User Perceptions of Sharing, Advertising, and Tracking

Farah Chanchary
School of Computer Science
Carleton University
Ottawa, Canada
farah.chanchary@carleton.ca

Sonia Chiasson
School of Computer Science
Carleton University
Ottawa, Canada
chiasson@scs.carleton.ca

ABSTRACT

Extending earlier work, we conducted an online user study to investigate users' understanding of online behavioral advertising (OBA) and tracking prevention tools (TPT), and whether users' willingness to share data with advertising companies varied depending on the type of first party website. We presented results of 368 participant responses across four types of websites - an online banking site, an online shopping site, a search engine and a social networking site.

In general, we identified that participants had positive responses for OBA and that they demonstrated clear preferences for which classes of information they would like to disclose online. Our results generalize over a variety of website categories containing data with different levels of sensitivity, as opposed to only the medical context as was shown in previous work by Leon et al. In our study, participants' privacy attitudes significantly dominated their sharing willingness. Interestingly, participants appreciated the idea of user-customized targeted ads and some would be more willing to share data if given prior control mechanisms for tracking protection tools.

1. INTRODUCTION

Internet advertising has become increasingly user-sensitive. Advertising networks track users online and create user profiles based on their online activities and preferences without consent from users. These profiles help advertising networks decide which ads are more likely to be of interest to a particular user. The main mechanism for online tracking is third party HTTP cookies by advertising domains [9]. Since users directly interact with first party websites and may be unaware of hidden third parties, the data collection process may presumably violate their online privacy. Previous studies showed that familiarity with advertising companies influenced participants' data sharing willingness [23] and participants' choice to disclose certain classes of information mostly depended on the third parties collecting the data [8].

Symposium on Usable Privacy and Security (SOUPS) 2015, July 22–24, 2015, Ottawa, Canada.

Leon et al. [8] compared two similar online health/medical websites as the first party to explore how privacy practices of their assigned site might influence participants' data sharing willingness, but the study results did not reveal any significant impact of the first party site. In general, medical information is sensitive and contains many unique characteristics that might make it different from other domains. We re-investigate users' perceptions of OBA based on their interactions with first party websites of varying sensitivity. We further extend our investigation by incorporating the impact of participants' privacy attitude, privacy practices, and technical background.

According to Consumer Action's 2013 survey [5], 69% of consumers were unwilling to allow companies to track them in exchange for a free service or product, and 87% believed they should have the right to control what is collected about them online. A variety of privacy tools are available to control OBA [9]. Some tools use opt-out cookies to store a user's preference not to receive OBA, while other tools transmit *Do Not Track* headers to websites to signal a user's request. These tools are challenging for users to understand [9] and sometimes users cannot properly distinguish between tracking prevention tools and ad blocking tools [1]. We examined users' understanding of TPT and what control features might make them more willing to share information for OBA.

In this online study, we aimed to understand how users experience behavioral advertising online and how their preferences across website categories and privacy control features of TPT influenced their willingness to share data. Using an online survey, we collected responses from 368 participants. Confirming and extending Leon et al.'s work, our participants showed a relatively consistent level of willingness to share personal information with different web sites they visited. Participants with the highest general concern for privacy (Privacy Fundamentalists) were least willing to share any type of information online. Participants with technical (computer or IT related) background showed increased willingness to share information for OBA. User friendly tracking-prevention tool (TPT) features also made participants more inclined to share data. However, having access to view and edit user profiles had only moderate impact on their data sharing willingness. Overall, participants were not interested in paying money to block online tracking or targeted ads. On the contrary, their responses showed that they preferred to see relevant website ads and would

share their personal information with online advertisers to receive these ads if they could control what information to share and with whom.

We summarized related work that motivated us to conduct this study in Section 2. In Section 3, we described our study methodology and analysis techniques. In Section 4, we presented study results covering participants' demographic information, understanding of OBA and TPT, willingness to share data online, and other factors that influenced their willingness. Discussion and limitations of our study are in Section 5 and our conclusions are in Section 6.

2. RELATED WORK

Recently, a number of studies have been conducted on the practices of OBA and the usability of privacy tools that allow users to control online advertising. In 2012, Ur et al. [23] presented results of 48 semi-structured interviews where participants found OBA to be simultaneously useful and privacy invasive. They also reported that participants had strong concerns about advertising companies collecting personally identifiable information but their attitudes were context dependent. Participants' willingness to share information varied depending on their familiarity with and the level of advertising activities of these ad companies. In a similar interview-based study by Agarwal et al. [1], the authors reported that the issue of online tracking made users concerned and sensitive about the content in online ads and how the context surrounding their browsing behavior could lead to varying levels of embarrassment. Moreover, the authors mentioned third-party-indifference as a major finding since they did not observe any difference between participants' sensitivities towards the trust levels across third parties. A study by Costante et al. [6] investigated Internet users' perception of the trustworthiness of websites using four types of websites (e-commerce, e-health, e-bank and e-portfolio) and showed that users' perception of trust varied with application domains and users' IT related knowledge. A 2012 survey [18] on the use of search engines showed that despite majority of users viewing these websites as useful and trustworthy, they neither agreed to share search data for receiving personalized results nor were aware of ways to restrict the data collection process. In 2014, Rader [19] examined participants' level of awareness of behavioral tracking and privacy concern based on first party data collection using a social network site (Facebook) and a search engine (Google). Her study results showed that despite having profound knowledge about first party data tracking, participants were much less aware of automatic collection, collaboration and data aggregation across various websites.

Users' lack of knowledge of tracking prevention tools also affect their intentions to adopt suitable privacy practices. McDonald and Cranor [14] found that the majority of American Internet users (86%) were aware of targeted ads but lacked the knowledge to make informed decisions to protect their privacy. The authors also reported users' misconceptions about the purpose of cookies and the effects of clearing them. They highlighted discrepency between people's willingness to pay to protect their privacy and their willingness to accept discounts in exchange for private information. A survey by McDonald and Peha [15] in 2011 also suggested a large gap between the actual implementation of *Do Not Track* in web browsers and what users expected from it, e.g., stopping complete data collection and data aggregation across websites. Leon et al. [9] conducted a laboratory study investigating the usability of nine privacy tools to restrict OBA. Participants misunderstood how these tools worked and mistakenly believed that they were protected against tracking, while in reality they might no longer see targeted ads but continue to be tracked.

Lack of transparency of data collection practices also raised privacy concerns. In a 2006 study, Awad and Krishnan [2] investigated relationships between information transparency features (e.g., data removal and time expirations of data) and consumers' willingness to share information for online personalization. The authors reported that participants who were concerned about these features were less willing to have an online profile. A 2009 survey [22] showed that 92% of users were in favor of a law that requires online advertising companies to delete all stored information about an individual on request. An interesting finding of Leon et al.'s [8] paper was that 52% of participants would be equally or less likely to share data if they were given access to view and edit data collected about them. In a recent paper, Rao et al. [20] explored transparency of data collection practices and accuracy of data in user profiles. They found large number of user profiles with as much as 80% inaccuracy.

Leon et al. [8] presented how users' willingness to share personal information with advertising companies changed depending on these companies' privacy practices. In contrast to Agarwal et al.'s results, participants were mostly concerned with the third party that collected the data, rather than the first-party site. Since the authors explored only a few choices for the first party (i.e., two versions of an online health web site), we investigated in our study whether users truly had no concerns regarding first party tracking. We also explored whether users understood the advantages of using privacy tools or whether they preferred simple ad blocking tools.

3. METHODOLOGY

We conducted a between-subjects online study to investigate users' understanding and preferences for sharing information online. We partially followed the research methodology adopted by Leon et al. [8]. In this section, we describe our recruitment process using the CrowdFlower platform, the research objectives, the structure of our survey questionnaire, and the techniques used to analyze data.

3.1 Recruitment using CrowdFlower

We recruited participants from around the world using an online crowdsourcing service, namely CrowdFlower[1], in two phases. Initially, we recruited 45 participants to ensure the usability of our questionnaire and correctness of the data collection process. In the second phase, we collected responses from 355 participants using a similar procedure. Our recruitment materials indicated that the study would be about how individuals experience the Internet and OBA.

