Research Article **Open Access**

Maor Weinberger*, Dan Bouhnik, Maayan Zhitomirsky-Geffet

Factors Affecting Students' Privacy Paradox and Privacy Protection Behavior

DOI 10.1515/opis-2017-0002
Received December 2, 2016; accepted April 18, 2017

Abstract: In this exploratory study, we investigate the factors affecting two opposite types of online privacy behavior: 1) online privacy paradox, i.e. a mismatch between users' online privacy attitudes and their online privacy behavior; and 2) online privacy protection. To assess these two types of behavior, we devised a new direct scale comprising 25 items explicitly highlighting benefits and risks of the examined behavior. Various factors related to online privacy and anonymity were considered in light of the existing theories on online privacy behavior. To this end, 169 students from different fields of study in Israeli academia were administered closed-ended questionnaires. The multivariate linear regression analysis showed that information science students had a significantly lower tendency toward privacy paradox behavior compared to other students. In addition, we found that as the participants' privacy concern and online privacy self-efficacy increase, their tendency toward privacy paradox behavior decreases. However, surprisingly, there was no significant association between privacy protection behavior and high technical skills or online privacy literacy. This research has social implications for academia and the general public, as it shows that the protection of online privacy does not depend on technical knowledge or complicated tool usage, but rather can be achieved by raising users' online privacy concern and self-efficacy.

Keywords: online privacy, privacy paradox, privacy concern, online privacy literacy, online privacy self-efficacy

1 Introduction

Anonymity – "the state of being not identifiable within a set of subjects" (Pfitzmann & Köhntopp 2001: 3) – is one of the unique features that the Internet provides, as it presents an exclusive platform which allows a user to shape the setting in which s/he operates (Mayer, 2009). Inside this uniquely-shaped setting, the user holds the privilege not to expose his/her personal details, and choose an alias or a pseudonym (Qian & Scott, 2007). Online privacy is defined as "an individual's ability to determine when, how, and to what extent personal information is disseminated to others in the virtual environment" (Metzger 2007; as seen in Cho 2012: 901). Thus, online anonymity is a unique feature supposed to lead to the maximal level of privacy and personal detail protection, since it ensures the individual's ability to keep and protect his/her identity. However, it seems that the Internet has created a conflict regarding the concept of privacy, since technology (including software and different applications), which enable users to exercise their online preferences, at the same time allows service providers and other users to collect their personal information, in many cases without consent (Barnes, 2006). Thus, users are constantly faced with a dilemma: whether to choose online privacy over personalization, usability and interactivity.

***Corresponding author: Maor Weinberger,** Bar-Ilan University, Ramat-Gan, Israel, E-mail: maor89@gmail.com
Dan Bouhnik, Jerusalem College of Technology, Jerusalem, Israel
Maayan Zhitomirsky-Geffet, Bar-Ilan University, Ramat-Gan, Israel

This discrepancy has been investigated in many studies of user attitudes towards online privacy, anonymity and self-disclosure, e.g. privacy concern, self-efficacy and threat awareness (Fogel & Nehmad 2009; Graeff & Harmon 2002; Hoy & Milne 2010; Milne, Rohm & Bahl 2004; O'Neill 2001; Paine et al. 2007; Sheehan 1999; Taddicken 2014; Wills & Zeljkovic 2010). Virtually all studies found that users are concerned with their online privacy and wish to protect it (e.g. Paine et al. 2007; Wills & Zeljkovic 2010). However, the results regarding the actual behavior and its correlation with attitudes and intents reported in previous research are mixed and inconclusive. Some studies found that users' behavior was consistence with their attitudes and they chose to protect their privacy even if this might limit their usability of the cyberspace (Akhter 2014; Awad & Krishnan 2006; Castañeda & Montoro 2007; Heirman, Walrave & Ponnet 2013; Hoffman, Novak & Peralta 1999; Lee & Letho 2010; Phelps, Nowak & Ferrell 2000; Phelps, D'Souza & Nowak 2001; Potoglou, Palacios & Feijóo 2015; Taylor, Davis & Jillapalli 2009). But, others showed that despite their attitudes and intents, users voluntarily disclose personal information about themselves on the Internet (Acquisti & Gross 2006; Bronstein 2012; Debatin, Lovejoy, Horn & Hughes 2009; Dienlin & Trepte 2015; Guo, Zhang & Sun 2016; Gross & Acquisti 2005; Jensen, Potts & Jensen 2005; Lee, Park & Kim 2013; Norberg, Horne & Horne 2007; Taddicken 2014; Tufekci 2008; Zafeiropoulou, Millard, Webber & O'Hara 2013; Zhitomirsky-Geffet & Bratspiess 2014). This mismatch between users' online privacy attitudes and their actual behavior, when they prefer to utilize the malleability of cyberspace at the expense of privacy and anonymity protection, was termed the "privacy paradox" (Barnes 2006, Norberg et al. 2007).

Several hypotheses have been suggested to explain users' online self-disclosure behavior, i.e. self-exposure of personal details to others voluntarily (for example, on social networks and e-commerce sites). These hypotheses include 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). Park (2013) suggested that online privacy literacy (OPL) might serve as a "stopgap" between online privacy attitudes and online privacy behavior and help decrease the online privacy paradox behavior. Another hypothesis described in the literature is 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). In addition, a theory of optimistic bias, also known as unrealistic optimism or comparative risk judgments (Weinstein 1989), was considered as an explanation of online self-disclosure where users perceive themselves to be less vulnerable to these risks than their peers (Baek, Kim & Bae 2014; Cho 2012; Cho, Lee & Chung 2010).

