What Matters to Users? Factors that Affect Users' Willingness to Share Information with Online Advertisers

Pedro Giovanni Leon*, Blase Ur*, Yang Wang‡, Manya Sleeper*, Rebecca Balebako*, Richard Shay*, Lujo Bauer*, Mihai Christodorescu†, Lorrie Faith Cranor*

*Carnegie Mellon University
{pedrogln, bur, msleeper, balebako, rshay, lbauer, lorrie}@cmu.edu

†Qualcomm Research Silicon Valley
mihai@qti.qualcomm.com

‡Syracuse University
ywang@syr.edu

ABSTRACT

Much of the debate surrounding online behavioral advertising (OBA) has centered on how to provide users with notice and choice. An important element left unexplored is how advertising companies' privacy practices affect users' attitudes toward data sharing. We present the results of a 2,912-participant online study investigating how facets of privacy practices—data retention, access to collected data, and scope of use—affect users' willingness to allow the collection of behavioral data. We asked participants to visit a health website, explained OBA to them, and outlined policies governing data collection for OBA purposes. These policies varied by condition. We then asked participants about their willingness to permit the collection of 30 types of information. We identified classes of information that most participants would not share, as well as classes that nearly half of participants would share. More restrictive data-retention and scope-of-use policies increased participants' willingness to allow data collection. In contrast, whether the data was collected on a well-known site and whether users could review and modify their data had minimal impact. We discuss public policy implications and improvements to user interfaces to align with users' privacy preferences.

Categories and Subject Descriptors

K.4.1 [**Computers and Society**]: Public Policy Issues—*Privacy*

General Terms

Human Factors, Design

Keywords

Privacy, User Preferences, Online Behavioral Advertising, OBA, Tracking, Data Retention, Do Not Track

Symposium on Usable Privacy and Security (SOUPS) 2013, July 24–26, 2013, Newcastle, UK.

1. INTRODUCTION

Online behavioral advertising (OBA), the practice of targeting online advertising based on users' past online activities, has been the subject of a major privacy debate in recent years. Reports released in 2012 by the U.S. Federal Trade Commission [5] and the White House [36] discuss the privacy tradeoffs inherent in this practice. At the same time, browser vendors have recently taken steps to reduce tracking: Microsoft sends a Do Not Track signal by default in IE 10 [22], and Mozilla has announced that Firefox will eventually block third-party cookies by default [6].

As battles rage about default behaviors and options, average users are asked to make choices about their privacy preferences regarding online behavioral advertising. In some cases, these choices have limited granularity. For instance, with the Do Not Track signal under debate [31], users have the choice of actively turning Do Not Track on or off, or leaving it unset. In many other cases, however, users have a more complex decision to make. As part of the advertising industry's self-regulation program, users can opt out of behavioral advertising from individual companies [25]. Similarly, third-party privacy tools like Abine's DoNotTrackMe[1] and Evidon's Ghostery[2] enable users to see which companies are tracking their activities on a particular site, and to block particular companies. In past work, researchers have found that familiarity with a third-party tracking company influences users' attitudes about data collection [34].

Unfortunately, little is known about other factors that may influence users' preferences. For instance, does the length of time behavioral data is retained actually matter to most users? Does it make a difference whether data is used to target advertisements only on a single first-party website, or on Facebook, or on any website on the Internet? This understanding is crucial for the design of future OBA privacy tools. For instance, when a privacy tool asks the user to decide whether to permit or block the collection of data by a particular entity, the tool could highlight that entity's privacy practices that most strongly affect users' decisions. Better understanding the drivers of user behavior might also influence public policy. For instance, laws and regulations designed to support consumer privacy could focus on practices that most affect users' comfort with data collection and sharing, rather than focusing on distinctions that have little bearing on users' preferences.

[1] https://www.abine.com
[2] http://www.ghostery.com

In this paper, we examine how four dimensions of privacy practices impact users' willingness to permit the collection of data for OBA. These dimensions are the length of time data will be retained, whether or not a user will have access to review and modify this data, the range of websites on which advertising will be targeted based on this data, and whether the data was collected on a well-known website.

To this end, we conducted a 2,912-participant online survey. We asked participants to visit a health website. After they explored this page, we explained the value proposition of online behavioral advertising: that advertising and the collection of data for targeted ads enable websites to be free. We then showed the participant this website's data-collection practices, with details varied based on the participant's condition. In different conditions, participants were told that data would be retained for one day or indefinitely; they were told or not told that they would be provided access to review and modify collected data; participants were told that data would be used for targeted advertising only on the health site, on both the health site and Facebook, or on any website; and the health site itself was either well known or a site we invented. We then asked participants to rate their willingness to allow the collection of 30 different types of information, and to answer additional questions related to their OBA preferences.

Nearly half of our participants were unwilling to allow the collection of any data, while the site's privacy practices impacted the remaining participants' attitudes. Of the four dimensions we examined, the scope of use and the period of data retention had the greatest impact on participants' willingness to allow their information to be collected. Having access to view and modify data collected, as well as participants' familiarity with the website on which data was being collected, did not appear to affect their willingness to allow data collection, at least in the narrow scenario we investigated. Furthermore, the majority of participants were not willing to pay any money to prevent data collection or remove advertising, believing websites should be free.

We provide background on the debate surrounding online behavioral advertising and highlight related work in Section 2. In Section 3, we describe our methodology. We present our results in Section 4, beginning with our factor analysis and proceeding through the four dimensions of privacy practices we investigated. We discuss our results in Section 5 before concluding in Section 6.

2. BACKGROUND AND RELATED WORK

In OBA, third-party advertisers track users as they browse websites. The purpose of this tracking is to build profiles of users in order to target ads. Tracking can be performed using third-party cookies or more complex techniques [19].

Third-party tracking for OBA is widespread. In 2011, third-party trackers were present on 79% of pages examined among the Alexa top 500 websites [27]. Among a set of selected U.S. and Canadian health websites, 85% contained at least one tracker [3]. In a study performed from 2005 to 2008, Krishnamurthy and Wills found the number of third-party trackers was growing, while the number of companies controlling the collected information was shrinking [14].

Online social networks also track user data and leak data in potentially privacy-invasive ways. In a study of twelve online social networks, Krishamurthy and Wills found that the sites tended to leak unique identifiers to third parties, allowing users to be linked to one or more social networking profiles. They also found that some websites directly leaked personally identifiable information [15]. Roosendaal found that Facebook tracked both users and non-users of Facebook across the Internet using cookies attached to "Like" buttons embedded in other pages [28].

This large data footprint leads to privacy concerns. Retailers can combine credit or debit card histories with data from online tracking to create detailed customer profiles revealing potentially sensitive "lifestyle or medical issue[s]" [9]. Even when data is collected in an aggregated, ostensibly anonymized manner, bulk collection leaves the potential for re-identification [7, 24].

Users tend to dislike the idea of being tracked and profiled by third parties [8]. Based on 48 semi-structured interviews, Ur et al. found that participants recognized both pros and cons of OBA, pointing out that OBA can be useful to both users and companies, yet also privacy-invasive. Participants did not understand how ads were targeted and believed companies collected more information than they generally collect [34]. Respondents to a 2011 survey conducted by McDonald and Peha also believed that websites could collect more data than is currently accessible [21]. Wills and Zelijkovic created a JavaScript tool to show a user's location, age range and gender, all of which could be determined by third-party sites. Approximately half of their 1,800 participants were concerned about third-party tracking, the level of data collection, and the ability of third-party data trackers to infer demographic information after seeing these data [38].

OBA is currently self-regulated under guidelines created by the advertising industry. These guidelines require that users be provided the option to opt out of targeted ads [25], but do not mandate options for fine-grained control [19]. Under current guidelines, users are notified of the presence of behavioral advertising through an AdChoices icon that appears near or inside the ad. However, Leon et al. found that most users did not understand the purpose of this icon [17].

Users are currently able to limit online behavioral advertising in several ways. By clicking on the AdChoices icon, users can visit an opt-out page that allows them to opt out of ad networks individually. Alternatively, they can use third-party tools that block tracking, or even block ads entirely. However, there are problems with all of these opt-out mechanisms. For instance, Komanduri et al. found many gaps in advertising networks' compliance with industry opt-out requirements [12], while Leon et al. found serious usability issues with all nine privacy tools they tested, including tools provided by industry coalitions and by third parties [16]. Users could instead follow links to natural-language privacy policies and evaluate hundreds of companies, but the opportunity cost of doing so would be prohibitive [20].