[1] `http://www.crowdflower.com/`

There was no indication that privacy would be one of the research components of this study. Our survey did not collect any sensitive information and all participants remained anonymous. Participants received $0.50 for completing the survey. This study was approved by our Institutional Research Ethics Board.

3.2 Research Questions

We sought answers to these questions regarding users' understanding and preferences for sharing information online:

Q1. What are participants' current practices, understanding, and perception of OBA and targeted ads?

Q2. Do participants' preferences vary based on categories of first party websites? Is first party more important than the third party?

Q3. Do users' privacy attitudes affect their sharing willingness?

Q4. What features of TPT influence participants' willingness to share?

3.3 Structure of the Questionnaire

Our survey questionnaire was divided into six parts.

1. *Demographic Information*: we collected participants' age, gender, highest level of education, occupation and the amount of time they spent online.

2. *Basic Understanding of Online Advertising*: we asked them to define website advertising, targeted ads, tracking prevention tool, and give their opinions about website advertising and online tracking.

3. *Informational Video*: we provided a link to a short informational video on OBA produced by the *Wall Street Journal* [2] to help them learn how OBA actually works, and we asked them two basic test questions on the concepts of third party cookies and behavioral targeting.

4. *Willingness to Share Information*: we explored participants' willingness to share information online using 5 point Likert-scales (from "Strongly Disagree" to "Strongly Agree"). We used 24 types of information that constituted a subset of 30 types used by Leon et al. [8]. These 24 types were selected because they contained both Personally Identifiable Information (PII) and Non-PII for users, as defined by the Network Advertising Initiative (NAI) [17]. Moreover, these were not related to properties of any specific type of website. For this part only, participants were evenly distributed into four groups and assigned to one type of website services, i.e., an Online Banking site (OB), Online Shopping site (OS), Search Engine (SE) or Social Network site (SN). Participants disclosed their willingness to share information with their assigned first party site. Next, we asked how concerned they were for both first and third party tracking using 5 point Likert-scales (from "Strongly Concerned" to "Strongly Unconcerned"). We also asked whether they would change their preferences if given a fee payment option to control the online data collection process or an option to access their online data for review, edit or deletion.

5. *Understanding of TPT*: we asked for participants' views on TPT, ad blocking tools, and privacy control features that might make them more comfortable with data sharing.

6. *Users' Privacy Attitudes and Practices*: we explored participants' general privacy views, using the Westin Index [21] and their previous privacy practices (e.g., deleting cookies, reading websites' privacy policies, refusing disclosure of sensitive personal information). Finally, we asked for their comments on OBA.

See Appendix B for the full questionnaire.

[2] `http://www.tamingdata.com/2010/10/18/how-advertisers-use-internet-cookies-to-track-your-online-habits/`

3.4 Test Questions

Using the two questions from Part 3, we performed a screening test to identify and discard information from participants who were not paying attention. We found 32 participants with incorrect answers (see Q23 and Q24 in Appendix B). All further data analysis used responses from 386 participants who passed both test questions.

3.5 Analysis

We performed statistical tests to identify significant patterns among several data elements collected through our survey questionnaire. All statistical tests were done with R version 3.1.2 and assumed a significance level of $p < 0.05$. We conducted a factor analysis to identify patterns in participants' sharing willingness and group closely related information together. This facilitated our investigation of how participants perceived concerns for online tracking of similar data types. We also employed the Westin Index to categorize participants according to their privacy outlook. We subsequently examined how participants with different privacy attitudes weighted online information disclosure. We first present our factor analysis and Westin Index analysis in this section. Results of these analyses will be used to help answer our research questions in Section 4.

3.5.1 Factor Analysis

To investigate how the categories of websites influenced participants' willingness to share 24 types of information, we performed factor analysis to reduce these 24 types to a smaller number of output variables. Factor analysis is a process that evaluates underlying associations of closely related variables and combines them into a single latent factor. If such underlying factors exist, then further analysis is performed based on these factors instead of the individual variables. A similar process was followed by Leon et al. [8].

Our exploratory factor analyses found that 17 variables could be grouped into 4 factors and the remaining 7 data

Table 1: Factor Analysis of willingness to disclose different types of information ($N = 386$). We present Cronbach's α for each resultant factor and the factor loading value for each variable. Percentage of agreement represents those who agreed or strongly agreed to disclose this information.

Factor **(Variables included)**	**Factor Loading**	**Agreement (%)**
Demographic Information **(α=0.897)**	–	**39**
Age	0.68	39
Gender	0.73	54
Weight and Height	0.65	35
Highest level of Education	0.70	44
Religion	0.69	32
Sexual Orientation	0.62	34
Marital Status	0.68	35
Personal Identification & Financial Information **(α=0.906)**	–	**13**
Address	0.76	14
Phone number	0.80	15
SIN/SSN	0.93	10
Credit Card No.	0.87	10
Credit Score Bracket	0.66	17
Location Information **(α=0.905)**	–	**46**
Country	0.67	55
State	0.82	44
Town	0.80	39
Computer Information **(α=0.826)**	–	**39**
Computer's OS	0.74	41
Computer's Browser	0.79	38
Variables that did not conform to any factor	–	–
Hobbies	NA	46
Name	NA	34
Zip code	NA	30
Email address	NA	28
Political preferences	NA	22
Income Bracket	NA	17
Computer's IP Address	NA	16

types did not conform to any particular factor. As in Leon et al. [8], we considered a variable part of a factor if it had a factor loading of at least 0.6 for the particular group, as well as factor loadings under 0.4 for all other groups. We named the resultant factors: *(1) Demographic Information*, *(2) Personal Identification & Financial Information*, *(3) Location Information*, and *(4) Computer Information*. The results of this factor analysis is given in Table 1. We used Cronbach's alpha (α) value for each factor to estimate the internal reliability of the factor analysis test. All four resultant factors had alpha values higher than 0.8, which is the standard to support high correlations between group members. All further analyses considered the four resultant factors. We created an index variable for each factor by averaging participants' responses to all the questions included in the factor.

3.5.2 Westin Index Analysis

The Westin Index [21] is a set of three questions (see Appendix B, Questions 74-76) designed to segment users into three groups: (1) Privacy Fundamentalists, who view privacy as having an especially high value which they feel very strongly about; (2) Privacy Pragmatists, who have strong feelings about privacy but can also see the benefits from surrendering some privacy in situations where they believe care is taken to prevent the misuse of this information; and (3) Privacy Unconcerned, who have no real concerns about privacy or about how other people and organizations use information about them.

The Westin Index has been widely used in the literature to measure users' attitudes towards privacy [4, 10–12]. In 2014, Woodruff et al. [24] argued based on their online survey results that generic privacy attitudes prescribed by the Westin Index did not correlate with individuals' attitudes and behavioral intentions for the protection or disclosure of personal information online. However, we followed the original segmentation index to remain consistent with earlier work since this was not central to our exploration.

Based on the Westin Index, we divided participants into three groups according to their privacy attitudes. We found that 30.4% of our participants were Privacy Fundamentalists, 45.9% were Privacy Pragmatics and 23.6% were Privacy Unconcerned. This conforms to typically observed demographics [21]. We used these groupings to explore how participants' privacy attitudes influenced their sharing willingness. Where appropriate, we further analyzed these correlations according to categories of websites.

4. RESULTS

In this section, we present an analysis of participants' survey responses addressing each of our research questions identified in Section 3.2. We analyzed responses from 386 participants between the ages 18 and 73 (mean=31.7 and σ=9.5). Participant demographics are summarized in Table 2.

4.1 Practices, Understanding & Perception (Q1)

We analyzed participants' responses by measuring their basic level of understanding of online advertising, tracking, and TPT. We asked open-ended questions requesting an explanation of these terms in their own words. We checked each answer and considered it as correct if it contained at least some basic keywords indicating that they understood the concepts. Our study results showed that 55% of participants could define website advertising. Only 6% of participants mentioned that website advertising was beneficial, while others thought it was spam (2%), annoying (6%) and false information (2%). Even though almost half of participants had degrees or work experience in computer related fields, we found that overall awareness about how targeted ads and privacy protection tools work was very low. We asked them to explain how targeted ads worked and 46% had at least partially correct answers. Only 38% of participants could correctly explain how TPT worked.

