.org/10.1016/j.dss.2010.11.017

Yoon, S. (2002). The antecedents and consequences of trust in online-purchase decisions. *Journal of Interactive Marketing, 16*(2), 47-62. https://doi.org/10.1002/dir.10008

Zafeiropoulou, A. M., Millard, D. E., Webber, C., & O'Hara, K. (2013). Unpicking the privacy paradox: Can structuration theory help to explain location-based privacy decisions? *Proceeding of the 5th annual ACM Web science conference*, Paris, France. https://doi.org/10.1145/2464464.2464503

Zhitomirsky-Geffet, M., & Bratspiess, Y. (2014). Professional information disclosure on social networks: the case of Facebook and LinkedIn in Israel. *Journal of the Association for Information Science and Technology, 67*(3), 493-504. https://doi.org/10.1002/asi.23393

APPENDIX

Questionnaire

Part A – Demographic Details

1. Gender: M / F
2. Year of Birth
3. Place of Birth
4. Academic Institution
5. Field of Study
6. Do you have either an academic or an occupational background on the fields of the Internet and/or information security?

Yes / No

7. How would you describe your level of Internet / computer proficiency? (Please circle)
    a. No proficient at all.
    b. Low proficiency.
    c. Average proficiency.
    d. High proficiency.
    e. Very high proficiency.

Part B – Awareness of the online privacy threats and attitudes to privacy protection

1. How anonymous do you feel while surfing the Web? (Please circle)
    a. Not anonymous at all.
    b. Partially anonymous.
    c. Moderately anonymous.
    d. Highly anonymous.
    e. Very highly anonymous.

2. Which of the following do you believe a website you visit could determine? (Multiple choices are permitted)
    a. Your operating system.
    b. Your computer type.
    c. Your Web-browser.
    d. Your IP address.
    e. Your browsing history.
    f. Your location.

3. In your opinion, how exposed are you to other users on the Internet? (Please circle)
    a. Completely exposed.
    b. Highly exposed.
    c. Moderately exposed.
    d. Lowly exposed.
    e. Not exposed at all.

4. Which of the following do you believe other users could determine? (Multiple choices are permitted)
    a. Your operating system.
    b. Your computer type.
    c. Your Web-browser.
    d. Your IP address.
    e. Your browsing history.
    f. Your location.

5. How concerned are you about the protection of your privacy on <u>the Web</u>? (Please circle)
    a. Not concerned at all.
    b. Slightly concerned.
    c. Moderately concerned.
    d. Highly concerned.
    e. Very highly concerned.

6. How concerned are you about the protection of your privacy when using <u>social network sites</u>? (Please circle)
    a. Not concerned at all.
    b. Slightly concerned.
    c. Moderately concerned.
    d. Highly concerned.
    e. Very highly concerned.

7. What is your level of belief in your own ability to browse the Web anonymously if necessary? (Please circle)
    a. No belief at all.
    b. Low level of belief.
    c. Low to moderate level of belief.
    d. Moderate level of belief.
    e. Moderate to high level of belief.
    f. High level of belief.
    g. Very high level of belief.

Part C – Online privacy literacy

1-8. What is your level of knowledge of each of the following privacy-enhancing tools? (Please circle for each tool). The possible answers for every tool separately were on the 1-5 Likert scale: 1) No knowledge of. 2) Low level of knowledge. 3) Moderate level of knowledge. 4) High level of knowledge. 5) Very high level of knowledge.

a. Logging-out from online accounts
b. Clearing history and other browsing details
c. Blocking cookies
d. Browsing via an Incognito Mode
e. IP spoofing
f. Using proxy servers.
g. Using VPN (Virtual Private Networks)
h. Using TOR (The Onion Routing)

9-16. What is your level of usage of each of the following privacy-enhancing tools? (Please circle for each tool). The possible answers for every tool were: 1) No usage at all. 2) Low level of usage.3) Moderate level of usage. 4) High level of usage. 5) Very high level of usage.

a. Logging-out from online accounts
b. Clearing history and other browsing details
c. Blocking cookies
d. Browsing via an Incognito Mode
e. IP spoofing
f. Using proxy servers
g. Using VPN (Virtual Private Networks)
h. Using TOR (The Onion Routing)

Part D – Personalization vs. privacy scale

Please circle your level of agreement with each of the following statements: 1) Disagree; 2) Slightly agree; 3) Moderately agree; 4) Highly agree; 5) Very highly agree.

1. I do not tend to use the option "save password", to protect my personal data, when it is offered to me by the Web browser.
2. I tend to download software and content that I find to be important, even from unfamiliar websites.
3. I tend to personalize my web-browser by installing extensions which are important for me, even when I know it may jeopardize my privacy.
4. I will be willing to submit personal information to websites, in order to get online advertisements that are customized to my personal interests despite on my online privacy.
5. I will be willing to submit personal information to social networks applications, in order to get messages and services that are customized to my personal interests despite the threat on my privacy.
6. I tend to install different extensions on my web-browser, even when it requires me to submit personal details.
7. I will be willing to submit information at e-commerce websites regarding my personal interests, in order to get discounts for products I desire.
8. I will be willing to submit personal information on websites, for the purpose of online advertising, in exchange for monetary compensation, despite the threat on my privacy.

9. I will be willing to disclose personal information on social networks despite the threat on my privacy, in order to gain better social interaction, social endorsement, to receive interesting services and information, or any other benefit.
10. In general, I prefer to comfortably use the Internet, even at the expense of protecting my personal information.
11. I tend to choose the option "save my credit card" when it is offered to me by the browser, while performing an online transaction.
12. I tend to download software and services aim to improve the performance of my computer / Web browser, even from seemingly unprotected websites.
13. I will not submit personal information on an unsecured website to protect my privacy, even if it offers me a service I desire.
14. I tend to visit websites that interest me, even though I know for certain they are using "cookies" for the purpose of personalized advertising which might pose a threat on my online privacy.
15. In general, I prefer to protect my information security, even at the expense of my comfortable use of the Internet.

Biographies

Maor Weinberger is a doctoral student at the Information Science Department in Bar-Ilan University (BIU), Israel. His professional interests include online privacy and anonymity and information security.

Dr. Dan Bouhnik is currently a lecturer in the Information Science department in Bar Ilan University (BIU) and in the Computer Science department in Jerusalem College of Technology (JCT) in Israel. He taught Computer Science and Logic in High Schools both in Israel and the United States. Dan is the author of a number of books used for teaching Advanced Computer Sciences in High Schools and his professional interests include virtual learning and its effect on the thinking process.