Impact of Privacy Awareness on Attitudes and Behaviors Online

Delfina Malandrino
Dipartimento di Informatica
Università di Salerno
I-84084, Fisciano (SA), ITALY
Email: delmal@dia.unisa.it

Vittorio Scarano
Dipartimento di Informatica
Università di Salerno
I-84084, Fisciano (SA), ITALY
Email: vitsca@dia.unisa.it

Raffaele Spinelli
Dipartimento di Informatica
Università di Salerno
I-84084, Fisciano (SA), ITALY
Email: spinelli@dia.unisa.it

ABSTRACT

People on the Web are generating and disclosing an ever-increasing amounts of data, often without full awareness of who is recording what about them, and who is aggregating and linking pieces of data with context information, for a variety of purposes. *Awareness* can help users to be informed about what silently happens during their navigation while *learning* from disclosure of personal information may help to discriminate potential harmful activities from daily and regular activities that can be performed online. Our main objective is to study whether a highly customized tool can help users to learn the value of privacy from their behaviors and make informed decisions to reduce their degree of exposure. To this aim, we present an evaluation study to analyze general perceptions, attitudes, and beliefs about privacy online, and to explore the *resultant behaviors* for two different groups of participants from an academic environment.

I INTRODUCTION

People everywhere are generating an ever-increasing amounts of data, often without being fully aware of who is tracking their actions, gathering their information, and aggregating them in order to provide free services and targeted advertising [1]. Although the behavioral advertising practice increases the effectiveness of the marketer's campaigns[1], it also has given rise to privacy concerns since private information may be collected and centralized by a limited number of companies [3]. Targeted advertising heavily relies on the use of valuable information that could lead to an accurate reconstruction of users' interests profile. Private information may be leaked to third party entities [4], that often intervene as uninvited guests during Web searches, online shopping, online business and financial transactions, social activities or during any type of communications on the Web. However, the risk is about the final use of these pseudo-anonymous data, that linked with personally identifiable information (i.e., phone number, credit card number, social security number and so on), may be disclosed or explicitly sold to third party entities. These data could be potentially used for secondary activities, such as identity theft, social engineering attacks, online and physical stalking and so on [5–8].

Recent statistics show that 63% of users agreed with a statement of concern for third party monitoring activities [9]. In another study Krishnamurthy *et al.* highlighted the criticality of the problem showing that 56% of sites analyzed (75% when considering userids) directly leak sensitive and identifiable information to third party aggregators [10]. The disclosure of personal information to third party sites, without users' permissions or consents, represents the greatest concern among Internet users, that call for more effective solutions to protect themselves against invasions into their private affairs.

Various meanings and dimensions of privacy have been discussed in literature [11, 12], even without a meaningful and accepted definition for it. More specifically, privacy has been defined as synonymous of the "*right to be let alone*" [13], or as synonymous of the *right to prevent the disclosure of personal information* [14]. Privacy has been also defined as the ability of the individual to control the terms under which his/her personal information is acquired and used [15]. The contextual nature is evident in several other definitions: "*Individuals have privacy to the extent that others have limited access to information about them, to the intimacies of their lives, to their thoughts or their bodies*" [16]. Individuals are different in their thoughts and beliefs with behaviors that change according to environmental and personal factors or user's orientation [17]. Finally, individuals are continuously searching for a balance between the desire for privacy and the desire for personal communication with others [18].

In this work we want to analyze if by making people aware of the information they reveal about themselves, they would take steps to prevent it. To this aim, we carried out a descriptive quantitative study to analyze whether a privacy-enhancing technology

[1]Behavioral advertising is more than twice as effective as non-targeted ads [2]

tool that we developed, named NoTrace [19–21], is able to make *tangible*, or perceptible, what sometimes is underestimated by unwary users, enabling individuals to make informed decisions when invasions to their privacy occur.

In our study, two subgroups of students, namely *ICT Group* (i.e., technology-oriented) and *non-ICT Group*, were surveyed to:

1. Assess generally and also to compare each group's understanding of privacy concerns about online activities.
2. Study whether technological knowledge may influence attitudes toward privacy, privacy-related behavioral intentions and actual behaviors.
3. Study whether awareness and learning from own behavior may increase the willingness of people to limit the diffusion of personal information and protect their privacy while they are navigating the Web.

Overall, we want to evaluate whether the *non-ICT* Group would have more concerns about privacy when compared with the *ICT* Group and if technological knowledge can influence the perception of the risks about privacy, as well as the corresponding privacy behaviors. We want also to evaluate whether awareness about information leakage and learning from online personal habits and behaviors may affect in the same way both groups.

The paper is organized as follows. Section II discusses some related works in the same field. In Section III we describe the main functionalities of NoTrace, that is the privacy-enhancing tool we used in our evaluation study. In Section IV we studied whether NoTrace was able to help people to value their privacy, by making tangible what sometimes is underestimated by unwary users, and we discussed some interesting findings in Section V. We will conclude with some final remarks in Section VI.

II RELATED WORK

Concerns about privacy are mainly focused on activities and interactions online, rather than on the typical interactions that may happen during everyday life. Over the past decade, several empirical studies have been conducted to analyze the level of concerns about privacy across US population. These surveys covered general privacy, consumer privacy, medical and health privacy, and other privacy-related areas. Specifically, several studies addressed the analysis of the privacy in e-commerce environments [22], the privacy of health information on social media [23], the privacy that may affect individual's purchasing decisions [24], or the privacy that may be violated by the behavioral advertising [25]. Other works aimed at analyzing users' behaviors and attitudes toward privacy, with emphasis on gender and technical differences [26–29], and on the propensity to disclose personal information [30, 31]. Recent works studied privacy concerns related to cloud storage [32], location sharing [33], and the use of Google+ circles as a means to control the information flow [34].

Other recent studies in the social area show concerns among Facebook users, their strong negative association between privacy concerns and engagement (posting, commenting and Like-ing of content) [35], their willingness to change privacy settings [36], even if, in a subsequent study [37] it was discovered that, due to the constant modifications and alterations to the policy, many users (i.e., 65.7%) are unaware of how their profiles are affected, and therefore, unaware of their personal privacy settings. Finally, Liu *et al.* showed that users are having trouble about correctly configuring their privacy settings and call for new tools to protect privacy [38].

Overall, several studies reported that an overwhelming majority of people are very concerned about a wide range of privacy issues [39–41] and that privacy concerns influence people's willingness to disclose personal information to a Web site [42]. However, studies analyzing the relationships between Internet users' concerns and the actions to take to address them, discovered an apparent dichotomy between privacy attitudes and resultant behaviors [43–45]. This dichotomy involves situations in which users are less willing to take actions to protect privacy (and, therefore, more likely to share their personal information and preferences) when some benefits can be obtained in return [46]. In fact, studies in this field show that only a small percentage of users read privacy policies, mainly because users find learning about privacy and reading privacy policies is difficult and time consuming. In general, most of the users are not able to reliable understand their content [47], and therefore, they are reluctant when adopting privacy protective techniques and technologies [43, 48, 49].

Most of the reported studies explored differences in individuals in respect to their privacy concerns. Our

goal in this work was to investigate concerns about the privacy of two groups of students from different academic areas and with different technological knowledge. We explored whether educating them about potential risks on the Web, through a direct learning from one's behavior during online activities, may involve increasing awareness about privacy as well as increasing willingness to reduce their degree of exposure to privacy attacks. Finally, we have to emphasize that this work extends the analysis presented in [50].

III NOTRACE

NoTrace [19–21] is a privacy-enhancing tool, implemented as a Mozilla Firefox add-on, whose main goal is to provide several instruments to protect privacy of users during Web navigation and to limit the diffusion of sensitive and personally identifiable information.

The approach implemented by NoTrace ensures:

• **Support for users**, in order to help them to make informed decisions.

• **Comprehensiveness**, in terms of privacy threats addressed and the corresponding countermeasures provided.