Another option for opting out of OBA is the "Do Not Track" initiative. In most modern web browsers, users can set a "Do Not Track" (DNT) signal to be sent to third-party advertising servers. This option is generally easy for users to set, though it lacks the fine-grained control needed to set preferences on a per-advertiser basis [31]. However, there is not yet a general consensus on the meaning of DNT or how advertisers should respond to the DNT signal. Further, users do not have a good idea of what the DNT button in their browser will actually do [21]. Despite these issues, 12 percent of desktop users and 14 percent of Android users have enabled DNT in Firefox [30].

There have been indications that users may be more comfortable sharing their data if provided with more granular choice or better control over their data sharing. Gomez et al. found that a large percentage of complaints submitted to the FTC from 2004 through 2008 were related to a lack of user control [8]. Users' willingness to share data tends to depend on context and the type of data being requested. Broadly, reputation and brand name have been found to influence user trust of websites [4].

Although factors influencing OBA decision-making have not been well studied, a handful of researchers have examined factors that impact information sharing more broadly. In a 1998 study of 401 participants, Awad and Krishnan found that users who valued information transparency were more concerned about being profiled online than those who did not [2]. Across two studies, Acquisti et al. found that the context of an information request affected users' willingness to share information. If more sensitive information was requested prior to less sensitive information, participants were more likely to reveal more information overall [1]. Taylor et al. found that general online trust made users less concerned about privacy [33]. Joinson et al. asked distance-learning students to sign up for a panel that requested a variety of sensitive personal information. They found that participants were least willing to share financial information [10].

Two studies have examined information sharing with online music sites. When asked to provide information to a mock online music retailer, Metzger found that participants were more likely to disclose information if they saw a strong privacy policy than if they saw a weak privacy policy. She also found that participants were most likely to be willing to provide information necessary for a retail transaction, specifically name and address, as well as basic demographic information. Participants were least likely to be willing to provide financial information [23]. In a study of how participants felt about revealing information to a music recommender system, van de Garde-Perik et al. found that some participants wanted to reveal information anonymously because of privacy concerns, while other participants were willing to reveal information tied to their identities to help improve the system. In both cases, the researchers found that participants wanted to know how the data would be used and who would have access to it [35].

In this paper, we examine which types of data users are more willing or less willing to allow websites to collect for OBA purposes based on different factors, including familiarity with the site, the length of time for which data will be retained, and the scope in which that data will be used.

3. METHODOLOGY

We conducted a between-subjects online study to investigate how online advertising companies' privacy practices impact users' willingness to allow the collection of information for OBA. Participants completed an online survey in which they were asked to visit a health website, were given notice about privacy practices that governed data collection for OBA on the site they visited, and answered a series of questions about their willingness to allow different types of personal information to be collected. Each participant was assigned to a condition that specified the exact privacy practices that would be presented to him or her. Participants answered additional questions investigating their attitudes toward OBA and online privacy.

In this section, we discuss participant recruitment, the conditions to which participants were assigned, and the design of the survey. We then provide an overview of our analysis methods.

3.1 Recruitment

We recruited our participants using Amazon's Mechanical Turk crowdsourcing service.[3] Recruitment materials indicated that the study would be about how individuals experience the Internet. They provided no indication that either OBA or privacy would be major components of the study. We required that participants live in the United States and be age 18 or over. All participants who completed the study were paid $1.00, which is typical for a task on Mechanical Turk that takes approximately twenty minutes to complete. The Carnegie Mellon University IRB approved our protocol.

3.2 Conditions

We assigned participants round-robin to a condition. This condition specified the privacy practices participants were told governed OBA on the website they visited. Our study's design was full-factorial across three dimensions of privacy practices. For our first dimension, we investigated three types of scope of use and sharing policies. Our second dimension varied the period for which the data collected would be retained. Finally, the third dimension investigated the impact of providing users the ability to review and modify data collected about their behavior. As our investigation was primarily exploratory, we considered only extremes; for example, data would be retained for a day or indefinitely. If diametrically opposed policies do not impact participants' attitudes, it is unlikely that gradations of these policies would.

Each participant's condition specified one of the following levels for each of these three dimensions:

- **Scope of use** (3 levels). Participants assigned the first treatment level were told that the XYZ Advertising Company would collect behavioral data only on the health website they were visiting, and that collected data would be used only to target advertisements on that website. Participants assigned the second level were told that the XYZ Advertising Company would collect behavioral data on any website on the Internet, and this data would be used for targeting ads on any website on the Internet. Those assigned the third level were told that Facebook, acting as the ad network, would collect and use data for targeting advertisements on both the health website and Facebook.

- **Data retention period** (2 levels). Participants were told either that all data collected for online behavioral advertising purposes would be retained for *one day*, or that the data would be retained *indefinitely*.

- **Level of access** (2 levels). Participants were either told the advertising company would provide "access to a webpage where you can review, edit, and delete the information that is being collected about you," or told nothing regarding data access.

We also investigated whether participants' familiarity with the health website they visited as part of the study, and on which behavioral data would be collected, would impact

[3] `https://www.mturk.com`

their willingness to allow data collection. As this investigation of familiarity with the first-party site was a secondary goal of the study, we did not include it in our full-factorial design. We assigned participants one of two levels for familiarity: Participants either visited WebMD, which is a popular health website; or they visited WebDR, a clone of WebMD that we invented and with which participants would presumably be unfamiliar.

3.3 Survey Flow

After reviewing and agreeing to a consent form, participants answered general questions about their impression of advertising on the Internet, exploring whether it was useful, relevant, or distracting. In order to gain a better understanding of our participants, we then asked them to answer demographic questions, as well as general questions about their use of the Internet and social networks.

In order to simulate the experience of visiting a website more closely, we instructed participants to follow a link in the survey to visit either the WebMD or WebDR website, depending on their condition. To eliminate variability caused by pages changing over time, we hosted an exact copy of the WebMD homepage as of February 5th, 2013. We disabled all hyperlinks and forms on the page so that participants would concentrate on the homepage, yet retained all other functionality on the page, such as interactive dropdown menus and scrolling news stories. The WebDR homepage was identical to WebMD's, except that all branding and logos had been changed to read "WebDR." In order to verify that participants examined the site, we asked them to identify three health conditions discussed on the site's homepage. To gauge whether WebMD was actually a familiar brand to participants, while WebDR was not, we asked questions about participants' history of visiting either WebMD or WebDR, as well as their impressions of the site's reputation and trustworthiness.

We next presented participants with a description of OBA, along with its value proposition. We explained that websites "are able to offer free services to their visitors by contracting with online advertising companies. The advertising companies pay websites for every ad they show, allowing the websites to provide free services for users like you."

Participants were told to imagine they were "experiencing a flaky scalp condition" and therefore visiting a health website. We explained that an advertising company contracting with the health site "collects information about your interactions with the {WebMD | WebDR} website in order to predict your preferences and to show you ads that are most likely to be of interest to you. These ads are known as targeted ads." Following this description, we presented participants with the details of the privacy practices governing online behavioral advertising according to their condition. They were immediately asked questions testing their comprehension of the privacy practices specified (e.g., "Based on the information that you just read, for how long may *company* use the information collected about you?"). Data from participants who answered any of these comprehension questions incorrectly were removed from our analysis.

We next asked participants to "answer the questions below indicating what information you would allow {XYZ Advertising Company | Facebook} to collect for the purpose of showing you targeted ads on {the WebMD website | the WebMD website and other websites that you visit | your Facebook page and the WebMD website}." We then asked about the 30 items of *personal information* shown in Table 3 in the appendix. To facilitate participant comprehension, we organized these 30 data items into five categories: computer-related information, demographic and preference information, interactions with the website, location information, and personally identifiable information (PII), which we referred to only as "information" in the survey. For each item, participants rated their agreement with the statement "I would be willing to allow *company* to use and store the following information related to my interactions with the *name* website" on a five-point Likert scale ("Strongly Disagree" to "Strongly Agree"). The data collected during this part of the study are used for the bulk of our analyses.

We then asked a number of additional questions related to privacy and online behavioral advertising. For instance, we asked participants about their willingness to share for different data-retention periods, whether participants might be willing to pay money for stopping data collection or advertising, and how they felt about online behavioral advertising on a number of different types of websites. We also presented participants with six features a hypothetical browser plugin might have that could help users understand or control data collection. We also asked whether the presence of each feature would increase their willingness to allow advertisers to collect their personal information. The final page of the survey asked participants about their general privacy attitudes and whether they had taken privacy steps, such as opting out of OBA or enabling Do Not Track in their web browser.