Table 2: Participants' Demographic Information.

Demographic	Number	Percent
Gender		
Female	99	27
Male	265	72
Decline to answer	4	1
Occupation		
Administrative support	29	8
Art, writing, or journalism	16	4
Business, management, or finance	45	12
Computer engineering	75	20
Education (e.g., Teacher)	26	7
Engineering	18	5
Homemaker	13	4
Service (e.g., retail clerks)	20	5
Skilled labor	21	6
Student	57	16
Unemployed	29	8
Other	12	4
Decline to answer	7	2
Educational Background		
No/Some high school	13	4
High school graduate	75	20
Some college	59	16
Associate's degree	35	10
Bachelor's degree	121	33
Graduate degree	61	17
Decline to answer	4	1
IT Background		
Yes	180	49
No	188	51
Internet Usage (hrs./day)		
1-5	85	23
5-9	149	40
9-13	74	20
13-17	45	12
>17	15	4

4.1.1 Website Ads and Online Tracking

Using 5-point Likert scales (1 = "most negative", 5 = "most positive"), participants expressed their views about different aspects of website advertising. Results are available in Figure 1. Half of participants agreed that website advertising is necessary to enjoy free services on the Internet, 42% found website advertising useful, and 42% believed that website advertising relevant to their interests can save time. However, half also said that they did not normally notice the ads that appeared on the websites that they visited.

Using another 5-point Likert scales (1 = "impossible", 5 = "very common"), participants expressed their understanding of online tracking. Approximately half of participants were aware of the various tracking capabilities. Figure 2 summarizes participants' opinions. Nearly one-fifth of participants believed it was impossible for online tracking systems to track all websites visited, and some wrongly believed that companies did not track individuals' online activities without users' permission (27%).

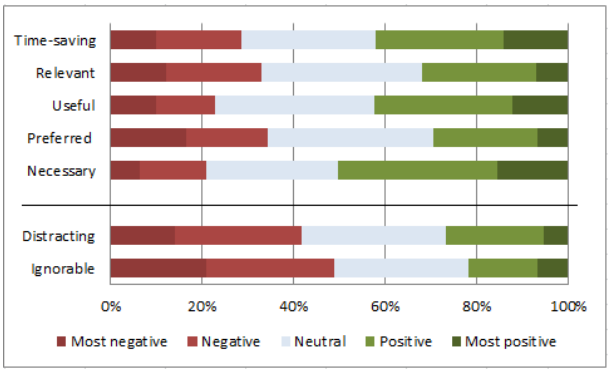

Figure 1: Views on website advertising. Statements included *"In general, I find website advertising..."*.

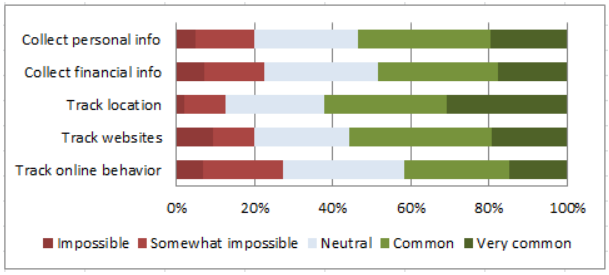

Figure 2: Views on online tracking. "Track websites" and "Track online behavior" are inverted for data presentation.

4.1.2 Targeted Ads

We inquired about users' perceptions of receiving targeted ads based on their online activities. Only 23% of participants liked receiving targeted ads reflecting their online activities, while 37% expressed clear dislike, and the remainder were neutral. In response to our open-ended question, *"Explain what, if anything, would make you feel more comfortable with receiving targeted ads?"*, participants displayed a variety of reactions, including criticisms for currently generated targeted ads. Participants did not perceive relevance or value from targeted ads based on their browsing histories. They saw much more value in seeing ads based on their actual expressed interests. This was clearly articulated by participants in our study: *"Most of the time I get ads that have nothing to do with me, being a girl doesn't mean I'm looking for makeup or trying to get skinny or whatever other stereotyped information that make ads show up"* or *"I'm tired of keep getting ads that I searched over 1 month ago"*.

4.1.3 Current Privacy Practices

We explored participants' previous online behavior to measure how concerned they were about their online privacy in practice. Figure 3 shows that the majority of users (>80%) demonstrated conscious responses to preserve their online privacy either by refusing to provide unnecessary personal information to websites, deleting cookies from web browsers, or terminating online transactions when they were uncertain about the data retention and usage policies. The least popular practice was activating the *Do Not Track* option in web browsers or installing TPT on their computers (58%). We

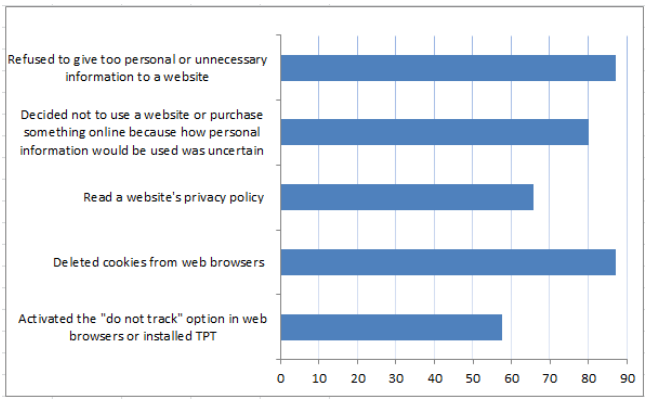

Figure 3: Percentage of participants who have previously employed 5 privacy practices.

found that while users are taking steps to prevent online data leakage, they use only a subset of available safeguards.

4.1.4 Answer to Q1

Q1 asks *What are participants' current practices, understanding, and perception of OBA and targeted ads?* Half of our participants were aware of OBA and were actively protecting their online privacy, but most of them were oblivious to the functionalities of TPT. In general, participants were not satisfied with receiving targeted ads based on their online activities. While half of participants appreciated the idea of user-customized targeted ads, half (not mutually exclusive) reported generally ignoring current targeted ads.

4.2 Impact of First and Third Parties (Q2)

This section summarizes participants' willingness to share their information online for the purpose of showing targeted ads on websites.

4.2.1 Effects of First Party and Data Types

We were interested in whether Internet users' preferences vary for different types of first party websites. We compared financial websites, shopping sites, search engines, and social networks. We did not find any major differences between website categories, confirmed by statistical analysis.

However, participants do distinguish between different types of information. Figure 4 shows participants' responses for sharing willingness based on a 5 point Likert scale across all websites. We found that participants expressed relatively consistent preferences for 24 types of information across the four website categories. Responses from individual website categories are available in the appendix (Figures 8, 9, 10 and 11). Overall, participants were more willing to share their country (55%), gender (54%), hobby (46%) or state (44%). Few wanted to disclose their credit card number (10%), social identification or security number SIN/SSN (10%), phone number (15%) or exact address (14%). Factor analysis results also uniformly confirms that more participants were willing to share their location information (46%), demographic and computer information (39%) than their personal

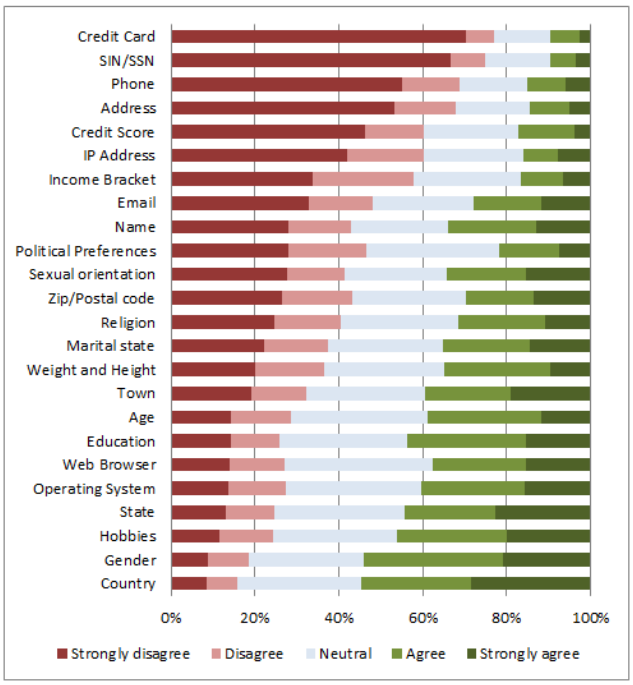

Figure 4: Willingness to disclose to a first party website.