• **Awareness and full control** over privacy leakage and countermeasures to adopt to limit its diffusion.

• **Performance and effectiveness** in order to make the tool longer used by users, since excessive delays involve an abandonment by users after first use [51].

NoTrace supports users' needs through several privacy settings that can be fine-tuned according, for example, to experience and expertise (See Fig. 1). Specifically, NoTrace offers a "Standard Protection" for Novice students (with three different levels of protections that can be selected) and a "Customized Protection" for Experienced users. The latter modality allows users to choose any of the provided countermeasures for the selected category of privacy threats they want to address that is, "Personal Information", "Web Tracking" or "Third Party Activities and Ads" (shown in Fig. 1). Conversely to Novice, Experienced users can also fine-tune the privacy settings, enabling and disabling specific functionalities whenever they want.

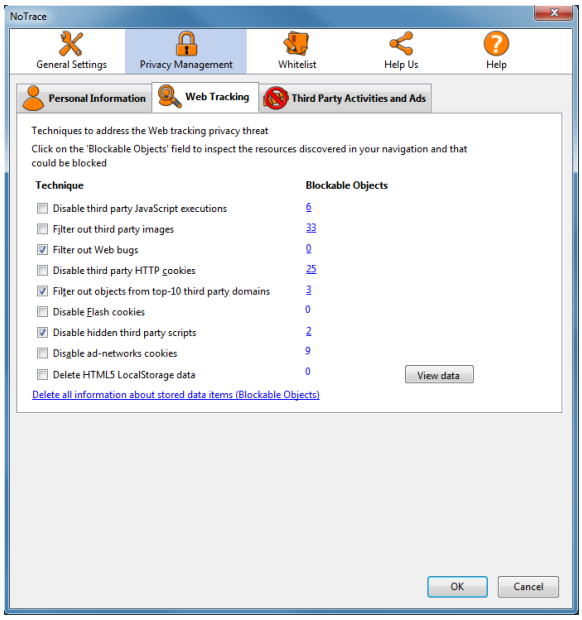

Fig. 1. NoTrace configuration: how protection measures can be enabled. The "Blockable Objects" link allows users to inspect which objects can be blocked when selecting, with a simple check, the corresponding technique.

Conversely to other popular tools in this field (i.e., AdBlock Plus [52], Ghostery [53], Abine [54]), that only provide an URL-based blocking mechanism, NoTrace provides new filtering mechanisms that are able to access the stream of bytes received by the browser immediately before the rendering of the Web page. In this way, it is able to address privacy threats unprecedentedly not dealt with, as well as, avoid a large variety of loopholes and tricks that could be used to overcome the filtering.

To educate users on what information about their browsing behavior is sent to third-party entities and the information that is inferred based upon their behavior, we designed NoTrace so that it can steadily monitor the Web navigation, allowing users to be constantly informed about both potential harmful activities on the Web and the extent of their personal information leakage.

Specifically, the NoTrace's "Blocked Object Panel" allows users to inspect all blocked URLs, while to enhance awareness we show, in a specific panel, the personally identifiable information disclosed to third party sites, for each visited Web site (See Fig. 2).

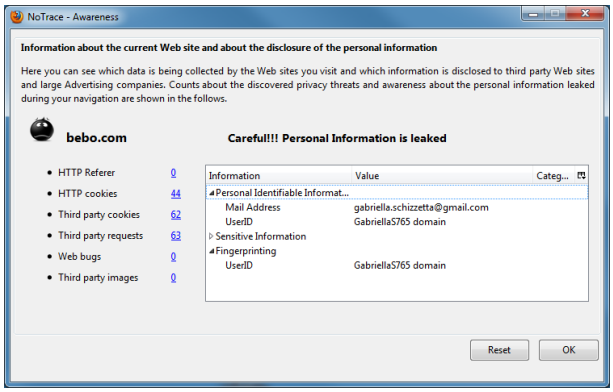

Fig. 2. NoTrace awareness: Information leaked towards the bebo.com Web site.

IV EVALUATION STUDY

In this Section we describe results about the comparison among two samples of students that we recruited from an university environment. As mentioned before, the main goal of this study is to find out if a highly customized privacy-enhancing tool can contribute to make users aware of their privacy leakage and increase their responsibility when managing their privacy online. Specifically, in this study, we tried to respond to the following questions:

1. Are there significant differences among two groups of students with regards to beliefs, attitudes and concerns about privacy? (Online privacy concerns, Section V(1) for the results).
2. Experience in online activities and general technological knowledge can influence how different users "value" their privacy? (How skills influence behaviors, Section V(2) for the results).
3. Learning about privacy through the help of a privacy-enhancing tool can involve more informed decisions about the countermeasures to adopt? Learning can affect in the same way different types of groups? (How privacy awareness can change behaviors, Section V(3) for the results).

1 METHODOLOGY

For our study we recruited 36 participants among students of the Computer Science, Cultural Heritage, Business and Law Departments at the University of Salerno. We classified students into two groups, named *non-ICT* Group (18 students from the Cultural Heritage, Business and Law Departments) and *ICT* Group (18 students from the Computer Science department) according to their field study. It must be emphasized that these two groups are statistically different as we will show afterwards in this Section and also in Section V.

Students were recruited through email announcements to mailing lists, and word of mouth advertising. The participation in the study was voluntary and anonymous, and students were not compensated for taking part in the interviews. Participants were informed that all the information they provided would remain confidential. Finally, to avoid a biased sample, when recruited participants, we did not mention privacy or security, privacy risks and benefits, and we only said that we were looking for people interested in participating in an evaluation study.

The average age of the sample was 24, and the gender split was almost even (i.e., 53% female and 47% male). The majority of participants spent between two and six hours on Internet per day (72% of the *non-ICT* users and 50% of *ICT* users), while only 11% of *non-ICT* users and half of *ICT* users spent on Internet more than six hours. 83% of users in the *non-ICT* Group considers themselves incompetent with online activities, while 72% of *ICT* participants consider themselves as competent/expert (χ=9.488, p-value=0.0065, see also Table I). Statistical differences across groups are shown in Table I.

Table I. Participant Demographics.

Variables		***non-ICT* Group**	***ICT* Group**	***Chi-Square* Sig. Level**
Gender	Male	28%	67%	0.0194
	Female	72%	33%	
Age	20-23 years	33%	44%	N.S.
	24-26 years	61%	50%	
	27-32 years	6%	6%	
Education	Bachelors	50%	11%	0.0113
	Masters	50%	89%	
Time spent online per day	0-2 hours	17%	0%	0.0351
	2-6 hours	72%	50%	
	6+	11%	50%	
Internet Expertise	Inexpert	83%	28%	0.0065
	Competent	17%	33%	
	Expert	0%	39%	

2 PROCEDURE

The study was conducted at the ISISLab research laboratory, at the University of Salerno. It envisioned three different phases in which we carried out: a *preliminary survey*, the *tool testing*, and finally, a *sum-*

mary survey, respectively.

In the first phase we asked participants to fill in a preliminary questionnaire, composed of 32 questions in five categories. In this questionnaire we collected: *(a)* demographic information (i.e., gender, age, education level), *(b)* information about Internet usage, *(c)* general knowledge about privacy threats on the Web, *(d)* general attitudes toward privacy, *(e)* information about awareness and general behaviors about privacy online.

Specifically, the first section asked for standard demographic information, and for technical skills (such as, time spent on Internet, level of expertise with online activities). The second part asked for general information about the preferred browser (i.e., Mozilla Firefox, Google Chrome, and so on) and knowledge and/or usage of browsers' add-ons or extensions. The third part tested participants' knowledge about some potential privacy threats on the Web (rating on a 5-point Likert scale with *strongly agree/strongly disagree* as verbal anchors). The fourth section tested participants' concerns about privacy and general attitudes toward online privacy (rating on a 5-point Likert scale). The last section gauged general participants' behaviors about privacy online.