3.4 Analysis

We were interested in understanding how the practices participants were told governed data collection impacted their willingness to share the 30 types of information we asked about. As shown in Table 3 in the appendix, we examined both sensitive and non-sensitive information. The Network Advertising Initiative (NAI) requires opt in or "robust notice" for some, but not all, of the sensitive items we studied [25]. To reduce these 30 types of information to a smaller number of output variables, we performed exploratory factor analysis. Factor analysis reveals underlying associations by evaluating which variables are closely related, combining variables that are highly correlated into a single latent factor. If such underlying factors are observed, further analysis considers these factors in place of the individual variables.

We performed exploratory factor analyses and found that 22 data types were grouped into five factors, while 8 data types did not conform to any particular factor. These five groups closely mirrored the categories from our original survey. We used the standard procedure of considering a factor part of a group 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. In Section 4.1, we discuss the results of this process, including which types of information were grouped or excluded. We further verified our groupings by calculating Cronbach's alpha for each group, using the standard value of 0.8 or higher to indicate good reliability.

Our further analyses focus on these five resultant factors. We created an index variable for each of the five factors by averaging participants' responses to the question items included in each factor. Using the participant's treatment for each dimension of privacy policy as independent variables and the five factors' indices as dependent variables, we

performed a multivariate multiple regression, evaluating the effect of multiple independent variables on multiple dependent variables. Our model considered covariates including age, gender, and privacy attitudes, as well as interactions between independent variables. We confirmed our results by running repeated measures ANCOVA and MANOVA, which yielded similar results. For all statistical tests, $\alpha = 0.05$.

4. RESULTS

We analyzed responses from 2,912 participants between the ages of 18 and 74 (mean = 31, σ = 11.1). Around half of our participants were unwilling to disclose any personal information in exchange for targeted ads. The remaining participants were willing to disclose their gender, low-granularity location, operating system, and web pages they had visited at a higher rate than other types of personal information. We found the type of information collected, the scope of use of the information, and the retention period impacted participants' willingness to disclose information.

We first describe the results of our exploratory factor analysis that used participants' responses to group different types of information (Section 4.1). We then identify which factors affected participants' willingness to disclose different types of information (Section 4.2). In Section 4.3, we discuss participants' attitudes toward targeted ads in different first-party browsing contexts. We then discuss our qualitative results investigating participants' willingness to pay to remove ads and stop data collection (Section 4.4). Finally, in Section 4.5, we discuss the impact of mechanisms for controlling data collection on participants' disclosure preferences.

Participant demographics are summarized in Table 1. We did not observe any statistical differences in the education, technical background, gender, age, or Internet-usage patterns of participants assigned to different conditions.

Demographic	Number	Percent
Gender		
Female	1,375	47%
Male	1,537	53%
IT Background		
Yes	695	24%
No	2,217	76%
Internet Usage (hours/day)		
<1	72	3%
1–5	1,144	39%
5–9	975	34%
9–13	519	18%
13–17	135	5%
>17	67	2%
Occupation		
Administrative support	183	6%
Art, writing, or journalism	178	6%
Business, management, or finance	205	7%
Computer engineering	299	10%
Education (e.g., teacher)	184	6%
Engineering	48	2%
Homemaker	176	6%
Legal	43	2%
Medical	102	4%
Retired	44	2%
Scientist	80	3%
Service (e.g., retail clerks)	177	6%
Skilled labor	77	3%
Student	624	21%
Unemployed	253	9%
Other	212	7%
Decline to answer	27	1%
Education		
Some high school	46	2%
High school degree	243	8%
Some college	987	34%
Associate's degree	266	9%
Bachelor's degree	1,038	36%
Graduate degree	331	11%

Table 1: Demographics of our 2,912 participants.

4.1 Factor Analysis

Our exploratory factor analysis created five groups that included 22 of the 30 types of information. Table 2 lists these groups by the names we gave them, as well as the types of information in each group. We provide greater detail about the factor loadings for each type of information, as well as how we created these groups, in Appendix A.

Throughout the remainder of this paper, we refer to these five groups by name: *browsing* information, *computer* information, *demographic* information, *location* information, and *personally identifiable* information. The remaining 8 types of information were not associated with any of the five groups and are excluded from our regression.

To verify that the types of information in each group were highly correlated, we calculated Cronbach's Alpha for each group. Our results for this correlation analysis supported the groups from factor analysis. Alpha values of 0.8 or higher are considered to be correlated, and our five groups had overall alpha values ranging from 0.81 to 0.94.

4.2 Willingness to Disclose Information

Nearly half of our participants were not willing to disclose information for the purpose of receiving targeted ads. The remaining participants distinguished between the types of information they would disclose, as shown in Figure 1. For instance, 45% of participants were willing to disclose the operating system they used, while under 1% were willing to disclose their Social Security number or credit card number.

The data-retention period and scope of use significantly impacted participants' willingness to disclose the types of information for which participants had varied responses. Providing the opportunity to access and edit information that had been collected, as well as familiarity with the website on which data was collected, had minimal impact. A participant's level of privacy concern, frequency of Facebook usage, age, and positive opinions about targeted ads also impacted their willingness to disclose information.

4.2.1 Impact of Type of Information

Participants were willing to disclose different types of information at vastly different rates. Unsurprisingly, most participants strongly objected to the collection of personally identifiable information (PII), and these attitudes did not vary significantly by condition. For example, across all treatments, under 3% of participants would disclose their phone number. On the other extreme, participants were most willing to disclose arguably innocuous information, such as their country (53%) and gender (46%). Between these two extremes were types of information for which users' willingness to disclose was affected by the scope of use of the information, and for how long it would be retained.

Browsing information ($\alpha = 0.92$)
Medications taken (inferred from browsing)
Pages visited
Search terms entered
Survey responses
Time spent on each page
Computer information ($\alpha = 0.93$)
Operating system
Web browser version
Demographic information ($\alpha = 0.94$)
Age
Gender
Highest level of education
Hobbies
Income bracket
Marital status
Political views
Religion
Sexual orientation
Location information ($\alpha = 0.91$)
Country
State
Town/City
ZIP code
Personally identifiable information ($\alpha = 0.81$)
Email address
Name

Table 2: The five factor groups that resulted from factor analysis, comprising 22 of the 30 types of information from the survey.

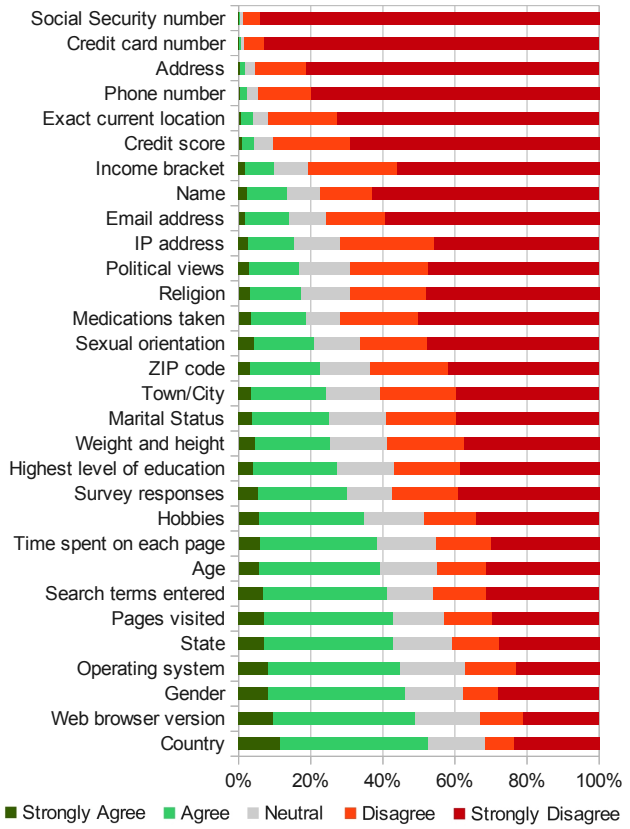

Figure 1: Participants' responses to the statement, "I would be willing to allow *advertising company* to use and store" 30 different types of information. The two shades of green represent willingness to share, while the two shades of red indicate unwillingness to do so.