Based on the aforementioned theories and inspired by recent societal discussion about privacy concerns and user behavior on the Web (for example: Facebook's recurring privacy issues as discussed in https://www.theguardian.com/technology/2016/jun/29/facebook-privacy-secret-profile-exposed), our primary objective in this exploratory study was to examine possible predictive factors affecting users' tendency toward privacy paradox behavior. In addition, we also measured and explored the factors of the opposite behavior type – privacy protection behavior. One possible reason for mixed results in the literature regarding the tendency to privacy paradox is that there is no direct scale for the assessment of this phenomenon. Previous studies measured the attitudes toward online privacy and the actual behavior of online self-disclosure as two separate variables and then compared them to assess the tendency toward the privacy paradox. Kokolakis (2017) has argued that, based on the logical theories the literature provides, the dichotomy between privacy attitude and behavior perhaps should not be considered a "paradox" anymore, but rather a complex phenomenon which has not been fully explained yet. Hence, one of the main contributions of this research is that we devised and applied a direct scale to measure the level of privacy paradox behavior as a single variable. The scale was based on previous studies on online privacy behavior (e.g. Aydin & Chouseinoglou 2013; Chellappa & Sin 2005; Talib, Clarke & Furnell 2010).

For the purposes of this research, we conducted a user study with 169 students from Israeli academia, who were administered a closed-ended questionnaire comprising 56 questions on online privacy attitudes and behavior. Further, the questionnaire was analyzed using multivariate linear regression models to determine the predictive factors of users' tendency toward the privacy paradox and privacy protection behavior.

2 Related Work

2.1 Types of online privacy and anonymity threats

Information that might expose users' identity on the Internet could potentially exist at different layers of the network. The most available and thus threatened piece of information is the user's IP address, which is easily acquirable and provides external access to users' information. Another common method for online surveillance, even without IP detection, is the tracking cookie (Mayer 2009). 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 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, Friedman & Felten 2001). Many popular web browsers provide users with the capability of exclusive shaping of the 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 that is different from the settings of any other user. This uniquely-shaped web browsing environment is effectively a digital fingerprint that might also be used by external parties for exposing the user's identity (Eckersley 2010; Mayer 2009).

2.2 The tradeoff between online personalization and self-disclosure

The tradeoff between online personalization and privacy protection is a widely-explored topic in the context of electronic commerce (e.g. Awad & Krishnan 2006; Chellappa & Sin 2005; Culnan 1993; Goodwin 1991; Lee & Letho 2010; Lee & Rha 2016; Milne & Gordon 1993). Chellappa & Sin (2005) argue that personalization – the shaping of the user's online environment according to his/her personal preferences – helps improve customer satisfaction, predict demand, develop customer loyalty and increase cross-selling possibilities. The consumer can upload his/her personal details (e.g. name, address and preferred mode of delivery) to an online profile and use them repeatedly in future purchases. The consumer can also create his/her own list of products of interest and set an instant alert to be sent when the prices drop or when an auction comes to close. In addition, the consumer can ask for product suggestions; compatible with a predefined list on his/her profile or purchase history. However, personalization also requires a certain level of self-disclosure.

Self-disclosure was also widely investigated in the setting of social networks. Social networks encourage self-disclosure by their very nature. The most important benefit of self-disclosure on social networks is probably the social capital gained from creating and maintaining interpersonal relationships and friendships (Ellison, Steinfield & Lampe 2007). Ibrahim (2008) claims that in social networks personal information becomes social capital which is traded and exchanged. This might be achieved more easily when privacy settings are less strict and the profile information is not restricted (Acquisti & Gross 2006; Debatin et al. 2009; Gross & Acquisti 2005). Thus, Gross & Acquisti (2005) found that 91% of the respondents uploaded a profile picture to their Facebook account, 88% of the respondents shared their date of birth, around 40% posted their landline phone number (including approximately 30% who posted their cell phone number as well), and about 51% stated their current home address. In addition, most of the respondents revealed their sexual preferences (male or female) and their relationship status (single, married, etc.), while about 63% of the non-single shared the identity of their partner. Furthermore, 89% of the profile names examined were found to be genuine, with 3% giving only their first name and only 8% giving a fake name. However, a later study (Fogel & Nehmad 2009) reported a decrease in the extent of self-disclosure on social networks, where, for example, only about 10% of the respondents published their home address. Recently, Taddicken (2014) examined self-disclosure on social networks and found that about 75% of the participants revealed factual information, such as surname, date of birth and occupation. Sensitive information was found to be less frequently disclosed, but was still revealed in

great extent – about 67% posted personal pictures (about 45% without any access restriction) and about half of the participants shared personal experiences. Likewise, Lee et al. (2013) found that users actively share personal information despite their concerns, due to the expected benefits of information sharing. Therefore, it seems that self-disclosure on social networks did not decrease substantially throughout the years, despite constant reports of high privacy concerns of the users.

Numerous studies found that even though social network users recognize the importance of online privacy protection (Barnes 2006, Debatin et al. 2009; Gross & Acquisti 2005; Livingston 2008; Tufekci 2008), in practice, they usually prefer not to limit the social gains of self-disclosure (Acquisti & Gross 2006; Acquisti & Grossklags 2004; Debatin et al. 2009; Dienlin & Trepte 2015; Gross & Acquisti 2005; Ellison et al. 2011; Lee et al. 2013; Livingston 2008; Tufekci 2008, Stutzman & Kramer-Duffield 2010).