In the tool testing phase, we asked users to use NoTrace, our evaluation tool, for a 30-minutes browsing session. We asked them to choose any of the provided modalities of privacy protection or select any of the provided advanced functionalities. We gave them details about NoTrace goals and main features. We also provided them with basic information on how to use it. Users were not directly monitored, so that they could feel free to test and explore the tool, but they could call for assistance if they did not understand any of the instructions posed. The test was performed in an isolated environment within our research lab in order to avoid distractions due to the presence of other people. Users were also encouraged to provide informal feedback such as general comments, suggestions or observations for developers.

At the end of the testing phase we asked users to spend other 10 minutes to fill in the standard QUIS[2] and CSUQ[3] questionnaires. The aim was to provide additional information about system usability and user satisfaction when using NoTrace and differences experienced by the two tested groups. Specifically, the original QUIS questionnaire, developed at the University of Maryland, was composed of 27 questions. We dropped 10 that did not seem to be appropriate to our tool (e.g., questions about task to execute). Each question was a rating on a 10-point scale with appropriate anchors at each end (e.g., "Overall Reaction to the software: Terrible/Wonderful"), where small values corresponded to unsatisfactory or negative responses and large values corresponded to satisfactory results. The original CSUQ questionnaire was composed of 19 questions. As we did for the QUIS questionnaire, we dropped 7 of them that not seem appropriate for our objectives (e.g., questions about work to complete). Specifically, we asked users to answer to the provided 12 questions indicating their agreement or disagreement through a 7-point Likert scale with *strongly agree* and *strongly disagree* as verbal anchors.

Finally, in the third phase, we asked participants to fill in a summary questionnaire, composed of 12 questions, with a rating on a 5-point Likert scale with *strongly agree/strongly disagree* as verbal anchors. We have to emphasize that this questionnaire also included three questions that were asked in the first phase, in the preliminary survey. We want to measure whether any change has occurred in users' opinions, habits or behaviors after gaining a greater awareness about certain activities performed online by third party entities, and a greater consciousness about the potentialities of the proposed tool.

The entire study lasted between 60 and 70 minutes. We included the preliminary survey, the summary survey and the QUIS and CSUQ questionnaires in the Appendix A.

Finally, for data analysis and statistics results we used IBM Statistical Package for Social Sciences (SPSS, Inc.) software[4].

V RESULTS

Results of the demographic survey have been reported in the previous Section and, specifically, in the description of the study participants. Results are shown in Table I.

When interviewed about familiarities with some privacy threats, groups showed different results. Specifically, we asked users if they had familiarity with some privacy threats, asking them also to provide a

[2] http://oldwww.acm.org/perlman/question.cgi?form=QUIS
[3] http://oldwww.acm.org/perlman/question.cgi?form=CSUQ
[4] http://www-01.ibm.com/software/analytics/spss/

clear definition for terms such as "Web bug", "Flash cookie", "behavioral advertising". We also asked them whether they knew the risks associated with behavioral advertising.

The *non-ICT* Group showed a small familiarity with these privacy threats, with agreement about familiarity with Web bug, Flash cookie and behavioral advertising of 5%, 11% and 33%, respectively. Only 28% of *non-ICT* users is aware of the risks of the behavioral advertising. Conversely, the *ICT* Group reported greater familiarity for all privacy threats. We also found statistical differences among groups, with corresponding results shown in Table II. We found a relation among the familiarity with privacy threats and concern about privacy online (question Q4 shown in Table III). Intuitively, increase of familiarity would decrease general privacy concerns (Pearson correlation between privacy concern and familiarity with Flash cookie, behavioral advertising, and behavioral advertising risks are -0.3883, -0.3434, -0.3607, $p<.05$, respectively).

Table II. Familiarity with some privacy threats.

Variables		***non-ICT*** **Group**	***ICT*** **Group**	**Chi-Square Sig. Level**
Web bug	Disagree	72%	22%	
	Neutral	22%	0%	<0.0001
	Agree	6 %	78%	
Flash Cookie	Disagree	61%	28%	
	Neutral	28%	0%	0.00047
	Agree	11%	72%	
Behavioral	Disagree	33%	0%	
Advertising	Neutral	34%	0%	0.00012
	Agree	33%	100%	
Behavioral	Disagree	33%	39%	
Advertising	Neutral	39%	0%	0.00943
risks	Agree	28%	61%	

1 ONLINE PRIVACY CONCERNS

We look at association with self-reported concerns about privacy in everyday life (Q3), general concerns about privacy on Internet (Q4), as well as 2 questions related to the behavioral advertising (Q10 and Q11). These questions are shown in detail in Table III and also in Appendix A. We reported the questions with the same ID used in the survey questionnaires that we submitted to the participants at the study.

The analysis of concerns about privacy shows that all participants equally consider the privacy very important in everyday life, while less concern is perceived by the *ICT* Group about privacy online (agreement for 50% of participants). We did not observe any statistical difference about privacy concerns across groups. Results are shown in Table III.

Users seem also to be concerned about tracking of their movements on the Web, performed by large business companies to provide them targeted advertising (Q10 and Q11 questions in Table III). Although aware that their browsing history may be collected for advertising purposes, more than half of participants in both groups are uncomfortable even when their personal information cannot be tied to their browsing history. Once again, we did not observe any statistical difference with regards to these concerns across groups.

To further categorize students based on their privacy concern we decided to group participants by applying standard clustering techniques [43]. Specifically, we employed the k-means [55] to investigate the data collected. We selected two questions strictly related to concerns about privacy (i.e., Q3 & Q4) and other two questions related to the behavioral advertising privacy threat (i.e., Q10 & Q11).

In contrast to the results by Westin [56] and Ackerman *et al.* [57] we found out four clusters of participants. Specifically, we identified a group of *Fundamentalists* and a group of *Marginally Concerned*, while the *Pragmatists* group was further decomposed in two distinct groups whose privacy concerns focused either on the awareness of the risks of the behavioral advertising phenomenon or on the linking of users' history information with personally identifiable information. This categorization results are shown for both groups in Table VI.

Specifically, Fundamentalists users provided privacy-oriented responses to all the questions selected for that analysis, by highlighting their concerns to both beliefs about privacy online and the risks of the behavioral advertising. Marginally Concerned users exhibited mild general concerns about privacy and a propensity to enjoy the benefits of the behavioral advertising but only when personal information are not being collected and linked with the browser's history information. As anticipated before, the Pragmatists users were organized in two distinct groups which we called "*Personal Information Concerned*" and "*Behavioral Advertising Concerned*" because of their major concerns about personally information and the risks of the behavioral advertising, respectively.

Table III. Participants privacy concerns. 5-Point Mean Likert scores. Groups are not statistically different according to these metrics.

ID	Question	Mean		Agreement	
		non-ICT	***ICT***	***non-ICT***	***ICT***
Q3	I consider important the privacy in everyday life	4.17	4.17	89%	83%
Q4	I am concerned about my privacy online	3.94	3.56	83%	50%
Q10	When I am online, I am aware that my browsing information may be collected by a third party for advertising purposes	3.28	3.94	67%	78%
Q11	I am comfortable with advertisers using my browsing history to serve me relevant ads, as long as that information cannot be tied to my name or any other personal information	2.72	2.89	39%	44%

Table IV. Participants privacy attitudes. 5-Point Mean Likert scores.

ID	Question	Mean		Agreement		Unpaired T
		non-ICT	***ICT***	***non-ICT***	***ICT***	**Sig. Level**
Q12	I am comfortable with the privacy I have when I use search engines	2.39	2.44	17%	11%	N.S.
Q13	It is my responsibility to protect my personal information on the Web	3.17	2.61	44%	22%	N.S.
Q14	I am aware of the tools that exist online to help me protect my privacy online	3.17	4.33	55%	100%	<0.001

Table V. Participants privacy attitudes.