Figure 1 summarizes participants' responses across all conditions to the 30 different types of information in our survey. While participants' willingness to disclose many types of information differed significantly by condition, participants had relatively homogeneous answers for the most and least sensitive types of information. Very few participants were willing to disclose sensitive information. For instance, only a handful of participants were willing to disclose their SSN (<1%), credit card number (<1%), address (2%), phone number (3%), exact current location (4%), and credit score (5%). We did not observe significant differences across conditions for these types of information. Participants' unwillingness to disclose these types of information is particularly notable in light of Krishnamurthy et al.'s finding that a majority of popular websites actually leak some types of sensitive information to advertising companies [13].

In contrast, nearly half of our participants were willing to disclose less sensitive information. Many participants were willing to disclose their web browser version (43%), operating system (45%), and gender (46%). Participants were similarly willing to disclose coarse-grained information about their location, such as the state (43%) and country (53%) from which they were visiting the health website. These results also did not vary significantly by condition.

4.2.2 *Impact of Retention Period*

The data-retention period significantly impacted participants' willingness to disclose various types of information for three of the five groups of information, as shown in Figure 2. In particular, participants who were told that data would be retained only for one day were significantly more willing to disclose browsing information ($p < .001$), demographic information ($p = .025$), and location information ($p = .001$) than those told data would be retained indefinitely. We did not observe significant differences for computer information or personally identifiable information.

We next asked participants, "How would your willingness to allow {XYZ Advertising Company / Facebook} to collect your information change if it retained your information" for periods ranging from the duration of a browsing session to indefinitely. These results, shown in Figure 3, further suggest that the data-retention period impacts preferences. In particular, 39% of participants in the one-day treatment and 56% of participants in the indefinite treatment indicated that they would be more willing to disclose if their information were retained for the duration of their browsing session. On the other hand, participants were considerably less likely to disclose information for periods greater than one week. Further research is needed to determine whether a data-retention period longer than the duration of a browsing session would align with Internet users' preferences.

4.2.3 *Impact of Scope of Use*

How collected information would be used outside the first-party site also impacted participants' willingness to disclose information, as shown in Figure 4. Based on their condition, participants were told that XYZ Advertising would collect and use their data only on the health website, that XYZ

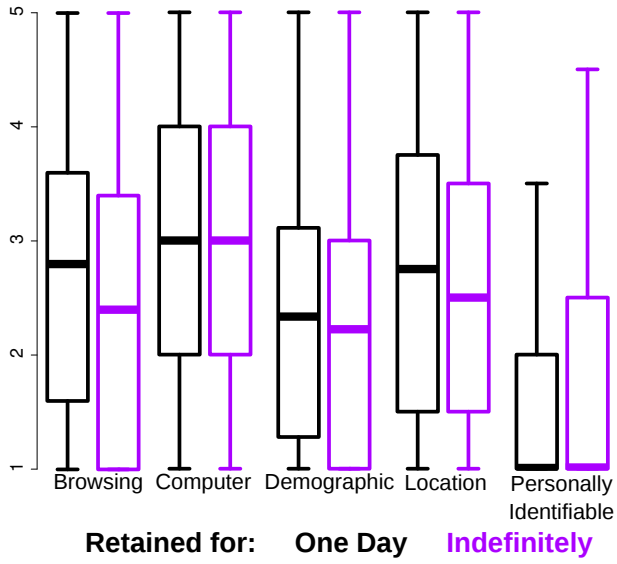

Figure 2: A comparison of participants' willingness to share the five groups of information given different retention policies. The y axis represents participants' willingness to share (5=strongly agree, 1=strongly disagree), averaged over all types of information in that group. Differences between the one-day and indefinite treatments are significant for browsing, demographic, and location information.

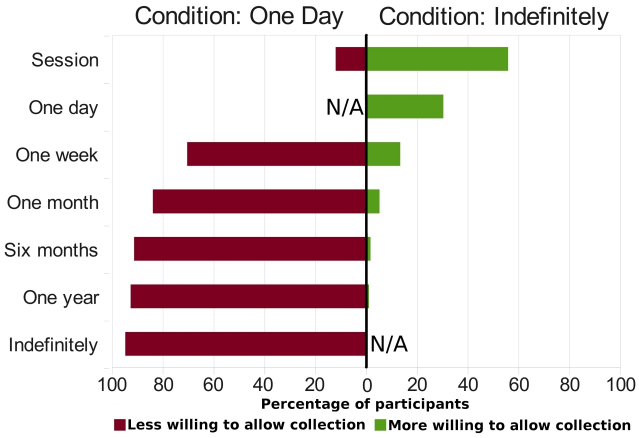

Figure 3: The percentage of participants originally told that data would be retained for one day who would be less willing to allow data collection for different retention periods, as well as the percentage originally told data would be retained indefinitely who would be more willing for different periods.

Advertising would collect and use their data on any website on the Internet, or that Facebook would collect and use their data on both the health website and Facebook.

Participants in the Facebook treatment were significantly less willing to disclose browsing information ($p < .001$) and location information ($p < .001$), than participants told that XYZ Advertising would collect and use their information only on the health website. In contrast, participants in the Facebook scenario were significantly more willing to disclose personally identifiable information ($p < .001$). As users share personal information on Facebook, this result might be explained by the contextual nature of privacy [26].

In addition, participants told that XYZ Advertising would collect and use their information on any website on the Internet were significantly less willing to disclose browsing information ($p < .001$) than participants told that information would only be collected and used on the health website. We did not observe significant differences across conditions for computer or demographic information.

4.2.4 *Impact of Access to Collected Data*

Access to the collected information had a more moderate impact than data-retention and scope-of-use policies. In particular, we did not observe significant differences between participants told they could review and edit the information collected and those not told about this opportunity for any of the five groups of information.

A number of factors might explain this lack of an effect. The concept of "access" to data collected by third parties (e.g., advertising networks) might have sounded strange or vague to participants. Additionally, reviewing and editing collected information represents a cost that may outweigh the expected benefit. The concept of "access" was also abstract in that we did not specify what participants might find on the hypothetical page where they could review the data that had been collected.

Later in the survey, we also asked questions about access to participants whose condition dictated they not be told originally about having access to the information collected. In particular, we asked these participants whether they would be more or less willing to share information if they were able to view and edit it after it was collected. Of these participants, 48% responded they would be more willing to disclose information if given access, 41% responded they would be equally willing, and 11% responded they would be less willing. Companies including Google, Microsoft, and Yahoo! currently provide users access to information through privacy dashboards. Nevertheless, very little is known about how people use these dashboards. More research is needed to understand at a deeper level how access impacts users' privacy decision making.

4.2.5 *Impact of Site Familiarity*

Our manipulation for site familiarity, having participants visit either the real WebMD or fictional WebDR, appeared to work as intended. While 81% of participants who visited WebMD felt the website was trustworthy, only 62% of those who visited WebDR felt the same ($p < 0.001$, χ^2). Similarly, 73% of participants who visited WebMD said they were familiar with the website, compared with 20% of those who visited WebDR ($p < 0.001$, χ^2), and 82% of participants believed that WebMD had a good reputation, compared with 39% of WebDR visitors ($p < 0.001$, χ^2).

However, whether the participant visited WebMD or WebDR did not significantly affect the participant's willingness to disclose information. This result suggests that participants' opinions were mostly based on the third party collecting the data, rather than the first-party site. Although we must be careful about extrapolating this result, participants' willingness to disclose information in other first-party contexts may not be drastically different.

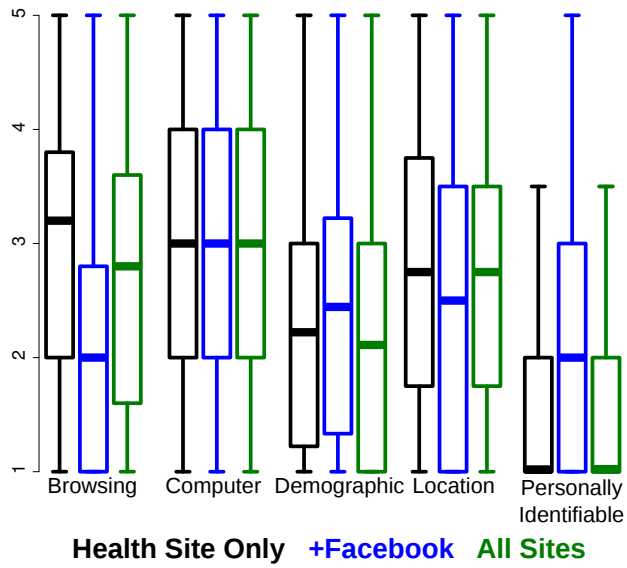

Figure 4: A comparison of participants' willingness to share the five groups of information given different scope-of-use policies. The y axis represents participants' willingness to share (5=strongly agree, 1=strongly disagree), averaged over all types of information in that group. Differences between the health-site and Facebook treatments are significant for browsing, location, and personally identifiable information. Differences between the health-site and all-site treatments are significant for browsing information.