Recent studies (Eastin et al. 2016; Lee & Rha 2016; Sutanto, Palme, Tan & Phang, 2013; Xu, Luo, Carroll & Rosson, 2011; Zafeiropoulou et al., 2013) have investigated the existence of the privacy paradox among mobile application usage, particularly among location-based mobile commerce. Eastin et al. (2016) found that even though concerns about control and unauthorized access to personal information have significant negative influence on mobile commerce activity, concerns over identity theft did not impact e-commerce behavior, consistent with the privacy paradox phenomenon. Likewise, Zafeiropoulou et al. (2013) found evidence that supports the existence of privacy paradox for location data.

Thus, it seems that there is a constant tension between maximal utilization of online tools and protection of online privacy and anonymity.

2.3 Factors of online self-disclosure

Previous works have mostly explored the factors affecting self-disclosure on e-commerce and social network sites. The following types of factors have been examined in the literature:

1. Socio-demographic factors such as gender and age (Baddeley 2011; Castañeda & Montoro, 2007; Milne & Boza 1999; Phelps et al. 2000). Numerous studies found that women publish more personal information than men (Acquisti & Gross 2006; Feng & Xie 2014; Fogel & Nehmad 2009; Hoy & Milne 2010; Kolek & Saunders 2008; Tufekci 2008), and rarely adopt privacy protection behavior (Milne, Rohm & Bahl 2004; Sheehan 1999; Yao & Linz 2008).
2. Users' OPL (Trepte et al. 2015), i.e. their knowledge of the tools available to protect their online information and 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). The studies suggest that higher OPL leads to lower levels of self-disclosure, while lower OPSE has the opposite effect.
3. Perceptions, attitudes and beliefs about online self-disclosure in e-commerce and social network sites (Acquisti, Brandimarte & Loewenstein 2015; Baddeley 2011; Chellappa & Sin 2005; Culnan 1993; Culnan & Armstrong 1999; Joinson, Reips & Buchanan 2010; Milne & Boza 1999; Phelps et al. 2000; Phelps et al. 2001; Yoon 2002). Acquisti et al. (2015) claimed that self-disclosure might be an outcome of users' unawareness of the information they are sharing or the ways it can be used. Thus, Hoffman et al. (1999) indicated that users, when explicitly aware of malpractices by sites, tend not to disclose information. Likewise, later studies found that consumers concerned with their information disclosure usually do not agree to apply profile personalization (Awad & Krishnan 2006; Lee & Letho,2010) or engage in e-commerce (Akhter 2014; Castañeda & Montoro 2007; Heirman, Walrave & Ponnet 2013; Phelps et al. 2000; Phelps et al. 2001; Potoglou, Palacios & Feijóo 2015; Taylor, Davis & Jillapalli 2009). Conversely, several studies found that privacy concern and awareness did not influence users' actual self-disclosure on social network sites (Acquisti & Gross 2006; Acquisti & Grossklags 2004; Debatin et al. 2009; Gross & Acquisti 2005; Livingston 2008; Tufekci 2008). A possible suggested reason is that the illusion of invulnerability and optimistic bias may cause users to refrain from using privacy protection tools, despite their high privacy concerns (Cho 2012).

4. Website-related variables, such as the 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 et al. 2010; Leon et al. 2013; Metzger 2006; Phelps et al. 2000; Sheehan & Hoy 2000). These studies found that higher perception of the website's ethics enhances the users' trust and willingness for self-disclosure.
5. Benefits of self-disclosure (Acquisti & Grossklags 2004; Awad & Krishnan 2006; Beuker 2016; Culnan & Armstrong 1999; Debatin et al. 2009; Phelps et al. 2000; Trepte et al. 2015; Xu, Michael & Chen 2013). It was found that the consumer's willingness to disclose personal information increases as he/she perceives it as more beneficial. Li & Unger (2012) found that the more personalization is perceived by the consumer to be effective, the higher the level of self-disclosure.

In the present study, we tried to resolve the disagreements among the aforementioned works regarding privacy paradox behavior. In addition, we explored the factors affecting this behavior in light of the factors for self-disclosure described above. Thus, the main research questions examined in this study were:

1. To what extent do users choose to forfeit their privacy for increased cyberspace utilization? In other words, to what extent does uses and gratification theory apply to online privacy behavior?
2. What demographic factors are related to the online privacy paradox or privacy protection behavior?
3. What users' attitudes toward online privacy and anonymity are related to the online privacy paradox or privacy protection behavior? Do users' attitudes reflect the optimistic bias theory?
4. Is online privacy literacy (OPL) related to the online privacy paradox or privacy protection behavior, as suggested by the knowledge gap hypothesis?
5. What are the main predictive factors of the tendency toward the privacy paradox and of privacy protection behavior?

Table 1 summarizes the main theories discussed in this paper and the potential factors explaining online privacy behaviors. Additionally mentioned are examples of past studies that are either substantiate or examine each of these theories.