ID	Question		Agreement		Chi-Square
			non-ICT	***ICT***	**Sig. Level**
Q23	If I have to prioritize between perfect search and perfect privacy I would choose...	Perfect Search	11%	17%	N.S.
		Search ahead of Privacy	28%	17%	
		Privacy ahead of Search	61%	61%	
		Perfect Privacy	0%	5%	
Q24	If you knew for a fact that topics you search for using a search engine were saved forever, would it change your search habits?	No change	17%	11%	N.S.
		Somewhat of a change	78%	77%	
		Significantly change	5%	11%	

Table VI. Privacy concern: typology comparison.

Group	***non-ICT***	***ICT***
	Group	*Group*
Fundamentalists	33%	22%
Pragmatists [Personal Information Concerned]	28%	33%
Pragmatists [Behavioral Advertising Concerned]	22%	34%
Marginally Concerned	17%	11%

When interviewed about the comfortability of the privacy of their search engines, our participants expressed their dissatisfaction (agreement of about 17% for the *non-ICT* Group and only of 11% for the *ICT* Group). Intuitively, this comfortability is related to concerns about privacy, as feelings of comfortability increase one would expect overall privacy concern to decrease (Pearson correlation r=-0.4497, p<.01).

In addition, although 56% of users in the *non-ICT* Group and 78% of *ICT* users stated that they are not personally responsible for protecting their online privacy (i.e., Q13, Table IV), and more than half of all participants are aware of the tools that exist online to protect it (greater awareness for the *ICT* Group, p-value=0.0002), all participants do not consistently take actions to effectively protect it (the whole *non-ICT* Group affirmed its inability to protect its personal information, p-value=0.0004). In general, users say that they care about privacy but they do not do anything about it.

We interviewed users about their preferences between

search quality and search privacy. Most of the users responded for a tradeoff between the two alternatives, with greater results for the *Privacy ahead of Search* option (rate of 61% for both groups).

To further inspect the nature of privacy concerns we analyzed responses from both groups to the following questions: "*What are your main privacy concerns online*?" We manually cluster five meta-categories of concern: (1) "*Tracking my behaviors by third party entities*", (2) "*I am worried about making financial transactions online*", (3) "*Identity theft*", (4) "*Any unauthorized access to my personal information*", (5) "*Internet will never forget my personal data after their dissemination*". Some answers fall in two categories and therefore the sum of columns is above 100%. Results for both groups are shown in Table VII.

Table VII. Nature of privacy concerns across the *ICT* and the *non-ICT* groups.

Meta-categories	***non-ICT* Group**	***ICT* Group**
Tracking my behavior online from third party entities	44%	56%
I am worried about making financial transactions online	11%	–
Identity theft	22%	28%
Any unauthorized access to my personal information	–	17%
Internet will never forget my personal data after their dissemination	–	11%
No answer	28%	33%

2 HOW SKILLS INFLUENCE BEHAVIORS

Some behaviors that could be indicative of a lack of privacy concern and that we studied include: (1) Increasing security settings on browsers (2) Installing tools to protect privacy (3) Deleting cookie saved on browsers (4) Deleting cache and temporary Internet files (5) Reading licence and privacy agreements. Users who are not worried about privacy typically just refrain from taking these precautions.

Our study shows that users in both groups do not change their browser privacy settings or install tools to protect privacy (Q16 and Q18, Table VIII). Only 17% of *non-ICT* and 61% of *ICT* participants regularly delete cookies and, finally, more than 70% of participants in both groups rarely/never read privacy policies (see Fig. 3 and Table VIII).

We also found statistical differences between our groups about the privacy behaviors measured. Specifically, we found significant differences across groups for "Deleting HTTP cookie" (p-value=0.0045) and "Deleting Internet files" (i.e., 0.0229). We found correlation among these two actions and privacy concerns (r=-0.3371, -0.3748, p<.05). We found differences about "Changing browser privacy settings" and about "Installing privacy tools". We did not find any significant result for the "Reading of Web sites' privacy policies" action, confirming earlier findings in this field, as discussed in Section II.

Users of the *non-ICT* Group are less aware of the tracking activities performed by large advertising companies to provide targeted advertising. They do not know the privacy vehicles used to track users and finally, they are less aware of the tools that exist online to protect the privacy. Finally, although aware that their browsing history may be collected for advertising purposes, most of the participants in both groups (61% of *non-ICT* and 56% of *ICT* users) are still uncomfortable, even when their personal data cannot be tied to their browsing history.

As further analysis, we can see in Fig. 4 that users who report to be slightly concerned about privacy online also report less engagement across the analyzed behaviors.

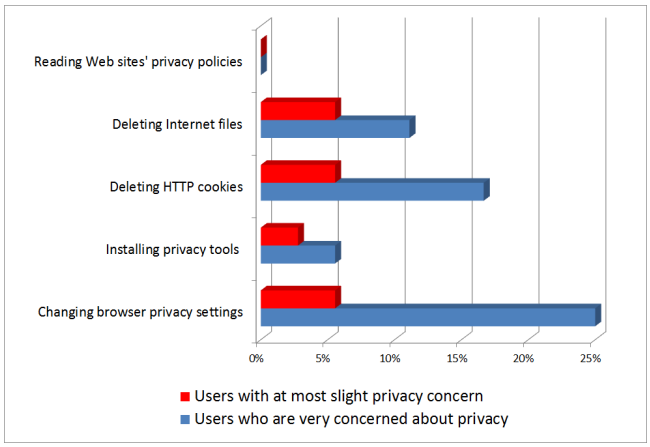

Fig. 4. Percentages of users reporting certain behaviors, grouped by level of privacy concern.

In summary, the first part of the study showed that our respondents are highly concerned about privacy in their everyday life and that *non-ICT* users are more concerned than *ICT* ones about the privacy during online activities. We did not identify statistical differences with regards to these concerns across groups.

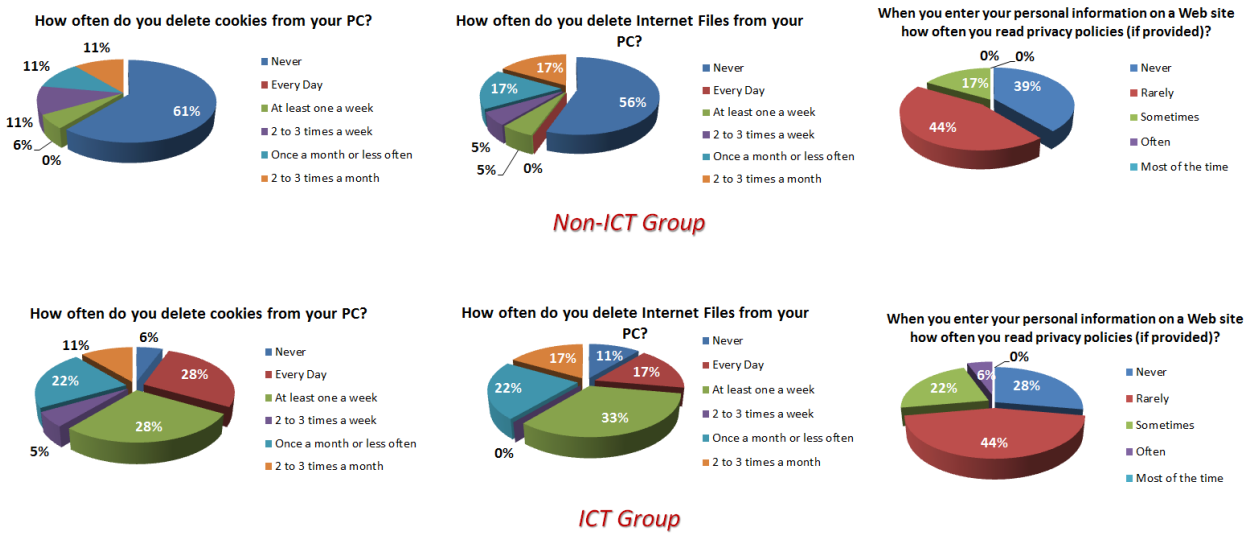

Fig. 3. Privacy behaviors: deleting HTTP cookies, deleting Temporary Internet files (cached resources), reading of Web sites' privacy policies. Results are shown for both groups.