Table 3: Level of Concern for First and Third parties.

Group	Concerned (%)		Unconcerned (%)	
	1^{st} party	3^{rd} party	1^{st} party	3^{rd} party
OB	37	55	20	14
OS	51	53	21	15
SE	42	41	9	20
SN	43	46	20	19

identification and financial information (13%) (see Table 1). These results are consistent with that of the previous study published by Leon et al. [8] where they used health websites. However, our results confirmed that preferences also holds for variety of first party websites (i.e., financial websites, shopping sites, search engines and social networks).

4.2.2 Concern for First and Third Party Tracking

We asked participants to express their concern for first party tracking (based on their designated website) and third party tracking without mentioning the name of any particular third party (see Appendix B, Questions 54 - 55). As shown in Table 3, only participants of the online banking (OB) group expressed increased concern (55%) for third party tracking compared to their online banking sites (37%). We suggest two possible reasons for this result. First, online banking sites generally do not show a large number of online ads compared to other sites so any ads may be viewed suspiciously. Secondly, users manage highly sensitive financial data through OB sites, and wish to avoid third party tracking of such data. In general, participants from other groups expressed approximately equal levels of concern for both first and third parties.

4.2.3 Answer to Q2

Q2 asks *Do participants' preferences vary based on categories of first party websites? Is first party more important than the third party?* There was no significant difference between first parties on participants' data sharing willingness. And except for online banking (OB), participants were equally concerned between first and third party tracking.

4.3 Impact of Privacy Attitudes (Q3)

We found that participants' privacy attitudes had significant impact on their willingness to share data. We used the three categories of participants derived from the Westin Index (see Section 3.5.2) for analyzing data in this section.

Table 4 shows all significant differences between Privacy Fundamentalists and other participants (i.e., Privacy Pragmatics and Privacy Unconcerned). Overall Privacy Fundamentalists were less willing to share their demographic data, and their personal identification information and financial information. Each row of this table represents one set of differences. For example, the first row of the table represents a significant difference in overall sharing willingness for demographic information among all participants (Kruskal-Wallis, $N = 386, \chi^2(2) = 18.125, p = 0.001$). Pairwise comparisons using Wilcoxon rank sum test (PW) show that more Privacy Fundamentalists were unwilling (16%) to disclose demographic information than Privacy Pragmatics ($8\%, p = 0.001$) and Privacy Unconcerned ($7\%, p = 0.001$).

4.3.1 Answer to Q3

Q3 asks *Do users' privacy attitudes affect their sharing willingness?* Participants' privacy attitudes significantly affected their data sharing willingness for two out of four overall factors: personal identification, financial and demographic data. In all cases, Privacy Fundamentalists showed the least interest to share any type of information.

4.4 Impact of TPT Features (Q4)

In this section, we explored what privacy control features of TPT might influence participants' willingness to share their data.

4.4.1 Usefulness of TPT

Agarwal et al. [1] mentioned that users were unsatisfied with mechanisms that only control tracking or OBA. Rather, users demanded selective filtering of ad contents. We presented hypothetical tools with specific features (see Table 5), generally matching to TPT and ad blocking tools (ABT) (without specifically mentioning their names), and asked participants to rate these tools with a 5-point Likert Scale (1 = "least useful", 5 = "most useful"). The description for TPT explained that it would control third party tracking on selected topics and hide related targeted ads, but not generic ads. The description for ABT explained that it would block embarrassing or irrelevant ads selected by participants, but would not stop third-party tracking of online activities.

As shown in Figure 5, 55% of participants thought TPT was useful; in comparison, only 37% found the ad blocking tool useful. We asked them which tool they preferred and 72% of participants chose TPT.

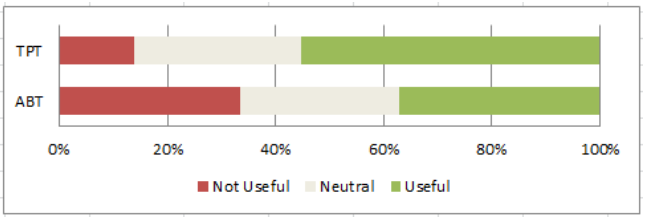

Figure 5: Participants' opinion of TPT and ABT.

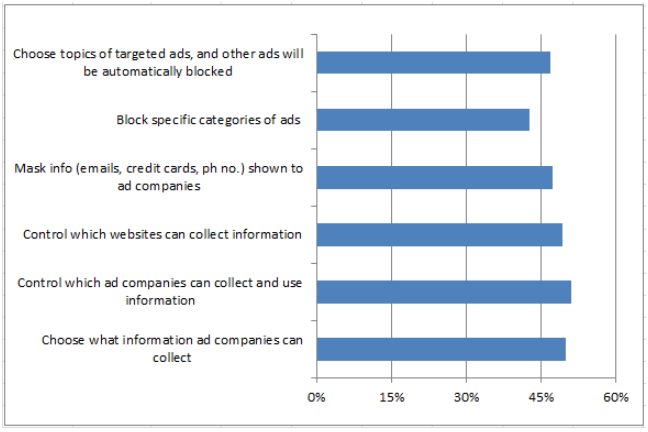

Figure 6: Percentage of participants more willing to share if six control features were provided by privacy tools.

4.4.2 Control Features of TPT

Current privacy protection tools for controlling OBA differ significantly from one another [9]. For example, opt-out tools only block particular advertising networks from showing targeted ads based on users' browsing behavior. The *Do Not Track* browser plugin attempts to block both first or third party cookies by sending a DNT header to visited websites. General blocking tools provide a range of options, including selectively blocking/unblocking groups of ad companies, setting opt-out cookies for ad networks, and installing filter subscriptions maintained by third parties to block websites. In this section, we investigate what features would increase participants' willingness to share information.

We presented six hypothetical control features to participants. Figure 6 shows the control features and the percentage of participants who would be more willing to share if each feature was available. Half of users personally want to control which sites can collect information (regardless of whether they are first or third parties). They also want to control which types of information to share (50%) and want the ability to customize targeted ads (47%). We further analyzed whether Privacy Fundamentalists were more inclined to adopt these tools (TPT/ABT) and found that participants' privacy attitudes had no significant impact on their preference for these tools.

Table 4: Statistical results comparing Fundamentalists (F), Pragmatics (PR) and Unconcerned (U) participants' willingness to share. The % *Unwilling* column represents the percentage of participants from each group who were unwilling to share the specified *Factorized data*. PW=p-value in Wilcoxon rank sum test pairwise comparisons with Bonferroni correction, n.s.=no significant difference. Only factors with significant results are included.

Factorized data	Group	% Unwilling			Kruskal-Wallis			PW	
		F	PR	U	N	χ^2	p	F - PR	F - U
Demographic Information	Overall	16	8	7	368	18.125	0.001	0.001	0.001
	SE	12	12	0	92	8.847	0.01	n.s.	0.01
Personal ID & Financial Information	Overall	55	36	21	368	47.189	0.001	0.001	0.001
	OB	73	32	25	91	8.403	0.01	n.s.	0.01
	OS	52	28	29	94	9.465	0.01	0.01	0.05
	SE	39	42	17	92	17.211	0.001	0.005	0.001
	SN	57	43	13	91	15.745	0.001	n.s.	0.001
Location Information	OB	35	10	21	91	8.999	0.01	0.01	0.05
PC Information	SN	37	21	4	91	6.342	0.05	n.s.	0.05

Table 5: Features offered by TPT and ABT.