Table 1. Online privacy theories aligned to potential factors of online privacy behaviors

Theory	Explanation	Factor	Studies (e.g.)
Uses and gratification theory	Lack of willingness to forfeit the benefits of information disclosure	Privacy threat awareness; OPSE; Privacy concern	Acquisti & Gross 2006; Debatin et al. 2009; Xu et al. 2013
Optimistic bias theory	Misperception of Internet users to be less vulnerable to cybersecurity risks than others		Baek et al. 2014; Cho 2012; Cho, Lee & Chung 2010
Knowledge gap hypothesis	Lack of awareness of the risks posed by information disclosure	Gender; OPL level; Field of study	Park 2013; Trepte et al. 2015

These works explored factors affecting online self-disclosure. However, to the best of our knowledge, no previous work directly assessed and determined the main factors affecting the privacy paradox and privacy protection behavior. In particular, in this study we tested a variety of factors such as: gender, OPL level and field of study to assess the knowledge gap effect; and online privacy attitudes (e.g. privacy threat awareness, OPSE and privacy concern) to evaluate the influence of optimistic bias and uses and gratification theory on online privacy behavior. In addition, as opposed to previous research that examined the privacy paradox behavior in particular settings (e.g. electronic commerce or social network sites), our research examined this issue from a wider perspective, with no thematic limitation. Figure 1 demonstrates the research framework with various factors and theories whose relationships to online privacy paradox and privacy protection

behaviors are examined in this study.

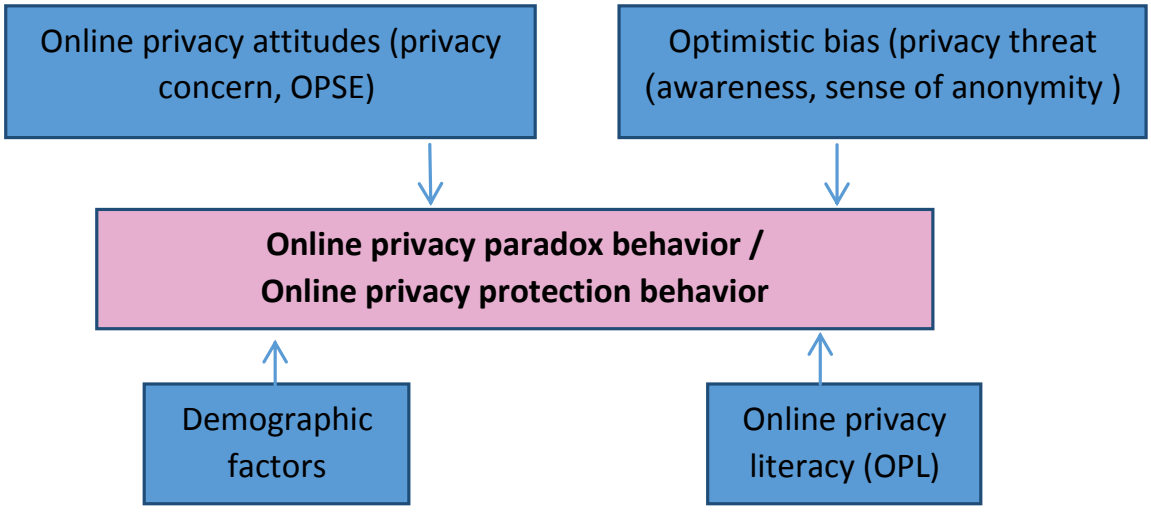

Figure 1. Schematic representation of the research framework which shows potential factors of influence (blue rectangles) of the privacy paradox and privacy protection behaviors (pink rectangles).

3 Methods

3.1 Sample Population

This study was conducted among 169 students from three different Israeli academic departments: 1) Accounting and Business Management at the Jerusalem College of Technology; 2) Information Science at Bar-Ilan University; and 3) Computer Science and Engineering at the Jerusalem College of Technology. The questionnaires were handed out throughout the academic courses of the 2014–15 school year, and were filled out in class. We note that all three programs are considered somewhat technologically oriented, but differ in the level and number of Internet and computer system courses. Thus, Accounting and Business Management students take only three Internet and computer–oriented courses and not a single course related to information protection and security. Information science students take many more Internet and computer–oriented courses (more than half of the courses), some of them purely dedicated to information security threats and tools. Finally, Computer Science and Engineering students naturally take the highest level and number of Internet and computer–oriented courses, including several specialized courses dealing with algorithms and the implementation of information security techniques.

As the sample population consisted of students alone, there is a relatively small range of ages. There was, however, equal gender distribution between different age groups, education levels and fields of study. Thus, demographic profiles and technical backgrounds of men and women could be considered similar and were not predicted to influence the inter-gender analysis presented in the next subsection. 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 2 presents the demographic characteristics of the sample.

Table 2. Demographic characteristics of the sample (N=169).

	Variable	Percentage %	N
Gender	Male	42%	71
	Female	58%	98
Age*	21>	31.36%	53
	21-25	39.64%	67
	>25	28.99%	49
Education*	Bachelor's degree	88.8%	150
	Master's degree	11.2%	19
Field of study	Accounting and Business Management	23.69%	40
	Information Science	32.54%	55
	Computer Science and Engineering	34.79%	74

* Since the sample population was comprised mostly of Bachelor's degree students, differences according to age and education level were not tested in this study.

In addition, the sample was approximately equally distributed by age and gender in the different fields of study.