4.2.6 *Other Factors Impacting Disclosure*

We found that aspects other than the website's privacy practices and type of information collected also impacted participants' willingness to disclose information. Participants with higher privacy concerns, identified through survey questions about privacy attitudes (Question 46 in Appendix C), were less willing to disclose all five types of information (all $p < .001$). In contrast, participants who expressed positive opinions toward targeted ads were significantly more willing to do so for all five groups of information (all $p < .001$). Participants who used Facebook more often were also more willing to share all five groups of information (all $p < .001$).

For certain types of information, we observed other significant covariates. Older participants were less willing to share demographic information ($p = .026$) and more willing to share location information ($p < .001$). A participant's stated background in technology, such as holding a degree or job in IT, was a significant covariate for demographic information ($p = .021$). We also observed a significant interaction effect between the Facebook scope-of-use scenario and indefinite data retention for browsing information ($p < .001$), demographic information ($p = .045$), and personally identifiable information ($p = .043$).

4.3 Site Context

As privacy attitudes depend on context [26], we also investigated how participants would feel about the type of website (e.g., banking website, travel website) on which data was collected. In particular, for nine categories of sites, we asked participants to rate on a five-point Likert scale their agreement or disagreement with the statement, "I am interested in receiving targeted ads on the websites that I visit based on my online activities on *category* sites."

Participants' willingness to have data collected and used for OBA purposes differed across the category of site. Figure 5 presents detailed results. More than half of our participants would not be willing to permit data collection on any of the nine categories of sites we presented. Participants were most willing to allow data collection on arts and entertainment websites (40% of participants), travel websites (34%), and news websites (32%). Only around 8% of participants would be willing to have their actions on dating or online banking sites used for targeting ads, and only 15% of participants felt the same for photo-sharing websites.

Although health information has been classified as sensitive by both the advertising industry [25] and government regulators [36], 25% of participants were willing to have data from health sites used for OBA purposes. On the one hand, this result might reflect bias in that participants had just answered questions about the collection of personal information on a health website. On the other hand, since a health website formed the basis for the scenario in our study, this result might suggest a baseline for how participants' willingness might have been different had the scenario taken place on another type of website.

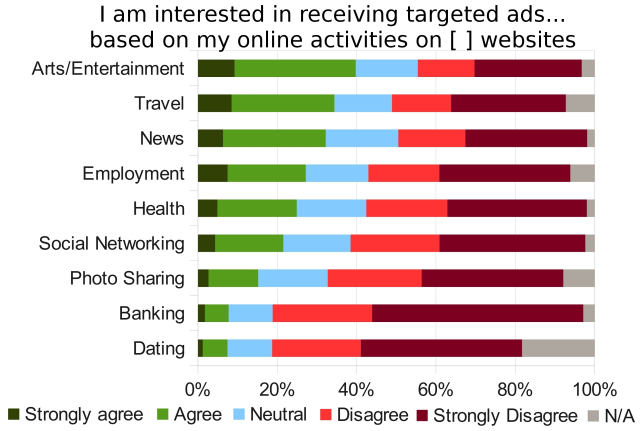

Figure 5: Participants' interest in having their behaviors on different types of websites used to target ads. Participants who said they do not use that type of site are listed as "N/A."

4.4 Willingness to Pay

A user's willingness to pay for a feature can be used as a proxy for how much the user values that feature. We asked three questions about participants' willingness to pay a monthly fee for different advertising and data-collection scenarios. These scenarios were "not showing you any ads," "not showing you targeted ads, but only generic ads," and "stopping collection of any information about you or your online activities." Items 29, 31, and 33 in Appendix C show the specific questions that we asked.

We found that the majority of participants were not willing to pay anything for these changes. Across all conditions, 62% of participants would not pay to stop data collection,

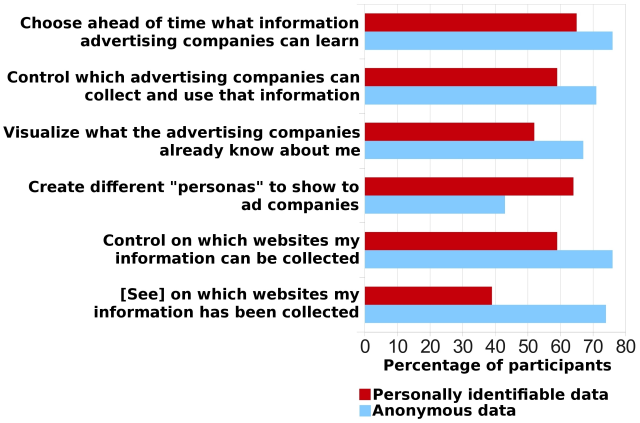

Figure 6: Percentage of users who would be "more willing to allow collection of {anonymous | personal} information for the purpose of receiving targeted ads," if their web browser provided them six different options for control.

69% would not pay to remove ads, and 80% would not pay to see generic ads in place of targeted ads. Participants cited several reasons for not being willing to pay. They commonly felt they could obtain the information they wanted on other websites without paying, or use free software to block ads. They also felt that websites should be free, and that privacy is a right they should not have to pay for.

Participants who were willing to pay said they would pay a median amount of $3.00 to stop data collection, $2.25 to remove all ads, and $2.00 to show generic ads in place of targeted ads. That a larger proportion of participants were willing to pay money to stop data collection than to remove ads, and that those who were willing to do so would pay more, indicate that many participants value stopping data collection more than removing ads. However, participants' low willingness overall to pay for any of these scenarios suggests that their perceptions are rooted in the belief that websites and ad-blocking tools should be free.

4.5 Levels of Control

Current web browsers do not provide usable, fine-grained control over data collection for OBA purposes, nor over the display of targeted ads. To explore whether the introduction of new, fine-grained controls would help users feel more comfortable sharing data with advertisers, we asked six questions about a hypothetical browser plugin that would give the user control over, as well as better visibility into, the information collected by online advertising companies for the purpose of showing targeted advertisements.

For each feature, we asked users whether they would be more willing to disclose information if they were able to take advantage of a plugin with this feature. The six plugin features were "choose ahead of time what information to disclose," "control which ad companies can collect the information," "visualize and edit information already disclosed," "create different 'personas'," "control which websites [can collect information]," and "visualize which websites already collected information." Independent of their condition, half of our participants were asked about plugins for controlling anonymous information, and half about plugins for controlling personally identifiable information.

Respondents reported that a plugin with some of the six proposed features would make them more willing to share anonymous (84% of participants) and personally identifiable (74% of participants) information with advertisers. This difference—where participants asked about sharing anonymous information were more likely to share more in the presence of a plugin—was consistent across five of our six proposed plugin features. The exception was the "create different 'personas' " feature, where the trend was reversed. This result was consistent with our expectations, since the concept of a persona is less relevant to anonymous than to personally identifiable information.

Which plugin features participants thought would most increase their willingness to share differed between the set of participants who were asked about sharing anonymous information and those who were asked about sharing personally identifiable information. Perhaps unsurprisingly, participants who were asked about sharing personally identifiable information were most frequently interested in plugin features that allowed them to prevent information from being sent to advertisers in the first place (59–64% reported that they would share more). A smaller proportion would share more if they could see after the fact what information had been gathered (52%), or on what sites (39%). Most participants who were asked about sharing anonymous information reported that these features would increase their sharing.

Overall, we believe these results suggest that although participants were not willing to disclose much information online, offering more adequate control over disclosure could mitigate some of their privacy concerns.

5. DISCUSSION

While general attitudes toward online behavioral advertising have been investigated numerous times [19], our study is the first to investigate how companies' privacy practices impact users' willingness to disclose different types of information for OBA. When making choices given only the names of companies, participants in a prior study said they would decide whether to permit data collection based on the companies' non-OBA activities [34]. While scope-of-use and data-retention practices had a statistically significant effect on participants' willingness to share, we note that the effect size was relatively small. Nevertheless, even a small effect size has important practical implications when applied to millions of Internet users. Knowing which OBA privacy practices matter most to users can inform the policy debate surrounding online behavioral advertising, as well as the design of user interfaces that highlight the most pertinent information when users make privacy decisions.