Feature	TPT	ABT
Control third party tracking	Yes	No
Hide targeted ads	Yes	No
Hide generic ads	No	No
Block embarrassing ads	No	Yes
Block irrelevant ads	No	Yes
Selection option available	Yes	Yes

4.4.3 Answer to Q4

Q4 asks *What features of TPT influence participants' willingness to share?* Participants clearly distinguished between TPT and ABT, and the majority considered TPT more useful than ABT. Nearly half of participants, across all websites and irrespective of their privacy attitudes, were more willing to share data if they could restrict both first and third parties from collecting data, select types of information to share, and customize topics of targeted ads.

4.5 Other Factors Affecting Willingness to Share

Sharing willingness might depend on many other factors apart from website categories and privacy attitudes. So we conducted post-hoc exploration of a few other options and report the results.

4.5.1 Frequency of Website Visit

Frequency of visiting a particular type of website significantly influenced overall willingness to share for location data (Kruskal-Wallis test: $N = 386, \chi^2(5) = 11.936, p < 0.05$) and personal identification & financial data (Kruskal-Wallis test: $N = 92, \chi^2(5) = 19.559, p = 0.001$). Pairwise comparisons using Wilcoxon tests showed that frequent visitors (daily visits) were more willing (34%) to share location information than infrequent visitors (12%). We also found that frequent visitors of search engines (SE) were less likely to share personal identification information and financial data than who visited SE websites only a few times in the last year.

Many websites, like shopping sites and search engines, provide location-based selection or search facilities for their client services. Frequent Internet users might perceive this as a useful feature and hence be more willing to share these data. However, financial (e.g., credit card number) or personal identification data (e.g., SIN/SSN) are too sensitive and frequent users appear aware of the risk of online exposure, thus oppose disclosure of this information.

4.5.2 Computer Related Background

Participants' computer or IT related background had significant impacts on sharing willingness (IT = technical background, non-IT = with no technical background). Wilcoxon tests revealed that IT participants were significantly more willing to share their personal identification data & financial information ($W = 12367.5, p = 0.001$) and computer related information ($W = 14704, p < 0.05$) than the non-IT users. Study results showed that 42% of non-IT participants refused to share personal identification & financial information compared to 27% of IT participants. Similarly, 13% of non-IT participants refused to share computer related data compared to 5% who had computer related background. We may assume that people with degrees or work experience in computer related fields are more confident in their abilities to handle the risk of information leaking and thus are more willing to share these data.

4.5.3 Intentions to Explore Online Ads

Some of our participants expressed interests in exploring online ads by clicking links on websites. We identified significant impact of this *intent to explore* on participants' concerns for receiving targeted ads (Wilcoxon rank test: $N = 386, W = 8341, p = 0.001$). More users who clicked links to explore online ads (25%) would like to receive targeted ads based on their online activities than users who did not explore ads (17%).

We further found significant impact of this intention on participants' concern for third party tracking (Wilcoxon rank sum test: $N = 386, W = 9462, p < 0.05$). Users who clicked links to explore online ads (52%) knew that they might be at risk and showed increased concern for third party tracking compared to users who did not explore ads (38%). However,

participants' intentions to explore ads did not influence their concern for first party tracking.

4.5.4 Access to Collected Data

We next found that data retention policies had moderate impact on the sharing willingness. We proposed three hypothetical scenarios to participants. One scenario was based on users' access to collected data and two others were based on fee payment by Internet users to control online information tracking.

We asked participants whether they would change their willingness to share if given an option for having access to collected data for reviewing, editing or even permanently deleting from the online platforms. We found that 25% of participants were more willing to share information if they were given this access. They specifically mentioned that they would be in favor of targeted ads based on their online activities if they were in control of selecting what data could be used for generating these ads.

To increase data collection transparency, some companies recently allow users to access and edit their online profiles [8]. Some companies provide users access to their profiles based on browser cookies (e.g., Google [7], Yahoo! Pulse [25] and BlueKai [3]), while others like Microsoft [16] provide users access to information through a privacy dashboard that requires users to create an account with them [20]. 25% of participants felt this option was acceptable and became more willing to share information.

Interestingly, the majority of participants did not change their sharing willingness. Some participants with negative views expressed privacy related concerns such as "*I don't like my private info to be on the Internet, it's just for me*", concerns relating to time costs, "*Who has time for that. I don't want information collected about me, period. I'm supposed to do that for every website I visit? Craziness..*". Some participants did not attribute much value to targeted ads, "*I don't really care if my information are correct or not, if it is for ad purpose*". Many participants would not trust this mechanism, "*They should not collect that information on first place without our consent. Even if I wanted to remove I wouldn't trust them to actually discard my data*".

4.5.5 Fee Payment

We presented two fee payment options (Scenario 1 & 2) to our participants to measure the extent of their interest in controlling online information tracking.

Scenario 1: Their favorite websites would charge a monthly fee in exchange for not showing any ads, but companies might still collect information from users for other purposes.

Scenario 2: This payment method would stop advertising companies from collecting any information about users' online activities on the website but display general ads.

The majority of our participants were unwilling to pay to stop targeted ads (61%) or online tracking (51%). Overall responses for each scenario are shown in Figure 7. This result supports our findings from Section 4.4.1 and also matches with results published in Leon et al. [8].

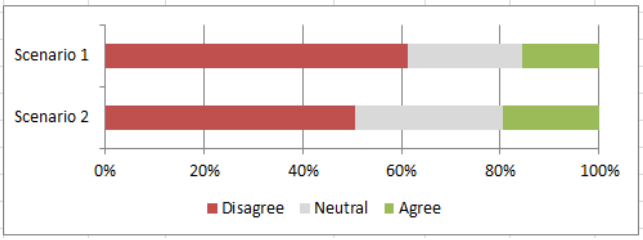

Figure 7: Percentage of participants who are willing to payment for controlling targeted ads and online tracking.

4.6 Summary of Results

To summarize overall results, we list all the factors examined in this study and their relative impact on participants' sharing willingness in Table 6. We identified four factors that greatly influenced participants willingness to share various types of PII and non-PII data: (1) participants' privacy attitudes, (2) frequency of visiting a specific type of website, (3) having technical background, and (4) intention to explore online ads. The choice of first party websites had no impact on participants' data sharing willingness, suggesting that Leon et al.'s findings [8] may be generalizable. Our participants also showed preferences for the types of data they were willing to share online.

Some factors influenced a subset of our participants, such as options that allowed access to participants' user profiles for performing necessary modification, and TPT features to restrict data collection or to select topics for targeted ads.

Table 6: Factors affecting participants' sharing willingness.

Factors	Impact Level	Section
First party websites	None	4.3
Control features of TPT	Moderate	4.5.2
Access to collected data	Moderate	4.6.4
Privacy attitude	High	4.4
Frequency of website visit	High	4.6.1
Computer/IT background	High	4.6.2
Exploring Online ads	High	4.6.3

5. DISCUSSION

Leon et al. [8] investigated the impact of privacy practices using two health-themed first party websites (i.e., a familiar online medical site and a fictitious online medical site) on participants' willingness to share data. They suggested that hidden third party tracking was more important than site familiarity for users' willingness to disclose information online. Other studies demonstrated that participants considered companies' non-OBA related activities when deciding whether to allow data collection [23] and that participants' showed indifference towards third parties when sharing information online [1].

Confirming and extending these prior studies, we investigated users' sharing preferences across different first party website categories (banking sites, shopping sites, search engines and social networking sites) for the purpose of receiving targeted ads. We carefully selected a range of first party sites that would be familiar to users and that would cover scenarios with data of varying sensitivity. We found that the type of first party website had no major impact on participants' willingness to sharing. Furthermore, participants expressed equal concern for both first and third party tracking. However, we confirm that participants' privacy attitudes significantly influenced their sharing willingness. In general, participants with strong concern for privacy were unwilling to disclose personal, financial and demographic data for any type of website. These types of data are considered sensitive by NAI [17] and therefore, should only be collected with users' consent. Consent mechanisms should offer some assurance that opt out preferences are being observed. Other types of data were also of concern to smaller segments of the population; providing opportunity to voice a preference would also be beneficial in these cases.