Our study also showed the "lazy" attitude of *non-ICT* users who largely do not take actions to protect their privacy, highlighting a situation in which more support is needed for non-technical students (statistical results are shown in Table VIII).

Table VIII. Participant privacy *actual* behaviors.

ID	Question	Agreement *non-ICT*	Agreement *ICT*	Chi-Square Sig. Level
Q16	Have you ever changed your browser privacy settings?	22%	78%	0.0022
Q18	Have you ever installed a tool to protect your privacy?	0%	28%	0.0159
Q26	Are you able to protect your personal information?	0%	61%	<0.001

3 HOW PRIVACY AWARENESS CAN CHANGE BEHAVIORS

Before discussing the results of the second part of the study we remind the reader that students, in this phase, were asked to use NoTrace during a 30-minutes browsing session. At the end of the testing phase, we first collected information about users' satisfaction and perceptions about the usability of the evaluation tool. Second, we interviewed students in order to understand if NoTrace had some effect on them, in terms of increased awareness and willingness to adopt any type of strategy to improve privacy.

As we can see from Fig. 5, on average, the posed questions were rated positively. Some lower values for the *non-ICT* users are relative to the complexity of the experimented tool and the low intuitiveness of the used terminology. In general, at the question "*Overall, It was easy to use NoTrace*" (Q27), 61% of *non-ICT* users expressed their agreement against 94% of *ICT* ones (p-value=0.0177).

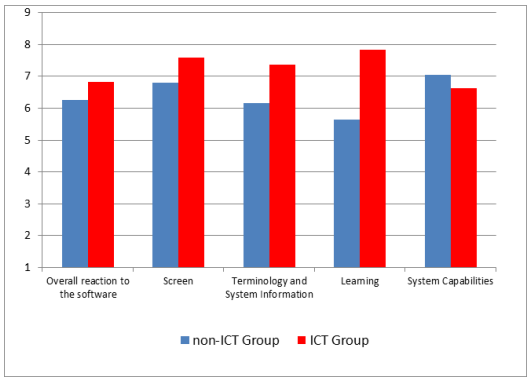

Fig. 5. QUIS results. Comparison between *non-ICT* and *ICT* groups.

Additionally, the *ICT* Group responded with more positive results than the other Group. The same trend is still valid for the analysis of results of the second questionnaire. Specifically, as we can see from Fig. 6, "Satisfaction" and "Clearness" are equally positively rated by both groups, while differences exists about easiness of use and learning and usefulness of the tool. These results confirm that non-

technological users need more support, even to understand the usefulness of any tool to protect privacy.

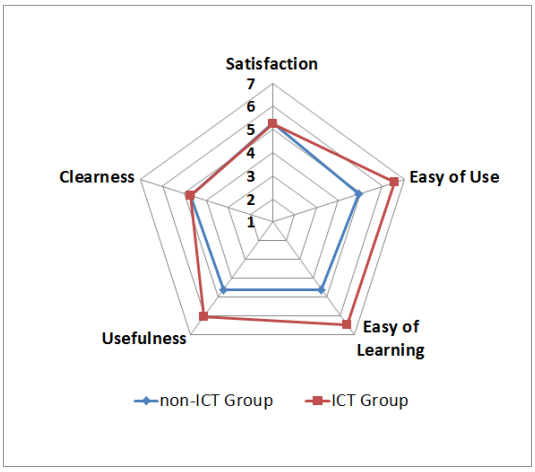

Fig. 6. CSUQ results organized according to five metrics: Satisfaction, Easy of Use and Learning, Usefulness and Clearness.

Finally, the reliability of the QUIS and CSUQ questionnaires was good (Cronbach's $\alpha = 0,91$ and $\alpha = 0,94$, respectively).

Now we are going to analyze results about the investigation of whether a privacy-enhancing tool is able to impact on the users' perceptions, beliefs and concerns about privacy online. The question to respond is if learning about privacy through NoTrace can involve more informed decisions about the countermeasures to adopt, and if this learning affects, in the same way, both the analyzed groups.

We asked users to provide their thoughts about the concerns related to the access to their personal data and, if after using NoTrace, they were willing to take actions to protect their privacy.

Results in Table IX show positive ratings for both groups highlighting how NoTrace was able to increase user awareness about the dangers of certain activities on the Web. However, the higher positive result was for the question: "*I consider important the privacy and I want to make actions and use tools to protect it*" with agreement of 83% for *non-ICT* users and 72% of *ICT* users. Although all users rated positively all three questions shown in Table IX, more willingness to change their behavior online was expressed by *non-ICT* ones, even if we did not find statistically significant differences.

From Fig. 7 we can see that users who report to be slightly concerned about privacy online also report less willingness to take actions to protect themselves against privacy invasions. Another interesting result is about the high percentage of "Neutral" users (neither concerned nor unconcerned about privacy online) who reported higher willingness against the slightly concerned users, to protect their privacy online.

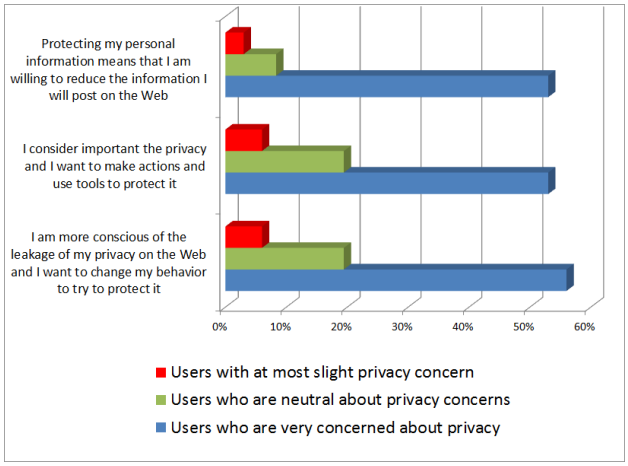

Fig. 7. Percentages of users reporting final behaviors, grouped by level of privacy concern.

It is worth to note that when interviewed about the possibility to reduce personal information posted on the Web, and specifically on the `Facebook.com` Web site, the agreement percentages, respect to the previous 2 questions (Q33 and Q34, Table IX), dropped for both groups. Even concerned about privacy, users seem not be worried about the leakage of their personal information, when some benefits can be obtained in return. Some reasons, in fact, output of open-ended text questions, include: (a) "*I need to add accurate information to OSNs to increase my visibility*", (b) "*I need to add accurate information to OSNs to find my old friends*", (c) "*I am comfortable with how much information I share, I have a control over my personal information*".

The most important result of this part of the study is the comparative assessment between some specific questions asked before and after the tool testing phase, in order to evaluate if changes occurred in users' opinions and habits after using a tool to protect privacy, NoTrace. Questions are shown in Table X.

When students were made informed about the potential harmful activities on the Web, and have learned by NoTrace in which way their personal information were leaked, they expressed increased concerns about risks to their privacy, especially when their data are disclosed to third party sites.

Table IX. Participants privacy *resultant* behaviors. 5-Point Mean Likert scores.

ID	Question	Mean		Agreement	
		non-ICT	***ICT***	***non-ICT***	***ICT***
Q33	I am more conscious of the leakage of my privacy on the Web and I want to change my behavior to try to protect it	4.06	3.83	72%	78%
Q34	I consider important the privacy and I want to make actions and use tools to protect it	4.11	3.94	83%	72%
Q35	Protecting my personal information means that I am willing to reduce the information I will post on the Web	3.72	3.61	67%	61%

Table X. Comparative assessment of questions posed before and after the testing phase.