In contrast to prior studies that were more abstract, we aimed to ground our evaluation in a more concrete scenario. By asking participants to browse a particular health site before explaining how online behavioral advertising would work according to their assigned condition, we allowed participants to envision a realistic web-browsing scenario. We also verified that participants could correctly answer knowledge questions about both OBA and the privacy practices specified by their condition, mitigating concerns that participants' sharing decisions were based on an incorrect understanding of OBA or unawareness of the advertising companies' privacy practices.

5.1 Improving OBA Choice

That the data-retention period and scope of use communicated by our privacy notices significantly impacted participants' willingness to share suggests directions for improving privacy-choice mechanisms for OBA. Rather than asking users to make decisions about OBA when given an advertising company's name or very general information, information about a company's data-retention policies and the scope of ad targeting might help users make more meaningful privacy decisions. One can imagine privacy disclosures that briefly highlight these policies when allowing users to choose whether to opt out of OBA from that company. One could similarly imagine automated privacy agents that allow a user to specify acceptable values for these policies. The agent could act automatically based on these preferences.

Data-retention policies in the real world unfortunately do not match our participants' preferences. Based on a small sample of privacy policies for members of the Network Advertising Initiative (NAI), a major advertising industry group in the United States, we have observed that many advertising companies do indeed commit to retaining data for a definite period. Unfortunately, whereas the inflection point for our participants' preferences appeared to be on the order of days, the companies whose policies we observed tended to retain data for months or years. Furthermore, not all companies we observed commit to definite retention periods, yet we found data retention to be a significant factor in participants' decision making.

We also found that the scope of use was an important factor in participants' decision making. In our sample of NAI members' privacy policies, we found that many ad companies commit in their privacy policies to use collected data only for ad targeting, yet participants in past studies have voiced fear that data collected for OBA would be used for nefarious purposes [34]. We found that around half of participants were willing to disclose some types of data in exchange for targeted ads, including certain kinds of demographic information. However, fewer participants were willing to share personally identifiable information, or even many types of browsing information. To assuage users' concerns to a degree, advertising networks could highlight current policies regarding the scope of data use in their privacy interfaces. Some ad companies, however, provide fairly vague statements of data use, and these statements could be clarified and elucidated.

Providing users access to review data collected about them did not influence participants' preferences. This sort of access is already available for general interest categories using ad preference managers from a small number of companies, including Google,[4] Microsoft,[5] and Yahoo.[6] However, little is actually known about how users interact with ad managers and privacy dashboards. Our results suggest that giving users access to data does not substantially impact their willingness to share, and that further research is needed to investigate how access impacts individuals' attitudes.

Whereas familiarity with the advertising network collecting data was found in past work to influence participants' willingness to permit data collection [34], our study was the first to examine the influence of participants' familiarity with the first-party site on which data was collected. Although WebMD was rated more familiar, trustworthy, and reputable than the fictitious WebDR, the site participants saw had minimal impact on their willingness to disclose information for OBA purposes. Although one must take care not to overgeneralize from a particular site and scenario, this result suggests that the brand familiarity of the first-party site on which data is collected may be of less importance than the privacy practices of the advertising network.

Although we found that different policies regarding data retention and scope of use would impact participants' willingness to permit data collection, around half of our participants would not be willing to share any information for online behavioral advertising purposes. In light of such attitudes, intuition might suggest that providing users further opportunities to limit online behavioral advertising would lead users to reject online behavioral advertising entirely. We found, however, that many users would be *more* willing to permit data collection for OBA purposes if given the opportunity to control this collection a priori. We also found that privacy concerns significantly reduced willingness to share while perceived benefits from targeted ads significantly increased it. These results suggest that in order to increase users' comfort with OBA, privacy concerns should be mitigated by both better informing users about information-handling practices and providing them with greater control to limit behavioral advertising on their own terms.

Our results can also be instructive for legislating broader privacy practices. We found that many participants were willing to share certain types of information, while few participants wanted to share other types of information. That under 1% of participants across conditions would allow their Social Security number or credit card number to be collected, and that under 5% of participants would allow their credit score bracket, exact location, phone number, or home address to be collected, suggests that a prohibition on the collection of these types of information would match users' preferences. Similarly, between 5% and 20% of participants would allow the collection of their name, email address, medications taken, income bracket, religion, political preferences, or IP address, suggesting this information to be reasonably sensitive.

Unfortunately, even though it was updated in 2013, the NAI code of conduct [25] released as part of the advertising industry's self-regulation program does not mirror all of the preferences we observed in our study. Few users modify options that are set by default [18], highlighting the importance of reasonable default settings. The NAI code of conduct follows this guidance by defining certain types of data as "sensitive" and requiring that consumers opt in to the use of either sensitive data or personally identifiable information for OBA purposes. As defined by the NAI, these sensitive data include "Social Security numbers," "insurance plan numbers," "financial account numbers," "precise information about ... health or medical conditions or treatments," and "sexual orientation." Opt-ins are thus required for the collection of some types of data our participants were generally unwilling to share.

Unfortunately, a number of types of data our participants appeared to deem sensitive *can be* collected by network advertisers unless a user opts out. For instance, a user's credit-

[4] `http://www.google.com/ads/preferences/`
[5] `http://choice.live.com/AdvertisementChoice/Default.aspx`
[6] `http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/details.html`

score bracket, income bracket, religion, political preferences, and IP address could be collected or inferred unless a user has explicitly opted out under these regulations. Our results suggest that these defaults are inconsistent with users' preferences. This result is a problem not just in the letter of industry regulations, but also in practice; some of this information has been observed being collected and used for ad targeting in the wild [37].

Although nearly half of our participants were unwilling to allow any information to be collected for OBA purposes, certain types of data appeared not to be particularly sensitive for the remaining participants. Between 41% and 53% of participants were willing to allow their operating system, web browser version, gender, country, and state to be collected for OBA purposes. Among users who wish to have their data collected for OBA purposes, these types of information could likely be collected without prompting. However, given the fairly even split between participants who would permit those types of data to be collected and those that would not want any data to be collected, any default setting regarding data collection for OBA purposes would seem to mismatch half of our participants' preferences. We note that 35% of our participants would disclose information about their hobbies, which seems particularly useful for targeting advertisements based on interest.

Based on our results regarding participants' willingness to pay money to stop different facets of OBA, we found that users are more concerned about data collection than advertisements. In current practice, however, advertising industry opt-out mechanisms are only required [25] to stop ad targeting, not necessarily stopping data collection. As with data-retention practices, industry guidelines appear misaligned with users' wishes regarding data collection.

Although users' relative concern about different types of data should likely be a major factor in data-collection policy and practice, it should not be taken as gospel. For instance, data that may seem innocuous on their own can sometimes reveal unintended information [32]. The burden should not fall on users to evaluate potential information leaks. For instance, over 40% of participants in our study would allow the collection of "search terms entered" or "pages visited" on a particular health site, yet less than half as many participants would permit the collection of "the medication I am taking (inferred from my interactions with the [same] site)," even though the search terms entered and pages visited could likely be used to infer this information. Privacy experts can advocate for user protections that users themselves may not realize are needed to match users' goals.

5.2 Limitations

While our choice of simulating a web-browsing scenario within an online survey allowed us to investigate concretely how different dimensions of privacy policy affect users' willingness to permit the collection of information for OBA, this approach has a number of limitations. First of all, our data are self-reported values based on participants' perceived willingness to permit the collection of data in a hypothetical scenario. While not a substitute for behavioral data in real-world scenarios, this type of self-reported data can still provide valuable insight into users' privacy attitudes when interface limitations are eliminated. Furthermore, the study design made privacy notices more prominent than in the real world, potentially emphasizing privacy in participants' decision making. One could argue, however, that privacy notices in the real world are insufficiently noticeable and that drawing attention to them better captures users' preferences.

Our study is primarily exploratory and has limited generalizability. For instance, we only explored the narrow scenario of a user visiting a single health website and having behavioral information collected by a single advertising network. Although this scenario is not generalizable to all types of websites and the full ecosystem of myriad companies tracking data [19], it provides valuable insight into privacy attitudes in a controlled scenario. Furthermore, we only discussed uses of data related to targeting advertisements, while a more general study might have considered other factors identified in past work, such as users' concerns about identity theft [34]. Finally, participants were recruited from among the population of Amazon's Mechanical Turk workers registered in the United States. Although this sample is not representative of the overall population of the United States, the demographics of Mechanical Turk workers have been studied previously [29] and have been shown to provide a sample at least as diverse as traditional human-subject recruitment channels [11].