3.2 Research variables and validation method

For the purposes of the study, a questionnaire of 56 items on online privacy behavior and its affecting factors was composed (as shown in Appendix A). Based on the questionnaire the following factors of the privacy paradox and privacy protection behavior as independent research variables were considered:

1) Gender (male was coded as 0 and female as 1);
2) To assess the influence of the knowledge gap hypothesis, the following variables were defined:
   a. Students' field of study (Part A, Item 5);
   b. The level of users' online literacy (Part A, Items 6,7) 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 and level of proficiency in the fields of computers and the Internet, based on their self-reports: low; moderate; high.
   c. The level of users' OPL was measured via two different indicators based on Park's (2013) technical skills parameter: 1) The level of knowledge of privacy-enhancing tools (part C, items 1-8); 2) The level of usage of privacy-enhancing tools (Part C, items 9-16). The participants were questioned about eight different privacy-enhancing tools examined in Rainie et al. (2013): 1) Logging-out from the online accounts; 2) Clearing of history and other browsing details; 3) Blocking cookies; 4) Browsing via Incognito Mode; 5) IP spoofing; 6) Using proxy servers; 7) Using VPN; 8) Using TOR.
   Each subject's responses were 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 $\alpha = 0.86$ and for the indicator measuring the level of usage of privacy-enhancing tools was $\alpha = 0.78$.
3) To measure the attitudes toward online privacy and the influence of optimistic bias, the following variables were defined (Part B, items 1-4):
   1. The level of privacy and anonymity threat awareness was measured via three different indicators: 1) The awareness of the social threat as the sense of exposure to other users; 2) The general awareness of privacy threats as users' sense of anonymity while visiting a website; 3) The awareness of the

technological threats as users' knowledge of concrete parameters that are prone to online surveillance. 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.

2. Users' OPSE level was measured through one indicator that examined the belief in one's ability to browse anonymously. The responses were coded on a 1-7 Likert scale (7 = high level of belief, 1 = no belief at all), and then were averaged.
3. The level of privacy concern was measured via two sets of indicators. Indicators of the privacy concern on the general websites were: 1) The level of concern for the protection of personal information on the Web (part B, item 5) - 1-5 Likert scale (5 = very highly concerned, 1 = not concerned at all); and 2) The importance of protecting personal information on the Web (part B, item 6) - 1-5 Likert scale (5 = very highly important, 1 = not important at all). The following two indicators of the privacy concern on social networks were used: 1) The level of concern for the protection of personal information on social networks (part B, item 7) - 1-5 Likert scale (5 = very highly concerned, 1 = not concerned at all); and 2) The importance of protecting personal information on social networks (part B, item 8) - 1-5 Likert scale (5 = very highly important, 1 = not important at all). Then, two separate indices, averaging each of these two sets of indicators respectively, were calculated.

The dependent research variables were the two types of users' online privacy behavior, defined based on (Chellappa & Sin, 2005) and information security surveys (Aydin & Chouseinoglou, 2013; Talib, Clarke & Furnell, 2010). Each item in this group comprised a certain privacy behavior. Based on the gratification hypothesis (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 privacy protection which matches the privacy threats' awareness or information disclosure despite the awareness of the privacy threats, i.e. the privacy paradox behavior. This group of items constitutes a direct scale of 25 items for assessing the privacy paradox and privacy protection behavior. The users' tendency toward privacy paradox behavior was measured by this scale (part D, items 1-25). To create a single variable, the values of items 1-4, 6, 8, 13, 15, 22, 25 that reflected the opposite tendency were reversed. The values were coded on a 1-5 Likert scale (5 = a strong tendency toward privacy paradox behavior, 1 = a weak tendency toward privacy the paradox behavior) and then averaged. The internal consistency reliability of the scale (Cronbach's alpha coefficient) was 0.84.

The users' tendency toward privacy protection behavior was measured by a sub-group of items from the privacy paradox scale above that reflect the opposite of privacy paradox tendency (Part D, items 1-4, 6, 8, 13, 15, 22, 25). The items were coded on a 1-5 Likert scale and then averaged. The internal consistency reliability of the scale was 0.70.

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 to privacy paradox and privacy protection behavior, we performed a multiple linear regression analysis using the above factors as independent variables.

4 Results

In this section we present 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. We found that almost half of the students (49.7%) reported that they are highly concerned or very highly concerned with privacy

threats posed on their personal information on the Web (M = 3.70, SD = 0.79) and even more students (57%) reported the same in the setting of social networks (M = 3.68, SD = 1.02). Furthermore, we measured the levels of OPL and OPSE among the general sample and distributed by field of study. We found that both the OPL and OPSE levels of the sample were medium, M=2.53 (in the range of 1-5) and M=3.5 (in the range of 1-7), respectively. When analyzing these factors by field of study, we found significant differences in OPL levels (by conducting an F-Test – F=3.67, p=0.025), as Information Science students reported the highest levels of OPL (M=2.76), compared to Computer Science and Engineering students (M=2.48) and Accounting and Business Management students (M=2.29). However, no significant differences were found for OPSE levels among field of study. In addition, the average students' tendency toward privacy paradox behavior was not high, M=2.71 (SD=0.43) in the range of 1-5. Similar results were found for students' tendency toward privacy protection behavior (M=2.64, SD=0.69).

Subsequently, we examined the role of the aforementioned factors in predicting the dependent variable, namely the users' tendency toward privacy paradox behavior. A multivariate linear regression analysis was therefore performed, using the various independent variables described in the Methods section. Table 3 presents the regression coefficients for predicting users' tendency toward privacy paradox behavior.