Question	***non-ICT***			***ICT***		
	Mean		Paired T	Mean		Paired T
	Before	After	Sig. Level	Before	After	Sig. Level
I consider important the privacy in everyday life	4.11	4.33	0.041	4.17	4.28	N.S.
I am concerned about my privacy online	3.94	4.44	0.024	3.61	3.89	N.S.
When I am online, I am aware that my browsing information may be collected by a third party for advertising purposes	3.22	4.22	0.011	3.94	4.44	0.0459

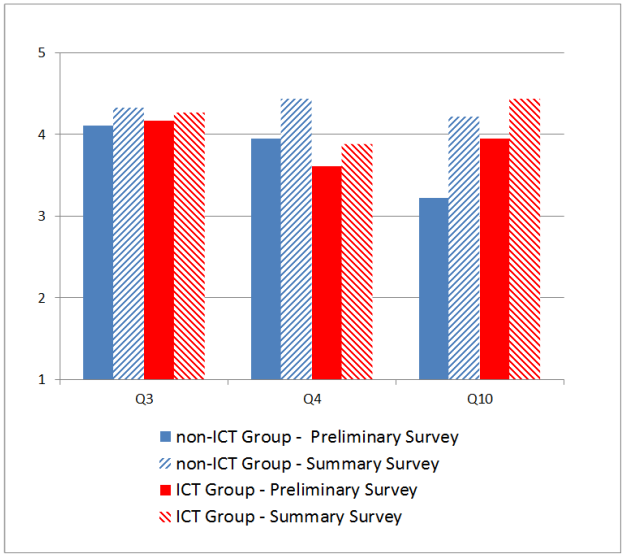

Fig. 8. Comparison of attitudes before and after using NoTrace during the testing phase.

In general, NoTrace allowed users to understand which personal and sensitive information they disclose during their online activities, in which extent and also, towards which third party sites. Support and awareness were able to involve changes in users' opinions, slightly increasing the level of concern about privacy in everyday life (mean values: 4.11 vs. 4.33 for the *non-ICT* Group and 4.17 vs. 4.28 for the *ICT* Group, Table X) and mostly increasing concerns about the online privacy for the *non-ICT* Group (3.94 vs. 4.44) and the awareness about third party tracking (for both groups). In Fig. 8 we can see how NoTrace involved greater concerns about privacy as well as a greater awareness about the tracking performed online by advertising companies. Additionally, in Table X we show that statistically significant differences for all questions exist only for the *non-ICT* users, highlighting, once again, the usefulness of NoTrace mainly for users without technological skills. For *ICT* users, instead, significant results are obtained only with regard to the awareness of the tracking performed by advertising companies. Both groups increased their awareness about the risks for their privacy related to the activities performed by large advertising companies (whose concerns were expressively disclosed in open-ended questions).

VI CONCLUSION

In this paper we presented an evaluation study to analyze if learning from one's behavior during online activities and awareness about who is gathering, collecting and linking personal information can help users to value their privacy and involve them to seriously take actions to protect it. To this aim we tested if a privacy-enhancing tool can contribute to increase both learning and awareness, helping users to learn from their actual behaviors, perceive what happens during their navigation, understand the corresponding risks and apply the correct countermeasures.

We evaluated that all participants equally (with no

statistical differences) consider important the privacy in everyday life, and that in general *non-ICT* students are more concerned about risks to their privacy online. We also showed that *non-ICT* students exhibit a little willingness to adopt privacy preserving technologies (i.e., install privacy tools, increase the security settings of the browsers, delete cookies and Internet files, read privacy policies) with statistical differences across groups except that for Web sites' policies, where groups exhibited similar behaviors.

When learning and awareness took place, after using NoTrace, all users expressed their willingness to change their behaviors online, from one side, and their unwillingness to withhold information mainly on social network sites, on the other side. Therefore, in the compromise between privacy leakage and achievable benefits for users, the winner is the need for them to make very easy their identification and to quickly expand their friends' community, continuing to generously provide an ever-increasing number of personal information.

Finally, we showed that NoTrace was helpful to make students aware of the risks to which they are continuously exposed during their navigation, involving changes in students' opinions, with statistical differences for *non-ICT* students with regards to general concerns about privacy and for both groups with regards to the risks of the behavioral advertising. Therefore, we showed that students without technical expertise, mostly unaware of privacy risks, and with lazy attitudes to protect their privacy, learned more when compared with technological-oriented students, representing the best beneficiaries of the instruments provided by NoTrace.

We have to emphasize that this work has some limitations. First, all participants at our study were students from an Italian academic environment. Our samples were composed of users with high education levels and with an age ranging from 20 to 30 years. Therefore, our results may not necessarily be representative of the entire world population.

Future work could look into privacy attitudes and behaviors with regard to older age groups, students from other academic areas and with even more diversified technological skills. Moreover, a larger number of subjects would provide more statistically significant results.

In conclusion, awareness about risks to the privacy and education about how to have control over own personal information, by using a privacy-enhancing technology, can effectively help individuals to value their own privacy, and reduce their degree of exposure while navigating the Web.

ACKNOWLEDGMENT

The authors would like to thank all users taking part at the study.

References

[1] D. Malandrino, A. Petta, V. Scarano, L. Serra, R. Spinelli, and B. Krishnamurthy, "Privacy Awareness about Information Leakage: Who knows what about me?" in *Workshop on Privacy in the Electronic Society (WPES)*, 2013.

[2] H. Beales, "The Value of Behavioral Targeting," http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf, 2010.

[3] C. Castelluccia, M.-A. Kaafar, and M.-D. Tran, "Betrayed by Your Ads! Reconstructing User Profiles From Targeted Ads," in *Proceedings of the 12^{th} International Conference on Privacy Enhancing Technologies*, ser. PETS, 2012, vol. 7384, pp. 1–17.

[4] B. Krishnamurthy and C. Wills, "Privacy diffusion on the web: a longitudinal perspective," in *Proceedings of the 18th International Conference on World Wide Web*, ser. WWW '09, 2009, pp. 541–550.

[5] C. Dwyer, "Privacy in the Age of Google and Facebook," *IEEE Technology and Society Magazine*, vol. 30, no. 3, pp. 58–63, 2011.

[6] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in *Workshop on Privacy in the Electronic Society*, ser. WPES '05, 2005, pp. 71–80.

[7] V. Lawton, "Privacy Commissioner of Canada. Popular websites in Canada disclosing personal information," http://www.priv.gc.ca/media/nr-c/2012/nr-c_120925_e.asp, 2012.

[8] D. Perito, C. Castelluccia, M. Kaafar, and P. Manils, "How Unique and Traceable Are Usernames?" in *11th Privacy Enhancing Technologies Symposium*, ser. PETS, 2011, vol. 6794, pp. 1–17.

[9] C. E. Wills and M. Zeljkovic, "A Personalized Approach to Web Privacy - Awareness, Attitudes and Actions," *Information Management & Computer Security*, vol. 19, no. 1, pp. 53–73, 2011.

[10] B. Krishnamurthy, K. Naryshkin, and C. E. Wills, "Privacy leakage vs. protection measures: the growing disconnect," in *Web 2.0 Security and Privacy Workshop*, 2011.

[11] J. K. Burgoon, R. Parrott, B. A. L. Poire, D. L. Kelley, J. B. Walther, and D. Perry, "Maintaining and Restoring Privacy through Communication in Different Types of Relationships," *Journal of Social and Personal Relationships*, vol. 6, no. 2, pp. 131–158, May 1989.

[12] DeCew Judith Wagner, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Cornell University Press, 1997.

[13] S. D. Warren and L. D. Brandeis, "The right to privacy," *Harward Law Review*, vol. 4, no. 5, pp. 193–220, December 1890.

[14] A. Westin, *Privacy and Freedom*. New York: New Jork Atheneum, 1967.

[15] M. J. Culnan, ""How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use," *MIS Quarterly*, vol. 17, no. 3, pp. pp. 341–363, 1993.

[16] F. D. Schoeman, *Privacy and Social Freedom*, D. MacLean, Ed. Cambridge University Press, 1992.

[17] J. B. Earp and F. C. Payton, "Information Privacy in the Service Sector: An Exploratory Study of Health Care and Banking Professionals," *Journal of Organizational Computing and Electronic Commerce*, vol. 16, no. 2, pp. 105–122, 2006.