In line with the results of Leon et al.'s study [8], participant responses clearly showed that some data items can be openly shared for OBA (e.g., 46% of the participants agreed to share hobbies, 55% for country, 54% for gender, and 43% for education), but these are user-specific. Advertising companies can maintain user profiles combining these details with the categories of ads preselected by users. A significant number of our participants were open to targeted ads, as long as they had some control over what information is being collected for their profile.

While a number of studies individually investigated users' concerns towards online behavioral advertising [14,23], users' understanding of tracking prevention tools [9] and preferences for ad blocking tools to control embarrassing ads rather than third party tracking [1], we combined exploration of participants' level of understanding of OBA and TPT, and preferences over the types of tools (TPT and ABT) and their control mechanisms. We also found that participants' having computer related background or a strong preference for online ads were more willing to share information online. Furthermore, sharing willingness of frequent website visitors varied significantly based on website categories. It would be interesting to further investigate the group-wise usage patterns to find what makes them more inclined to share.

As users' agitation about seeing embarrassing online ads had been emphasized by Agarwal et al. [1], we investigated users' preferences for tools specifically to block embarrassing or irrelavant ads. Our study results indicated that most users were more concerned over online tracking than blocking unwanted ad networks or topics. We assume that the definition of embarrassment is sensitive to both geographical location and culture, and users' concerns on this topic needs further investigation.

Current control mechanisms of privacy protection tools are controversial and have poor usability [9, 15]. Our hypothetical TPT features showed increase in participants' sharing willingness (>43%) across all categories of websites. As expected, half of participants prefered features that would provide them control over the types of collectable data as well as over the data collecting entities. The main downside of today's OBA mechanism is that it creates users' profiles based on their browsing histories and not on their actual interests in seeing ads [1]. For example, 47% of our participants would share more data online if they could choose topics for targeted ads. Therefore we suggest a more open privacy-choice mechanism for OBA, which would communicate with users regarding data collection by asking their preferences instead of showing ads that might surprise or annoy them based on users' general profiles. Rather than alienating users through "creepy" OBA practices, companies may be better served in starting a dialog with users and collecting information that users are comfortable revealing.

5.1 Limitations

The main limitation of our study is the data we collected are self-reported values based on participants' views towards OBA and perceived willingness to share personal information in hypothetical scenarios. From our data, we are unable to confirm how well this maps to users' actual behavior. In our recruitment notice, we intentionally avoided explicit mention of privacy, but the study design might have influenced responses nonetheless. These limitations are common with several other related studies available in the literature.

6. CONCLUSIONS

We conducted an online survey using CrowdFlower to investigate whether participants' willingness to share 24 types of personal information with online advertising companies varied depending on the type of first party websites they visited. We also explored users' understanding of online behavioral advertising and tracking prevention tools. Furthermore, we investigated how other aspects, such as participants' privacy attitudes, practices and features of privacy protection tools influenced their sharing willingness. Our work confirms and extends previous work, such as Leon et al.'s study exploring only one type of first party website.

We found that half of participants were well informed about OBA and the majority demonstrated at least some activities to protect their online privacy. However, their overall awareness about tracking prevention was low. Participants expressed clear preferences for which classes of data they were willing to share and these were mostly consistent regardless of which first party site was visited. In fact, the type of first party website had no significant impact on users' decisions. Our results generalize over several types of first-party sites where users would typically disclose data of varying sensitivity. Moreover, participants were similarly worried about first and third party tracking. We confirm significant differences in sharing willingness based on privacy attitudes (Westin Index), with Privacy Fundamentalists being most concerned. Our participants appreciated the idea of user-customized targeted ads and some would be more willing to share if given prior control mechanisms to specify which information can be collected by whom, and what types of targeted ads they wish to see. We recommend active involvement of users in decision-making about OBA and targeted ads.

7. ACKNOWLEDGEMENTS

Sonia Chiasson holds a Canada Research Chair in Human Oriented Computer Security. She acknowledges the Natural Sciences and Engineering Research Council of Canada (NSERC) for funding the Chair and her Discovery Grant.

8. REFERENCES

[1] L. Agarwal, N. Shrivastava, S. Jaiswal, S. Panjwani, Do Not Embarrass: Re-Examining User Concerns for Online Tracking and Advertising, In *Proc. Symposium on Usable Privacy and Security (SOUPS)*, July 24-26, 2013.

[2] N. F. Awad and M. Krishnan. The personalization privacy paradox: An empirical evaluation of information transparency and the willingeness to be profiled online for personalization. In *Management Information Systems Quarterly*, 30(1), 2006.

[3] The BlueKai Registry, `http://bluekai.com/registry/`, Accessed: March 2015.

[4] S. Consolvo, I. E. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. Powledge. Location disclosure to social relations: why, when, & what people want to share. In *Proc. of the SIGCHI Conference on Human Factors in Computing Systems*, pages 81-90. ACM, 2005.

[5] Consumer Action "Do Not Track" Survey Results, `http://www.consumer-action.org/downloads/english/Summary_DNT_survey.pdf`, Accessed: February 2015.

[6] E. Costante, J. den Hartog, and M. Petkovic, On-line trust perception: What really matters. In *Proc. STAST*, 2011.

[7] Google Ads Settings, `https://www.google.com/settings/u/0/ads`, Accessed: March 2015.

[8] P. G. Leon, B. Ur, Y. Wang, M. Sleeper, R. Balebako, R. Shay, L. Bauer, M. Christodorescu, L. F. Cranor, What Matters to Users? Factors that Affect Users' Willingness to Share Information with Online Advertisers, In *Proc. Symposium on Usable Privacy and Security (SOUPS)*, July 24-26, 2013.

[9] P. G. Leon, B. Ur, R. Balebako, L. F. Cranor, R. Shay, Y. Wang, Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising, In *Proc. CHI 2012*, ACM Press, 589-598, 2012.

[10] Kumaraguru and L. F. Cranor. Privacy Indexes: A Survey of Westin's Studies. *Technical report, Carnegie Mellon University CMU-ISRI-5-138*, 2005.

[11] M. Kwasny, K. Caine, W. A. Rogers, and A. D. Fisk. Privacy and technology: Folk definitions and perspectives. In *CHI'08 Extended Abstracts on Human Factors in Computing Systems*, pages 3291-3296. ACM, 2008.

[12] M. Malheiros, S. Preibusch, and M. Sasse. 'fairly truthful': The impact of perceived effort, fairness, relevance, and sensitivity on personal data disclosure. In *Proc. of the 6th International Conference on Trust & Trustworthy Computing (TRUST 2013)*, pages 250-266, 2013.

[13] J. R. Mayer and J. C. Mitchell, Third-party web tracking: Policy and technology. In *IEEE Symposium on Security and Privacy*, 2012.

[14] A. M. McDonald and L. F. Cranor, Americans' Attitudes About Internet Behavioral Advertising Practices. In *Workshop on Privacy in the Electronic Society*, October 4, 2010.

[15] A. McDonald and J. Peha. Track gap: Policy implications of user expectations for the "Do Not Track" internet privacy feature. In *Information Privacy Law eJournal*, 5, 2012.

[16] Microsoft. Microsoft personalized ad preferences. `https://choice.microsoft.com/en-US/opt-out`, Accessed: March 2015.

[17] NAI Code of Conduct 2013, `http://www.networkadvertising.org/2013_Principles.pdf`, Accessed: March 2015.

[18] K. Purcell, J. Brenner, and L. Rainie. Search engine use 2012. In *PewResearchCenter Technical Report*, March 2012.

[19] E. Rader, Awareness of Behavioral Tracking and Information Privacy Concern in Facebook and Google, In *Proc. Symposium on Usable Privacy and Security (SOUPS)*, July 9-11, 2014.

[20] A. Rao, F. Schaub, N. Sadeh, What do they know about me? Contents and Concerns of Online Behavioral Profiles, In *Proc. of ASE International Conference on Privacy, Security, Risk and Trust (PASSAT, 2014)*, December 14-16, 2014.

[21] H. Taylor, Most People are "Privacy Pragmatists" Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits. Harris Interactive, 2003.

[22] J. Turow, J. King, C. J. Hoofnagle, A. Bleakley, and M. Hennessy. Americans reject tailored advertising and three activities that enable it. `http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214`, 2009.