Table 3. The linear regression coefficient for predicting users' tendency toward privacy paradox behavior

Predictors	**Dependent variable: tendency to privacy paradox behavior**			
	β	**SE**	**B**	**T**
Sense of anonymity while visiting a website	0.16	0.04	0.07	**1.66**
Awareness of social threat	-0.04	0.05	-0.02	**-0.47**
OPSE level	-0.20	0.02	-0.05	***-2.16**
Awareness of technological threat	0.17	0.02	0.03	**1.80**
OPL level	0.002	0.05	0.001	**0.02**
Gender	-0.08	0.07	-0.06	**-0.87**
Field of study - Accounting and Business Management vs. Information Science and Computer Science and Engineering	-0.25	0.09	-0.25	****-2.93**
Field of study - Information science vs. Accounting and Business management and Computer Science and Engineering	-0.15	0.08	-0.13	****-1.66**
Online literacy - high vs. moderate and low	0.07	0.09	0.68	**0.77**
Online literacy - low vs. high and moderate	0.03	0.08	0.03	**0.36**
Privacy concern on the Web	-0.40	0.05	-0.21	****-3.97**
Privacy concern on social networks	-0.01	0.04	-0.01	**-0.15**

*** p<0.05, **p<0.01**

Table 3 shows that the regression for predicting the users' tendency toward privacy paradox behavior was significant, $F(13,147)=3.10$, $p<0.001$, with the predictor variables accounting for 22% of the explained variance ($R2=0.22$).

As the students' levels of OPSE and privacy concern on the Web increase, their tendency toward privacy paradox behavior decreases. Namely, the higher the students' level of privacy concern and self-efficacy in privacy protection, the lower the tendency toward privacy paradox behavior. In addition, we found significant differences between the fields of study with regard to students' tendency to privacy paradox behavior. Interestingly, Information Science students reported a significantly lower tendency toward privacy paradox behavior than other students, and Accounting and Business Management students had the highest tendency toward privacy paradox behavior.

Then, we examined the role of the aforementioned factors (presented in Table 3) in predicting users' online privacy protection behavior. A multivariate linear regression analysis was, therefore, performed

using the various independent variables described above. Table 4 presents the regression coefficients for predicting users' tendency toward online privacy protection.

Table 4. The linear regression coefficient for predicting users' preference of privacy and anonymity protection.

Predictors	**Dependent variable: preference of privacy and anonymity protection**			
	β	**SE**	**B**	**T**
Sense of anonymity while visiting a website	-0.15	0.07	-0.11	**-1.61**
Awareness of social threat	0.02	0.07	0.02	**0.29**
OPSE level	0.19	0.03	0.07	***2.15**
Awareness of technological threat	-0.22	0.03	-0.06	***-2.32**
OPL level	0.04	0.07	0.03	**0.40**
Gender	-0.06	0.11	-0.08	**-0.77**
Field of study - Accounting and Business Management vs. Information Science and Computer Science and Engineering	0.28	0.13	0.43	****3.40**
Field of study - Information Science vs. Accounting and Business Management and Computer Science and Engineering	0.32	0.12	0.43	****3.73**
Online literacy - high vs. moderate and low	-0.07	0.13	-0.10	**-0.77**
Online literacy - low vs. high and moderate	-0.11	0.11	-0.15	**-1.32**
Privacy concern on the Web	0.40	0.08	0.32	****4.17**
Privacy concern on social networks	-0.01	0.06	-0.01	**-1.13**

*** p<0.05, **p<0.01**

Table 4 shows that the regression for predicting users' preference of privacy and anonymity protection was significant, $F(13,147)=4.05$, $p<0.001$, with the predictor variables accounting for 26% of the variance ($R2=0.26$).

The higher the privacy concern on the Web and the OPSE level, the higher the students' preference of privacy protection on the Web. Furthermore, the higher the students' awareness of the technological threat, the lower their preference of privacy protection on the Web. In addition, there were differences between the fields of study with regard to the students' privacy protection behavior. In accordance with the findings presented in Table 3, Information Science students tended the most toward privacy protection behavior.

5 Discussion and Conclusions

Following the suggestion of Kokolakis (2017) that the online privacy paradox should not be considered as a dichotomy between privacy concerns and behavior, the main conceptual contribution of this study was a new direct scale for assessing online privacy paradox and privacy protection behavior. The proposed scale measures online privacy paradox behavior as a single variable and thus bridges the gap in the literature (Kokolakis 2017) that this complex phenomenon has not been explored directly yet. Putting this new scale into practice, we found that users with a higher level of concern for online privacy and higher privacy self-efficacy chose privacy protection behavior over usability and reported lower privacy paradox behavior. These results were in accordance with some of the above studies (Akhter 2014; Awad & Krishnan 2006; Castañeda & Montoro 2007; Heirman, Walrave & Ponnet 2013; Hoffman et al. 1999; Lee & Letho 2010; Phelps, Nowak & Ferrell 2000; Phelps, D'Souza & Nowak 2001; Potoglou, Palacios & Feijóo 2015; Taylor, Davis & Jillapalli 2009).

Another contribution of this study was the investigation of the predictive factors of the privacy paradox vs. privacy protection behavior. Several prominent theories were suggested as possible explanations for these phenomena, but most of them were not empirically tested in previous work. In this study we tested these theories' capabilities to explain users' online privacy behavior. In this respect, no significant evidence for the gratification hypothesis (Trepte et al. 2015) was revealed, as our results show that risks slightly outweigh the benefits of online self-disclosure. In addition, as opposed to some previous studies (Hoy & Milne 2010; Milne, Rohm & Bahl 2004; Sheehan 1999; Tufekci 2008; Yao & Linz 2008), no significant differences were found between men and women with regard to the users' tendency toward privacy paradox behavior. One possible explanation for the differences between our results and previous works is that previous studies dealt with privacy concern and behavior on social networks that strongly encourage information disclosure, while our findings are related to general-purpose websites as well. Furthermore, the differences may stem from the fact that these studies are relatively old, while our results might slightly point to a contraction of a widely discussed digital divide that was claimed to exist between the genders (Bimber 2000; Ono & Zavodny 2003). Another explanation might be the fact that we used a single variable based on a new direct scale to measure the privacy paradox behavior, while past research was based on the indirect evaluation of the relationship between the user's attitudes and their self-disclosure behavior as two separate variables.