[18] A. J. Kimmel, *Ethical Issues in Behavioral Research: Basic and Applied Perspectives*. Wiley-Blackwell, 2007.

[19] D. Malandrino and R. Spinelli, https://addons.mozilla.org/en-us/firefox/addon/notrace/.

[20] D. Malandrino and V. Scarano, "Supportive, Comprehensive and Improved Privacy Protection for Web Browsing," in *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust (PASSAT)*, 2011, pp. 1173–1176.

[21] D. Malandrino and Scarano, "Privacy leakage on the web: Diffusion and countermeasures," *Computer Networks*, vol. 57, no. 14, pp. 2833 – 2855, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128613001989

[22] M. J. Metzger, "Communication Privacy Management in Electronic Commerce," *Journal of Computer-Mediated Communication*, vol. 12, no. 2, pp. 335–361, 2007.

[23] M. van der Velden and K. E. Emam, "*Not all my friends need to know*": a qualitative study of teenage patients, privacy, and social media," *Journal of the American Medical Informatics Association, JAMIA '13*, vol. 20, no. 1, pp. 16–24, 2013.

[24] J. Y. Tsai, S. Egelman, L. Cranor, and A. Acquisti, "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study," *Information Systems Research*, vol. 22, pp. 254–268, June 2011.

[25] A. M. McDonald and L. F. Cranor, "Americans' attitudes about internet behavioral advertising practices," in *Proceedings of the* 9^{th} *annual ACM workshop on Privacy in the Electronic Society*, ser. WPES '10, 2010, pp. 63–72.

[26] E. Garbarino and M. Strahilevitz, "Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation," *Journal of Business Research*, vol. 57, no. 7, pp. 768 – 775, 2004.

[27] G. Grubbs M., Milne, "Gender Differences in Privacy-Related Measures for Young Adult Facebook Users," *Journal of Interactive Advertising*, vol. 10, no. 2, pp. 28–45, 2010.

[28] B. K. Sheehan, "An investigation of gender differences in online privacy concerns and resultant behaviors," *Journal of Interactive Marketing*, vol. 13, no. 4, pp. 24–38, 1999.

[29] L. S. Strickland and L. E. Hunt, "Technology, security, and individual privacy: New tools, new threats, and new public perceptions: Research articles," *Journal of the American Society for Information Science and Technology*, vol. 56, no. 3, pp. 221–234, Feb. 2005.

[30] A. Acquisti, K. J. Leslie, and G. Loewenstein, "The Impact of Relative Standards on the Propensity to Disclose," *Journal of Marketing Research*, pp. 1–15, 2011.

[31] A. N. Joinson, C. Paine, T. Buchanan, and U.-D. Reips, "Measuring self-disclosure online: Blurring and non-response to sensitive items in web-based surveys," *Computers in Human Behavior*, vol. 24, pp. 2158–2171, September 2008.

[32] I. Ion, N. Sachdeva, P. Kumaraguru, and S. Čapkun, "Home is safer than the cloud!: privacy concerns for consumer cloud storage," in *Proceedings of the Seventh Symposium on Usable Privacy and Security*, ser. SOUPS '11, 2011, pp. 13:1–13:20.

[33] S. Patil, G. Norcie, A. Kapadia, and A. J. Lee, "Reasons, rewards, regrets: privacy considerations in location sharing as an interactive practice," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ser. SOUPS '12, 2012, pp. 5:1–5:15.

[34] J. Watson, A. Besmer, and H. R. Lipford, "+Your circles: sharing behavior on Google+," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ser. SOUPS '12, 2012, pp. 12:1–12:9.

[35] J. Staddon, D. Huffaker, L. Brown, and A. Sedley, "Are privacy concerns a turn-off?: engagement and privacy in social networks," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ser. SOUPS '12, 2012, pp. 10:1–10:13.

[36] D. Boyd and E. Hargittai, "Facebook privacy settings: Who cares," *First Monday*, vol. 15, no. 8, 2010.

[37] E. Butler, E. McCann, and J. Thomas, "Privacy Setting Awareness on Facebook and Its Effect on User-Posted Content," *Human Communication*, vol. 14, no. 1, pp. 39–55, 2011.

[38] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing facebook privacy settings: user expectations vs. reality," in *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, ser. IMC '11, 2011, pp. 61–70.

[39] M. Johnson, S. Egelman, and S. M. Bellovin, "Facebook and privacy: it's complicated," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ser. SOUPS '12, 2012, pp. 1–15.

[40] C. Paine, U.-D. Reips, S. Stieger, A. Joinson, and T. Buchanan, "Internet users' perceptions of 'privacy concerns' and 'privacy actions'," *International Journal of Human-Computer Studies*, vol. 65, no. 6, pp. 526–536, Jun. 2007.

[41] B. Ur, P. G. Leon, L. F. Cranor, R. Shay, and Y. Wang, "Smart, useful, scary, creepy: perceptions of online behavioral advertising," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ser. SOUPS '12, 2012, pp. 4:1–4:15.

[42] A. N. Joinson, U.-D. Reips, T. Buchanan, and C. B. P. Schofield, "Privacy, Trust, and Self-Disclosure Online," *Human-Computer Interaction*, vol. 25, no. 1, pp. 1–24, 2010.

[43] A. Acquisti and J. Grossklags, "Privacy and Rationality in Individual Decision Making," *Security Privacy, IEEE*, vol. 3, no. 1, pp. 26 –33, 2005.

[44] N. F. Awad and M. S. Krishnan, "The personalization privacy paradox: an empirical evaluation of information transparency and the willingness to be profiled online for personalization," *MIS Quarterly*, vol. 30, no. 1, pp. 13–28, Mar. 2006.

[45] T. Buchanan, C. Paine, A. N. Joinson, and U.-D. Reips, "Development of Measures of Online Privacy Concern and Protection for Use on the Internet," *Journal Of The American Society For Iinformation Science And Technology*, vol. 58, pp. 157–165, January 2007.

[46] C. Jensen, C. Potts, and C. Jensen, "Privacy practices of Internet users: Self-reports versus observed behavior," *International Journal of Human-Computer Studies*, vol. 63, no. 1-2, pp. 203 – 227, 2005.

[47] A. M. McDonald, R. W. Reeder, P. G. Kelley, and L. F. Cranor, "A Comparative Study of Online Privacy Policies and Formats," in *Proceedings of the* 5^{th} *Symposium on Usable Privacy and Security*, ser. SOUPS '09, 2009, pp. 46:1–46:1.

[48] C. Canali, M. Colajanni, D. Malandrino, V. Scarano, and R. Spinelli, "A Novel Intermediary Framework for Dynamic Edge Service Composition," *Journal of Computer Science and Technology*, vol. 27, pp. 281–297, 2012.

[49] B. Krishnamurthy, D. Malandrino, and C. E. Wills, "Measuring privacy loss and the impact of privacy protection in web browsing," in *Symposium on Usable Privacy and Security, SOUPS '07*, 2007, pp. 52–63.

[50] D. Malandrino, V. Scarano, and R. Spinelli, "How increased awareness can impact attitudes and behaviors toward online privacy protection," in *2013 IEEE Third International Conference on Privacy, Security, Risk and Trust (PASSAT)*, 2013.

[51] D. F. Galletta, R. M. Henry, S. McCoy, and P. Polak, "Web site delays: How tolerant are users?" *Journal of the Association for Information Systems*, vol. 5, no. 1, 2004.

[52] W. Palant, "AdBlock Plus," http://adblockplus.org/.

[53] Ghostery, http://www.ghostery.com/.

[54] Abine, "DoNotTrackMe," https://www.abine.com/dntdetail.php.

[55] L. G. Berry, M., *Data Mining Techniques: For Marketing, Sales, and Customer Relationship Management*. Wiley, 1997.