[23] B. Ur, P. G. Leon, L. F. Cranor, R. Shay, Y. Wang, Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising, In *Proc. Symposium On Usable Privacy and Security (SOUPS)*, July 11-13, 2012.

[24] A. Woodruff, V. Pihur, S. Consolvo, L. Schmidt, L. Brandimarte and A. Acquisti, Would a privacy fundamentalist sell their DNA for $1000... if nothing bad happened as a result? The Westin categories, behavioral intentions, and consequences, In *Proc. Symposium on Usable Privacy and Security (SOUPS)*, July 9-11, 2014.

[25] Yahoo Ad Interest Manager. `https://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/details.html`, Accessed: March 2015.

APPENDIX

A. PARTICIPANTS' SHARING WILLINGNESS

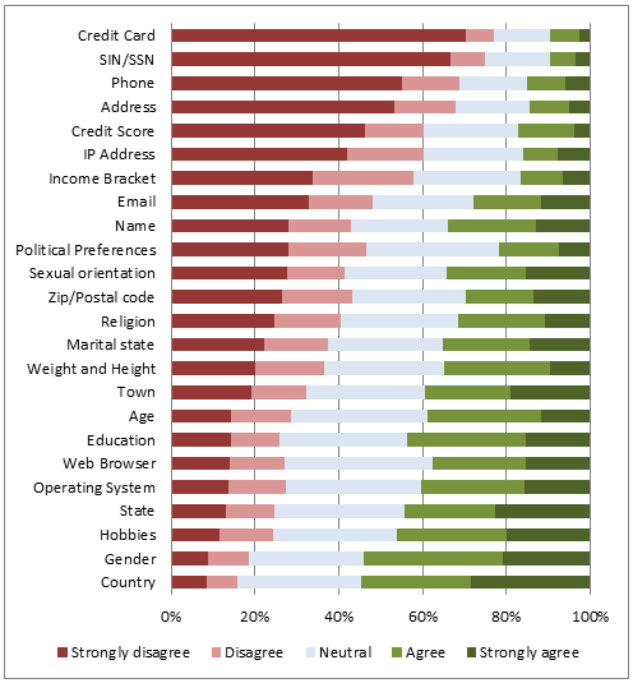

Figure 8: Willingness to disclose information with an online banking website.

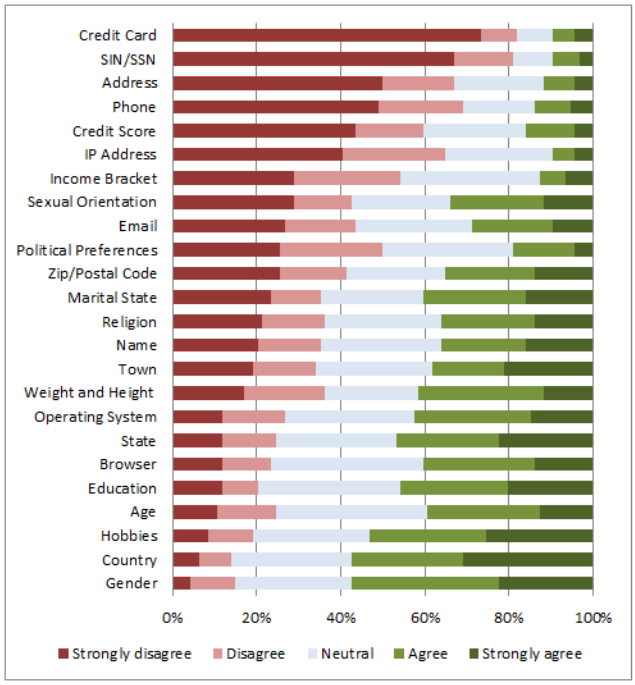

Figure 9: Willingness to disclose information with an online shopping site.

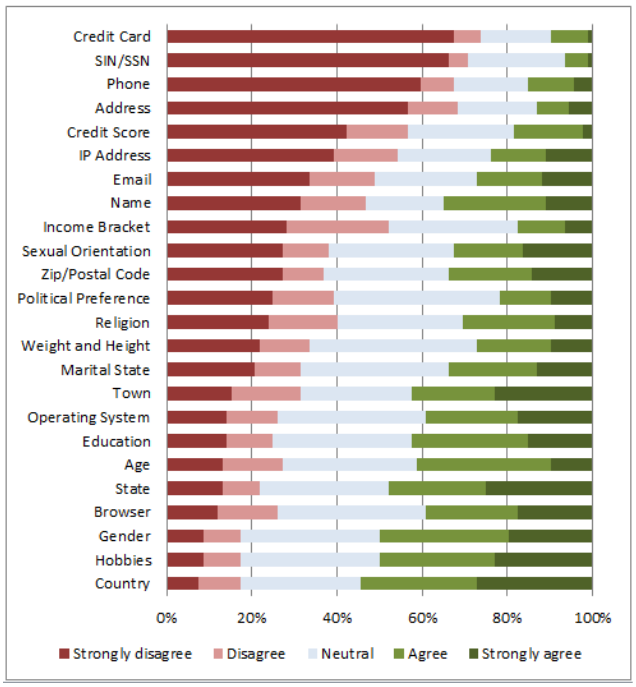

Figure 10: Willingness to disclose information with a search engine.

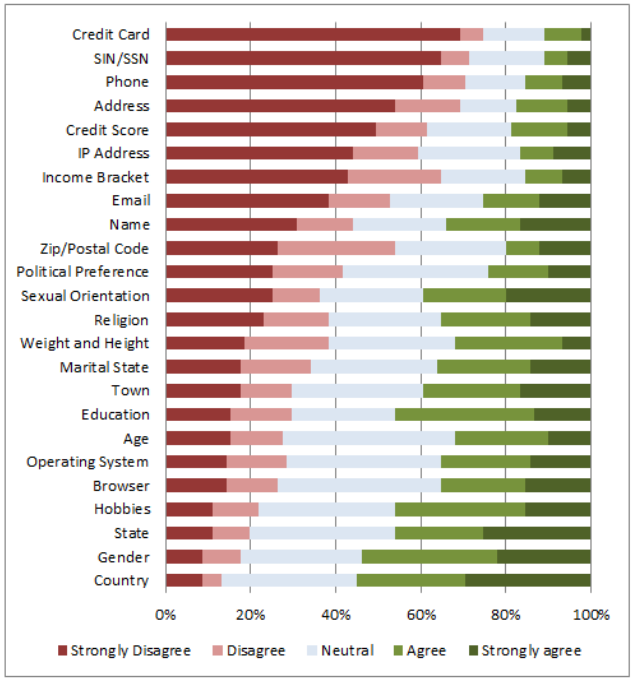

Figure 11: Willingness to disclose information with a social networking site.

B. SURVEY QUESTIONNAIRE

Please think thoroughly before answering each question. Your precise responses are very important for us. You may give an incomplete answer or say you do not know.

Part 1 - Demographic Information
In this part of the questionnaire we collect some demographic information. You can always decline to answer should you feel uncomfortable with a question.

Q1. What is your gender?
( ) Male ( ) Female ( ) Decline to answer

Q2. What is your age (in years)?

Q3. Which of the following best describes your primary occupation?
( ) Administrative support (e.g., secretary, assistant)
( ) Art, writing, or journalism (e.g., author, reporter)
( ) Business, management, or financial (e.g., manager, accountant, banker)
( ) Computer engineer or IT professional (e.g., systems administrator, programmer, IT consultant)
( ) Education (e.g., teacher)
( ) Engineer in other fields (e.g., civil engineer, bio-engineer)
( ) Homemaker
( ) Legal (e.g., lawyer, law clerk)
( ) Medical (e.g., doctor, nurse, dentist)
( ) Scientist (e.g., researcher, professor)
( ) Service (e.g., retail clerks, server)
( ) Skilled labor (e.g., electrician, plumber, carpenter)
( ) Student
( ) Unemployed
( ) Decline to answer

Q4. Which of the following best describes your highest achieved education level?
( ) No high school
( ) Some high school
( ) High school graduate
( ) Some college
( ) Associates/2 year degree
( ) Bachelors/4 year degree
( ) Graduate degree - Masters, PhD, professional, etc.
( ) Decline to answer

Q5. Do you have a college degree or work experience in computer science, software development, web development or similar computer-related fields?
( ) Yes ( ) No

Q6. Approximately how many hours do you spend on the Internet each day?
( ) None ( ) Fewer than 1 ( ) Between 1 and 5 ( ) Between 5 and 9 ( ) Between 9 and 13 ( ) Between 13 and 17 ( ) More than 17

Part 2 - Basic Understanding
We are interested in understanding how you experience things online. We will start with some questions that seek your views about website advertising. Here, "website advertising" refers to ads that are displayed on the web pages that you visit but it excludes pop-up windows or advertising sent over email.