Interestingly, we detected evidence supporting optimistic bias theory (Baek, Kim & Bae 2014; Cho 2012; Cho, Lee & Chung 2010), as a higher awareness of the monitored details while visiting a website quite surprisingly causes a decrease in privacy protection behavior. Our results partially support the knowledge gap hypothesis as a factor affecting users' tendency toward privacy paradox behavior. Thus, students from the Computer and Information Science departments, who apparently acquire a deeper understanding of the concept of online privacy, had a lower tendency to privacy paradox behavior. However, quite surprisingly, the OPL level did not play a significant role in students' online privacy behavior. However, Information Science students reported the highest OPL and their tendency toward privacy paradox behavior was the lowest. These two findings might show an indirect relation of increasing OPL to decreasing the tendency toward privacy paradox behavior. Computer Science students, whose technical skills for privacy protection were the highest, did not report a higher level of privacy protection behavior compared to Information Science students. In addition, we found no support for Barnes' (2006) and Debatin et al.'s (2009) hypothesis that the privacy paradox is a result of a lack of awareness of the risks posed by information disclosure, as no significant relation was found between students' privacy and anonymity threat awareness and their tendency toward privacy paradox behavior.

These findings lead us to the conclusion that there is no need for high technical knowledge and skills to adopt privacy protection behavior over privacy paradox behavior. The social implication of this study is that by increasing the concern and self-efficacy for the protection of personal information on the Web, it is possible to decrease the online privacy paradox behavior. In this respect, our results show the advantage of the course of study taught in Information Science departments.

Since our results were based on students' self-reports on their concerns and beliefs which might be biased, future work should apply qualitative analysis to explore additional types of and factors affecting online privacy behavior. Also, our results are limited by the relatively small study population and reflect Israeli students' behavior patterns. Most students today are digitally-oriented and proficient, at least to some extent, in using Web applications, which might influenced our results. In addition, due to the relatively low levels of the explained variance of both regressions, we assume there are other factors for predicting these behaviors that were not examined in this paper and are subject for further research. Therefore, further investigation aiming to generalize the study findings should apply the proposed methodology on additional population types comprising subjects with various education levels, occupation types, age groups, cultures and countries of origin. Future research might also examine additional factors of influence on users' online behavior, such as awareness of policies, website characteristics, authority and trust.

References

Acquisti, A., Brandimarte, L., Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347* (6221), 509-514.

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In the proceedings of: *the 6th International Workshop on Privacy Enhancing Technologies,* Cambridge, England.

Acquisti, A., Grossklags, J. (2004). Privacy attitudes and privacy behavior: Losses, gains and hyperbolic discounting. In: J. Camp & R. Lewis (Eds.), *Economics of information security* (pp. 165-178). New York, NY: Springer.

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.

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.

Aydin, O. M., & Chouseinoglou, O. (2013). Fuzzy assessment of health information system users' security awareness. *Journal of Medical Systems, 37* (6).

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.

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). Retrieved from http://firstmonday.org/article/view/1394/1312.

Beuker, S. (2016). *Privacy paradox: Factors influencing disclosure of personal information among German and Dutch SNS users.* Master's Thesis, University of Twente, Netherlands.

Bimber, B. (2000). Measuring the gender gap on the Internet. *Social Science Quarterly, 81* (3), 868-876. Retrieved from http://www.dleg.state.mi.us/mpsc/electric/workgroups/lowincome/internet_gender_ga p.pdf

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 Reference.

Castañeda, J. A., & Montoro, F. J. (2007). The effect of Internet general privacy concern on customer behavior. *Electronic Commerce Research, 7* (2), 117-141.

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.

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.

Cho, H. (2012). Responses to online privacy risks. In: Y. Zheng (Ed.), *Encyclopedia of cyber behavior* (pp. 900-910). Hershey, PA: IGI Global.

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.

Costante, E., den Hartog, J., & Petkovic, M. (2012). On-line trust perception: What really matters. In the 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.

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

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.

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.

Eastin, M. S., Brinson, N. H., Doorey, A, & Wilcox, G. (2016). Living in a big data world: Predicting mobile commerce activity through privacy concerns. *Computers in Human Behavior, 58*, 214-220.

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 Notes in Computer Science (pp. 1-18). Berlin, Heidelberg: Springer-Verlag.

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.

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In S. Trepte, & L. Reinecke (Eds.), *Privacy online. Perspectives on privacy and self-disclosure in the social web* (pp. 19-32). Berlin: Springer.

Feng, Y. & Xie, W. (2014). Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy- protecting behaviors. *Computers in Human Behavior, 33*, 153-162.

Fogel, J., & Nehmad, E. (2009).Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25* (1), 153-160.

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).

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In the proceedings of: *the 2005 ACM Workshop on Privacy in the Electronic Society (WPES '05)*, Alexandria, VA.

Guo, X. T., Zhang, X. F., & Sun, Y. Q. (2016). The privacy-personalization in mHealth services acceptance of different age groups. Electronic *Commerce Research and Applications, 16*, 55-65.

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.

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.

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.