[56] A. Westin, "Harris-equifax consumer privacy survey," WESTIN, A. AND HARRIS LOUIS & ASSOCIATES. Conducted for Equifax Inc, Tech. Rep., 1991.

[57] M. S. Ackerman, L. F. Cranor, and J. Reagle, "Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences," in *Proc. of the 1st ACM conference on Electronic commerce*, ser. EC '99, 1999, pp. 1–8.

APPENDICES

A SURVEY QUESTIONS

Questions of questionnaires have been translated from the Italian language.

1 PRELIMINARY SURVEY QUESTIONNAIRE

- Q1: How much time do you spend on Internet (hours per day)?
  - Less than two hours
  - Between two and four hours
  - between four and six hours
  - More than six hours

- Q2: Which browser do you usually use?
  - Mozilla Firefox
  - Google Chrome
  - Internet Explorer
  - Opena
  - Safari
  - Other

- Q3: I consider important the privacy in everyday life
  - Strongly disagree
  - Disagree
  - Neither agree nor disagree
  - Agree
  - Strongly agree

- Q4: I am concerned about my privacy online
  - *Same answer options as Q3*

- Q5: What do you worry about mostly of the privacy online?
  - *Open-ended text question*

- Q6: I am familiar with the Web Bug term
  - *Same answer options as Q3*

- Q7: I am familiar with the Flash cookie term
  - *Same answer options as Q3*

- Q8: I am familiar with behavioral advertising term
  - *Same answer options as Q3*

- Q9: I am aware of the risks of behavioral advertising
  - *Same answer options as Q3*

- Q10: When I am online, I am aware that my browsing information may be collected by third party entities for advertising purposes
  - *Same answer options as Q3*

- Q11: I am comfortable with advertisers using my browsing history to serve me relevant ads, as long as that information cannot be tied to my name or any other personal information
  - *Same answer options as Q3*

- Q12: I am comfortable with the privacy I have when I use search engines
  - *Same answer options as Q3*

- Q13: It is my responsibility to protect my personal information
  - *Same answer options as Q3*

- Q14: I am aware of the tools that exist online to help me protect my privacy online
  - *Same answer options as Q3*

- Q15: What privacy protection tool have you ever installed?
  - *Open-ended text question*

- Q16: Have you ever changed your browser privacy settings?
  - Yes
  - No

- Q17: Have you ever installed a privacy add-on for your browser?
  - *Same answer options as Q16*

- Q18: Have you ever installed a tool to protect your privacy?
  - *Same answer options as Q16*

- Q19: What do you expect from a privacy protection tool?
  - *Open-ended text question*

- Q20: How often do you delete cookies from your PC?
  - Never
  - Every Day
  - At least one a week
  - 2 to 3 times a week
  - Once a month or less often
  - 2 to 3 times a month

- Q21: How often do you delete Internet Files from your PC?
  - *Same answer options as Q20*

- Q22: When you enter your personal information on a Web site how often you read privacy policies (if provided)?
  - Never
  - Rarely
  - Sometimes
  - Often
  - Most of the time

- Q23: If I have to choose between search quality and search privacy, I would choose:
  - Search quality
  - Search ahead of privacy
  - Privacy ahead of search
  - Search privacy

- Q24: If you knew for a fact that topics you search for using a search engine were saved forever, would it change your search habits?
  - No changes
  - Minor changes
  - Major changes
  - Completely change

- Q25: How do you consider your technical experience online?
  - Beginner
  - More than a beginner, but I still have to learn
  - Competent
  - More than competent but not yet expert
  - Expert

- Q26: About protecting my personal and sensitive information leaked on the Web (Full name, SSN, phone number, login, password, beliefs, health information)
  - I know exactly how to protect them
  - I know exactly how to protect them but and I am not able to do it
  - I do not know how to protect them

2 SUMMARY SURVEY QUESTIONNAIRE

- Q27: Overall, It was easy to use NoTrace
  - Strongly disagree
  - Disagree
  - Neither agree nor disagree
  - Agree
  - Strongly agree

- Q28: NoTrace improved my Web experience
  - *Same answer options as Q27*

- Q29: How your Web experience was improved?
  - *Open-ended text question*

- Q30: Each enabled technique in NoTrace does exactly what I expected
  - *Same answer options as Q27*

- Q31: Do you will continue to use NoTrace?
  - *Same answer options as Q27*

- Q32: Would you suggest NoTrace to a friend?
  - Yes
  - No

- Q33: I am aware of the privacy leakage on the Web and I want to change my habits in order to protect it
  - *Same answer options as Q27*

- Q34: I consider important to protect my privacy by studying and installing tools that limit the diffusion of my personal information
  - *Same answer options as Q27*

- Q35: To protect my privacy, I am ready to limit the amount of personal information that I usually enter on the Web. For example, limiting the information on Facebook
  - *Same answer options as Q27*

2.1 QUESTIONS ALSO POSED IN THE PRELIMINARY SURVEY

- Q3_Post: I consider important the privacy in everyday life
  - Strongly disagree
  - Disagree
  - Neither agree nor disagree
  - Agree
  - Strongly agree

- Q4_Post: I am concerned about my privacy online
  - Strongly disagree
  - Disagree
  - Neither agree nor disagree
  - Agree
  - Strongly agree

- Q10_Post: When I am online, I am aware that my browsing information may be collected by a third party entities for advertising purposes
  - Strongly disagree
  - Disagree
  - Neither agree nor disagree
  - Agree
  - Strongly agree

3 QUIS QUESTIONNAIRE

Based on: Chin, J.P., Diehl, V.A., Norman, K.L. (1988) Development of an Instrument Measuring User Satisfaction of the Human-Computer Interface. ACM CHI'88 Proceedings, 213-218, 1998.

Please rate your satisfaction with the system.

- Overall reaction to the Software
  1. Terrible / Wonderful
  2. Difficult / Easy
  3. Frustrating / Satisfying
  4. Dull / Stimulating
  5. Rigid / Flexible

- Screen
  6. Reading characters on the screen
     – Hard / Easy
  7. Organization of information
     – Confusing / Very Clear

- Terminology and system information
  8. Use of terms throughout system
     – Inconsistent / Consistent
  9. Terminology related to task
     – Never / Always
  10. Position of messages on screen
     – Inconsistent / Consistent

- Learning
  11. Learning to operate the system
     – Difficult / Easy
  12. Remembering names and use of commands
     – Difficult / Easy
  13. Performing tasks is straightforward
     – Never / Always

- System capabilities
  14. System speed
     – Too slow / Fast enough
  15. System reliability
     – Unreliable / Reliable
  16. System tends to be
     – Noisy / Quiet
  17. Designed for all levels of users
     – Never / Always

4 CSUQ QUESTIONNAIRE

Based on: Lewis, J. R. (1995) IBM Computer Usability Satisfaction Questionnaires: Psychometric Evaluation and Instructions for Use. International Journal of Human-Computer Interaction, 7:1, 57-78.

1. Overall, I am satisfied with how easy it is to use this system
   - Strongly Disagree / Strongly Agree
2. It was simple to use this system
   - Strongly Disagree / Strongly Agree
3. I feel comfortable using this system
   - Strongly Disagree / Strongly Agree
4. It was easy to learn to use this system
   - Strongly Disagree / Strongly Agree
5. The information (such as online help, on-screen messages, and other documentation) provided with this system is clear
   - Strongly Disagree / Strongly Agree
6. It is easy to find the information I needed
   - Strongly Disagree / Strongly Agree
7. The information provided for the system is easy to understand
   - Strongly Disagree / Strongly Agree
8. The organization of information on the system screens is clear
   - Strongly Disagree / Strongly Agree
9. The interface of this system is pleasant
   - Strongly Disagree / Strongly Agree
10. I like using the interface of this system
    - Strongly Disagree / Strongly Agree
11. This system has all the functions and capabilities I expect it to have
    - Strongly Disagree / Strongly Agree
12. Overall, I am satisfied with this system
    - Strongly Disagree / Strongly Agree