6. CONCLUSION

While users' general attitudes toward online behavioral advertising have been studied repeatedly, less is known about how different privacy practices impact users' willingness to share information with advertisers. To this end, we conducted a 2,912-participant online study in which participants visited a health website, were presented with prominent notice about privacy practices governing data collection for OBA purposes, and rated their willingness to allow 30 different types of data to be collected.

We found that almost no one was willing to share some types of data, such as their credit card number, address, and phone number. While nearly half of our participants would not be willing to share any data for OBA purposes, most of the remainder were willing to share information about their country, gender, operating system, web browser, and pages they've visited on a particular health website.

We found that data-retention policies and the scope of data use significantly impacted participants' willingness to share personal information. We further found the majority of participants to be unwilling to pay money to stop data collection or even advertising, believing websites should be free. Further, participants would be more willing to share information if given greater control over what personal information would be collected, and by whom.

7. ACKNOWLEDGMENTS

We thank Julie Downs, Bart Knijnenburg, Alfred Kobsa, Saranga Komanduri, and Jeffrey Stanton for very helpful advice and feedback on analysis methods. This research was funded in part by National Science Foundation grants DGE0903659, CNS1012763, and CNS1116934, by the Department of Defense (DoD) through the National Defense Science & Engineering Graduate Fellowship (NDSEG) Program, and by a grant awarded to the University Corporation for Advanced Internet Development (Internet2) under the sponsorship of the U.S. Department of Commerce, National Institute of Standards and Technology.

8. REFERENCES

[1] A. Acquisti, L. K. John, and G. Loewenstein. The impact of relative standards on the propensity to disclose. *Journal of Marketing Research*, 49(2):160–174, 2012.

[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. *Management Information Systems Quarterly*, 30(1), 2006.

[3] J. Burkell and A. Fortier. Consumer health websites and behavioural tracking. In *Proc. of the 40th Annual Conference of the CAIS*, 2012.

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

[5] Federal Trade Commission. Protecting consumer privacy in an era of rapid change. `http://www.ftc.gov/os/2012/03/120326privacyreport.pdf`, March 2012.

[6] M. Geuss. Firefox will block third-party cookies in a future version. In *Ars Technica*. February 2013.

[7] P. Golle. Revisiting the uniqueness of simple demographics in the us population. In *Proc. WPES*, 2006.

[8] J. Gomez, T. Pinnick, and A. Soltani. KnowPrivacy. `http://www.knowprivacy.org/report/KnowPrivacy_Final_Report.pdf`, June 2009.

[9] S. Greengard. Advertising gets personal. *Communications of the ACM*, 55(8):18–20, 2012.

[10] A. N. Joinson, U.-D. Reips, T. Buchanan, and C. B. P. Schofield. Privacy, trust, and self-disclosure online. *Human–Computer Interaction*, 25(1):1–24, 2010.

[11] A. Kittur, E. H. Chi, and B. Suh. Crowdsourcing user studies with Mechanical Turk. In *Proc. CHI*, 2008.

[12] S. Komanduri, R. Shay, G. Norcie, B. Ur, and L. F. Cranor. AdChoices? Compliance with online behavioral advertising notice and choice requirements. *ISJLP*, 7:603–721, 2012.

[13] B. Krishnamurthy, K. Naryshkin, and C. Wills. Privacy leakage vs. protection measures: the growing disconnect. In *Proc. W2SP*, 2011.

[14] B. Krishnamurthy and C. Wills. Privacy diffusion on the web: A longitudinal perspective. In *Proc. WWW*, 2009.

[15] B. Krishnamurthy and C. E. Wills. On the leakage of personally identifiable information via online social networks. In *Proc. WOSN*, 2009.

[16] P. Leon, B. Ur, R. Shay, Y. Wang, R. Balebako, and L. Cranor. Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising. In *Proc. CHI*, 2012.

[17] P. G. Leon, J. Cranshaw, L. F. Cranor, J. Graves, M. Hastak, B. Ur, and G. Xu. What do online behavioral advertising disclosures communicate to users? In *Proc. WPES*, 2012.

[18] S. Lohr. The default choice, so hard to resist. In *New York Times*. October 2011.

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

[20] A. McDonald and L. Cranor. The cost of reading privacy policies. *ISJLP*, 4:543–897, 2009.

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

[22] J. McEntegart. Microsoft sticks to "Do Not Track" plans for IE in Windows 8. In *Tom's Hardware*. August 2012.

[23] M. J. Metzger. Effects of site, vendor, and consumer characteristics on web site trust and disclosure. *Communication Research*, 33(3):155–179, 2006.

[24] A. Narayanan and V. Shmatikov. Robust de-anonymization of large sparse datasets. In *Proc. IEEE Symposium on Security and Privacy*, 2008.

[25] Network Advertising Initiative. 2013 NAI code of conduct. `http://www.networkadvertising.org/2013_Principles.pdf`, 2013.

[26] H. Nissenbaum. A contextual approach to privacy online. *Daedalus*, 140(4):32–48, 2011.

[27] F. Roesner, T. Kohno, and D. Wetherall. Detecting and defending against third-party tracking on the web. In *Proc. NSDI*, 2012.

[28] A. Roosendaal. We are all connected to Facebook...by Facebook! In *European Data Protection: In Good Health?*, pages 3–19. Springer, 2012.

[29] J. Ross, L. Irani, M. S. Silberman, A. Zaldivar, and B. Tomlinson. Who are the crowdworkers? Shifting demographics in Mechanical Turk. In *Proc. CHI Extended Abstracts*, 2010.

[30] S. Sengupta. Web privacy becomes a business imperative. In *New York Times*. March 2013.

[31] N. Singer. Mediator joins contentious effort to add a "Do Not Track" option to web browsing. In *New York Times*. November 2012.

[32] L. Sweeney. Uniqueness of simple demographics in the U.S. population. Technical report, Carnegie Mellon University LIDAP-WP4, 2000.

[33] D. G. Taylor, D. F. Davis, and R. Jillapalli. Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research*, 9(3):203–223, 2009.

[34] B. Ur, P. G. Leon, L. F. Cranor, R. Shay, and Y. Wang. Smart, useful, scary, creepy: Perceptions of online behavioral advertising. In *Proc. SOUPS*, 2012.

[35] E. Van De Garde-Perik, P. Markopoulos, B. De Ruyter, B. Eggen, and W. Ijsselsteijn. Investigating privacy attitudes and behavior in relation to personalization. *Social Science Computer Review*, 26(1):20–43, 2008.

[36] White House. Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy. `http://www.whitehouse.gov/sites/default/files/privacy-final.pdf`, Feb. 2012.

[37] C. E. Wills and C. Tatar. Understanding what they do with what they know. In *Proc. WPES*, 2012.

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

APPENDIX

A. FACTOR ANALYSIS

Factor	Statement	Disclose	α if item removed	Factor Loading
Browsing Information ($\alpha = 0.92$)	How long I spent on each page of the *WebMD* website	25.3%	0.89	0.80
	My responses to health-related surveys	30.1%	0.91	0.77
	The medications I am taking (inferred from my interactions with the site)	18.7%	0.92	0.62
	The pages I've visited on the *WebMD* website	42.8%	0.89	0.98
	Which search terms I've entered on the *WebMD* website	41.2%	0.89	0.99
Computer Information ($\alpha = 0.93$)	The name and version of the web browser (e.g., Internet Explorer 9, Firefox 18.0.1, Safari 6.0.2, etc.) that I use to visit the *WebMD* website	42.9%	0.93	0.97
	The type of operating system (e.g., Windows, Mac, etc.) of my computer	44.8%	0.93	0.94
Demographic Information ($\alpha = 0.94$)	My age	39.1%	0.94	0.67
	My gender	46.3%	0.94	0.67
	My highest level of education	27.4%	0.93	0.89
	My hobbies	34.9%	0.94	0.76
	My income bracket	9.6%	0.94	0.65
	My marital status	25.2%	0.93	0.94
	My religion	17.3%	0.94	0.97
	My political preferences	16.7%	0.94	0.98
	My sexual orientation	21.1%	0.94	0.99
Location Information ($\alpha = 0.91$)	The country from which I'm visiting the *WebMD* website	52.7%	0.90	0.60
	The state from which I'm visiting the *WebMD* website	42.9%	0.90	0.79
	The town or city from which I'm visiting the *WebMD* website	24.4%	0.82	1.08
	The ZIP code from which I'm visiting the *WebMD* website	22.6%	0.85	1.06
Personally Identifiable ($\alpha = 0.81$)	My email address	14.0%	NA	*
	My name	13.6%	NA	*
Did not conform to a factor	My address	1.9%	NA	NA
	My credit card number	0.6%	NA	NA
	My credit score bracket	4.5%	NA	NA
	My phone number	2.6%	NA	NA
	My Social Security number	0.6%	NA	NA
	My weight and height	25.5%	NA	NA
	The exact address from which I'm visiting the *WebMD* website	3.9%	NA	NA
	The IP address of my computer (i.e., a computer identifier assigned by your Internet service provider)	15.3%	NA	NA