Ibrahim, Y. (2008). The new risk communities: Social networking sites and risk. *International Journal of Media & Cultural Politics, 4* (2), 245-253.

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.

Joinson, A. N., Reips, U. D., & Buchanan, T. (2010). Privacy, trust, and self-disclosure online. *Human-Computer Interaction, 25* (1), 1-24.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122-134.

Kolek, E. A., & Saunders, D. (2008). Online disclosure: An empirical examination of undergraduate Facebook profiles. *Journal of Student Affairs Research and Practice, 45* (1), 1-25.

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.

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.

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. In proceedings of: *the 9th Symposium on Usable Privacy and Security (SOUPS '13),* Newcastle: UK.

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.

Livingston, S. (2008). Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society, 10* (3), 393-411.

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.

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

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.

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.

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.

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.

Ono, H. & Zavodny, M. (2003).Gender and the Internet. *Social Science Quarterly, 84* (1), 111-121.

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.

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40* (2), 215-236.

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.

Phelps, J. E., 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.

Pfitzmann, A., & Köhntopp, M. (2001). Anonymity, unobservability, and pseudonymity - a proposal for terminology. In the proceedings of*: the International Workshop on Design Issues in Anonymity and Unobservability,* H. Federrath (Ed.), pp. 1-9. Berlin, Heidelberg: Springer-Verlag.

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.

Qian, H., & Scott, C. R. (2007). Anonymity and self-disclosure on weblogs. *Journal of Computer-Mediated Communication*, 12 (4), 1428-1451.

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_AnonymityOnlin e_090513.pdf

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.

Sheehan, K. B. & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing, 19* (1), 62-73.

Stutzman, F. & Kramer-Duffield, J. (2010). Friends only: Examining a privacy-enhancing behavior in Facebook. In the proceedings of: *the 28th Annual CHI Conference on Human Factors in Computing Systems (CHI '10),* Atlanta, GA.

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.

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.

Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An analysis of information security awareness within home and work environments. In the proceedings of: *the 5th International Conference on Availability, Reliability, and Security*, Krakow, Poland.

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.

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.

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.

Weinstein, N. D. (1989). Optimistic biases about personal risks. *Science, 246* (4935), 1232-1233.

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

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.

Xu, F., Michael, K., & Chen, X. (2013). Factors affecting privacy disclosure on social network sites: An integrated model. *Electronic Commerce Research, 13* (2), 151-168.

Yao, M. Z., & Linz, D. G. (2008). Predicting self-protections of online privacy. *Cyberpsychology & Behavior, 11* (5), 615-617.

Yoon, S. (2002). The antecedents and consequences of trust in online-purchase decisions. *Journal of Interactive Marketing, 16* (2), 47-62.

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? In the proceeding of: *the 5th annual ACM Web science conference*, Paris, France.

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.

Appendix A

Questionnaire

Part A – Demographic Details

1. Gender: M / F

2. Year of Birth

3. Education:
   a. Bachelor's Degree (B. A.)
   b. Master's Degree (M. A.)
   c. Doctor of Philosophy (PhD)
   d. Other

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. How concerned are you about the protection of your personal information on the Web? (Please circle)
   a. Not concerned at all.
   b. Slightly concerned.
   c. Moderately concerned.
   d. Highly concerned.
   e. Very highly concerned.

5. How important is it for you to protect your personal information when surfing a website? (Please circle)
   a. Not important at all.
   b. Slightly important.
   c. Moderately important.
   d. Highly important.
   e. Very highly important.

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

7. How important it is for you to protect your personal information on social networks? (Please circle)
   a. Not important at all.
   b. Slightly important.
   c. Moderately important.
   d. Highly important.
   e. Very highly important.

8. 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)

1-16. 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 – Privacy paradox and privacy protection behavior 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 use complicated passwords, even though it takes me more time, in order to reduce the risk posed on my personal information on the Internet.
2. 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.
3. I often change the passwords for my online accounts, even though it may be tedious.
4. I am willing to pay for services that will guarantee the protection of my personal information.
5. Online privacy-enhancing services flaw my surfing experience.
6. I tend to read the "privacy policy" statement of a website asking me to submit personal details.
7. I tend to download software and content that I find to be important, even from unfamiliar websites despite the threat on my personal information.
8. I do not tend to conduct online shopping, because I am concerned with my personal information security.
9. 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.
10. 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.
11. When I am required to set a new password, I tend to use a simple one that is easy to remember even at the expense of a threat on my privacy.
12. I use online banking services (not only for checking my account's status) despite the threat on my

personal information.

13. I do not tend to use the same password for different online accounts even though it requires some additional effort.
14. I tend to install different extensions on my Web browser, even when it requires me to submit personal details.
15. I seldom change the access passwords for my online accounts even though this might pose a threat on my privacy.
16. 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.
17. 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.
18. In general, I prefer to comfortably use the Internet, even at the expense of protecting my personal information.
19. I do not tend to read the "privacy policy" statement of a website I am visiting, even though this might be important for protecting my personal information.
20. I often tend to conduct online shopping, even though I know it might jeopardize my information security.
21. I tend to download software and services aim to improve the performance of my computer / Web browser, even from seemingly unprotected websites.
22. I will not submit personal information on an unsecured website to protect my privacy, even if it offers me a service I desire.
23. I tend to open "pop-ups" only when they are dealing with a matter of special personal interest, to protect my privacy.
24. 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.
25. In general, I prefer to protect my information security, even at the expense of my comfortable use of the Internet.