Q7. In your own words, define website advertising.

Q8. In your own words, describe how targeted ads work.

Q9. In your own words, describe how Tracking Prevention tools work.

How much do you agree or disagree with the following statements?
(5 Point Likert-Scale from "Strongly disagree" to "Strongly agree")
Q10. Website advertising is necessary to enjoy free services on the Internet.
Q11. In general, I like website advertising.
Q12. In general, I find that website advertising is useful.
Q13. In general, I find that website advertising is distracting.
Q14. In general, I find website advertising to be relevant to my interests.
Q15. In general, I find that website advertising relevant to my interests can save my time.
Q16. I usually don't look at the ads that appear on the websites that I visit.

Q17. Have you ever clicked on an ad that appeared on a website to get more information about the advertised product? (Yes/No)

How common are the following scenarios?
(5 Point Likert-Scale from "Impossible" to "Very common")

Q18. Companies collect detailed personal information about individuals, such as health conditions, without telling them.
Q19. Online companies collect detailed financial information about individuals, even when they are not purchasing something online.
Q20. Companies track individuals' locations when they are using a mobile phone.
Q21. Online tracking systems cannot follow an individual to all websites he has visited.
Q22. Companies do not track where individuals go and what they do online without their permission.

Part 3 - Willingness to Share
Please read this information carefully, then answer the questions below.

Many websites contract with online advertising companies. The advertising companies pay websites for every ad they show, allowing the websites to provide free services to its visitors. Clicking on the link below will open a new tab or window in your browser displaying a short video explaining how Online Behavioral Advertising (OBA) works. Please watch the video at your own pace and then based only on the information that you have learned from the video choose the correct answer for the following questions.
`http://www.tamingdata.com/2010/10/18/how-advertisers-use-internet-cookies-to-track-your-online-habits/`

Q23. A cookie is ...
(a) a software for browsing Internet
(b) a textfile that contains a ID number to recognize users
(c) your username for a website

Q24. Behavioral targeting ...
(a) tracks visitors' activities using third party cookies from

different websites
(b) does not create profiles for specific visitors
(c) uses information only from the original website visited by a user

Please answer the questions below indicating what information you would allow Advertising Companies to collect for the purpose of showing you targeted ads.

Q25. How often have you visited your favourite [Online Banking Website/Online Shopping site/Search engine/Social network] in the last 12 months?
( ) None ( ) Only once ( ) A few times ( ) A few times per month ( ) A few times per week ( ) A few times per day

Based on the information you know about OBA now, please indicate what information you would allow your [Online Banking Website/Online Shopping site/Search engine/Social network] to collect for the purpose of showing you targeted ads on any website.

(5 Point Likert-Scale from "Strongly disagree" to "Strongly agree")

Q26. My age
Q27. My gender
Q28. My weight and height
Q29. My highest level of education
Q30. My income bracket
Q31. My religion
Q32. My political preferences
Q33. My sexual orientation
Q34. My marital status
Q35. My hobbies
Q36. My credit score bracket
Q37. My country
Q38. My state / province
Q39. My town or city
Q40. My zip code / postal code
Q41. My exact address
Q42. My name
Q43. My email address
Q44. My phone number
Q45. My social security number / social insurance number
Q46. My credit card number
Q47. My computer's operating system
Q48. My computer's IP address
Q49. My web browser

Q50. Will you change your willingness to share if a website allows you to review, edit and delete the information collected about you? For example, you now have the option to confirm that your information and preferences are accurate and remove information that you no longer feel comfortable sharing.

If your favourite [Online Banking Website/Online Shopping site/Search engine/Social network] allows editing of your info, you will be...
( ) less willing to share
( ) equally willing to share
( ) more willing to share

Q51. Please explain the reason(s) for your answer in Q50.

Q52. Suppose your favourite [Online Banking Website/Online Shopping site/Search engine/Social network] offers you the opportunity to pay a monthly fee in exchange for not showing you any ads, but advertising companies may still collect information from you for other purposes. To what extend would you agree to pay? You will pay a fee for your favourite [Online Banking Website/Online Shopping site/Search engine/Social network] to hide ads but still collect your info.

(5 Point Likert-Scale from "Strongly disagree" to "Strongly agree")

Q53. Suppose your favourite [Online Banking Website/Online Shopping site/Search engine/Social network] offers you the opportunity to pay a monthly fee in exchange for stopping advertising companies from collecting any information about you or your online activities on this website, to what extend would you agree to pay? You will pay a fee for your favourite [Online Banking Website/Online Shopping site/Search engine/Social network] to stop collecting your info but display general ads.

(5 Point Likert-Scale from "Strongly disagree" to "Strongly agree")

Q54. How concerned are you for first party tracking (first party tracking means the website you are currently visiting is collecting information about you)?

(5 Point Likert-Scale from "Least concerned" to "Most concerned")

Q55. How concerned are you for third party tracking (third party tracking means a website having some sort of contracts with the first party is collecting information about you)?

(5 Point Likert-Scale from "Least concerned" to "Most concerned")

Q56. What do you consider the main benefit, if any, of receiving ads that are targeted based on your online activities?

Q57. What do you consider the main downside, if any, of receiving ads that are targeted based on your online activities?

Q58. Overall, how do you feel about receiving ads that are targeted based on your online activities?

(5 Point Likert-Scale from "Strongly dislike" to "Strongly like")

Q59. Explain what, if anything, would make you feel more comfortable with receiving targeted ads?

Part 4 - Understanding about Tracking Prevention Tools
Imagine you have two tools that you could install on your browser.

Q60. Tool-A protects you from being tracked online on particular topics. It will control online tracking on the topics

you select and hide related targeted ads. However, it will show generic ads. How useful is this tool?

(5 Point Likert-Scale from "least useful" to "very useful")

Q61. Tool-B blocks ads which you find embarrassing or irrelevant, but it does not stop tracking of your activities. How useful is this tool?

(5 Point Likert-Scale from "least useful" to "very useful")

Q62. If you have to pick only one, which tool would you choose?
a) Tool A
b) Tool B

Please state how much you agree or disagree with the following statements.

(5 Point Likert-Scale from "Strongly disagree" to "Strongly agree")

I would be more willing to share my personal information for the purpose of receiving targeted ads if tracking prevention tools...
Q63. allowed me to choose ahead of time what information advertising companies can learn about me
Q64. allowed me to control which advertising companies can collect and use my information
Q65. allowed me to control on which websites my information can be collected
Q66. allowed me to mask my information (accounts, emails, credit cards, phone numbers) to show to these advertising companies at different points in time
Q67. allowed me to block some specific categories of ad.
Q68. allowed me to choose some topics to see targeted ads, and other ads will be automatically blocked.

Part 5
Please indicate whether you have ever done any of the following. (Yes / No / Decline to answer)

Q69. Refused to give information to a website because you felt it was too personal or unnecessary
Q70. Decided not to use a website or not to purchase something online because you were not sure how your personal information would be used
Q71. Read a website's privacy policy
Q72. Deleted cookies from your web browser
Q73. Activated the "do not track" option in your web browser or installed tracking prevention tools

Do you agree or disagree with the following statements:
Q74. I feel that consumers have lost all control over how personal information is collected and used by companies.
Q75. I feel that most institutions handle consumers' personal information in a proper and confidential way.
Q76. I feel that existing laws and organizational practices provide a reasonable level of protection for consumer privacy.

Q77. Do you have any further comments?