Table 3: Participants' willingness to disclose different types of information for OBA purposes (N=2,912). Using exploratory factor analysis, we grouped 22 of the 30 types of information into five factors. The *disclose* column lists the percentage of participants who agreed or strongly agreed that they would be willing to disclose that type of information. The α *if item removed* column displays Cronbach's Alpha, the correlation of items in the group, if that item were to be removed from the group. The *loading* column displays the factor loading from exploratory factor analysis, or NA for types of information that had below 0.60 factor loading for all five factors. The two types of data with a factor loading of "*" did not meet the criteria for inclusion with a factor, while no types of information loaded sufficiently onto the fifth factor. Since these two types of information were correlated with each other ($\alpha = 0.81$), we considered them to be the fifth factor.

B. MULTIVARIATE MULTIPLE REGRESSION MODEL

Independent Variable	Control Category	Coefficient	SE	t	Pr(>|t|)
Dependent Variable: Browsing information					
Scope: Health site + Facebook	Only health site	-0.986	0.088	-11.202	<0.001
Scope: All sites	Only health site	-0.297	0.088	-3.363	<0.001
Retention: Indefinite	One day	-0.465	0.082	-5.639	<0.001
Facebook usage	Not Facebook user	0.154	0.043	3.560	<0.001
Privacy concern	Unconcerned	-0.291	0.030	-9.667	<0.001
Like targeted ads	Don't like	0.684	0.040	16.759	<0.001
Interaction: Facebook and Retention	NA	0.312	0.097	3.209	0.001
Dependent Variable: Computer information					
Facebook usage	Not Facebook user	0.220	0.051	4.302	<0.001
Privacy concern	Unconcerned	-0.254	0.035	-7.152	<0.001
Like targeted ads	Don't like	0.590	0.048	12.242	<0.001
Dependent Variable: Demographic information					
Retention: Indefinite	One day	-0.172	0.008	-2.248	0.025
Age	NA	-0.004	0.002	-2.228	0.026
IT experience	None	-0.073	0.031	-2.310	0.021
Facebook usage	Not Facebook user	0.210	0.040	5.206	<0.001
Privacy concern	Unconcerned	-0.326	0.028	-11.669	<0.001
Like targeted ads	Don't like	0.622	0.038	16.390	<0.001
Interaction: Facebook and Retention	NA	0.181	0.090	2.002	0.045
Dependent Variable: Location information					
Scope: Health site + Facebook	Only health site	-0.328	0.093	-3.531	<0.001
Retention: Indefinite	One day	-0.283	0.087	-3.249	0.001
Age	NA	0.008	0.002	3.924	<0.001
Facebook usage	Not Facebook user	0.187	0.046	4.092	<0.001
Privacy concern	Unconcerned	-0.340	0.032	-10.727	<0.001
Like targeted ads	Don't like	0.623	0.043	14.476	<0.001
Dependent Variable: Personally identifiable information					
Scope: Health site + Facebook	Only health site	0.329	0.083	3.959	<0.001
Facebook usage	Not Facebook user	0.190	0.041	4.638	<0.001
Privacy concern	Unconcerned	-0.262	0.028	-9.244	<0.001
Like targeted ads	Don't like	0.432	0.039	11.227	<0.001
Interaction: Facebook and Retention	NA	0.186	0.092	2.024	0.043

Table 4: This table shows the multivariate multiple regression model underlying our analysis of participants' willingness to disclose information. In addition to the retention, scope, access, and site familiarity treatments, we included the following co-variates: age, gender, frequency of Facebook usage (Q10 in Appendix C), whether or not the participant held a degree or job in IT or a related field (Q7), privacy concerns (Q46), and whether the participant likes targeted ads (Q38). Only terms significant at α<0.05 are shown.

C. SURVEY QUESTIONS

Important: Please think thoroughly before answering each question. Your precise responses are very important for us. We are not interested in what someone else thinks - we want to know what you think! You may give an incomplete answer or say you do not know.

1) 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. In a sentence or two, please tell us what you think about website advertising.*

---

2) How much do you agree or disagree with the following statements?*

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Website advertising is necessary to enjoy free services on the Internet	( )	( )	( )	( )	( )
In general, I find website advertising useful	( )	( )	( )	( )	( )
In general, I find website advertising distracting	( )	( )	( )	( )	( )
In general, I find website advertising to be relevant to my interests	( )	( )	( )	( )	( )
I usually don't look at the ads that appear on the websites that I visit	( )	( )	( )	( )	( )

---

3) What's your gender?*
( ) Male ( ) Female

4) What's your age (in years)?*

5) Which of the following best describes your primary occupation?*
( ) Administrative support (e.g., secretary, assistant)
( ) Art, writing, or journalism (e.g., author, reporter, sculptor)
( ) 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)
( ) Retired
( ) Scientist (e.g., researcher, professor)
( ) Service (e.g., retail clerks, server)
( ) Skilled labor (e.g., electrician, plumber, carpenter)
( ) Student
( ) Unemployed
( ) Decline to answer
( ) Other (Please specify): _____*

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

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

---

8) Using only desktop or laptop computers, either at home or at work, 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

9) Using only mobile devices (e.g., Android Smartphone, iPhone, iPad, tablet, or similar), approximately how much time 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

10) Approximately how often do you use Facebook?*
( ) Never
( ) A few times per month or less
( ) Once per week
( ) Several times per week
( ) Once per day
( ) Several times per day

11) Have you ever...? (Select all that apply)*
[ ] ...purchased a product or service online (e.g., music, books, clothing, etc.)
[ ] ...used a social networking site (e.g., Facebook, Twitter, LinkedIn, MySpace, etc.)
[ ] ...clicked on an ad that appeared on a website to get more information about the advertised product
[ ] ...accidentally clicked on an ad that appeared on a website
[ ] ...visited health, wellness, or medical information websites (e.g., MayoClinic, MyFitnessPal, Men's Health, etc.)
[ ] ...used a search engine to find information about a medical condition

[ ] None of the above

Visiting a healthcare website
[WebMD/WebDR] is a healthcare information website. It provides information about the symptoms, treatment, and prevention of a range of health conditions.

Clicking on the link below will open a new tab or window in your browser displaying a version of the [WebMD/WebDR] website homepage with links disabled. Please look through this page at your own pace and make sure to scroll down and look at the entire page. Then, answer the following questions. Feel free to review the opened tab as many times as you want to answer these questions.
Click here to visit the [WebMD/WebDR] homepage

12) Please select from the list below at least three of the health conditions that appear on the left-hand side of the [WebMD/WebDR] homepage.*
[ ] Acne
[ ] Allergies
[ ] Alzheimer
[ ] Asthma
[ ] Bipolar disorder
[ ] Cancer
[ ] Carpal tunnel
[ ] Conjunctivitis
[ ] Depression
[ ] Glaucoma
[ ] Herpes
[ ] Hyperactivity
[ ] Hypertension
[ ] Osteoporosis

13) Indicate how much you agree or disagree with the following statements.*

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I have a positive impression of the [WebMD/WebDR] website	( )	( )	( )	( )	( )
I believe [WebMD/WebDR] is a trustworthy website	( )	( )	( )	( )	( )
I believe the [WebMD/WebDR]website protects my privacy	( )	( )	( )	( )	( )
I am familiar with the [WebMD/WebDR]website	( )	( )	( )	( )	( )
I believe [WebMD/WebDR]is a well-known website	( )	( )	( )	( )	( )
I believe the [WebMD/WebDR]website has a good reputation	( )	( )	( )	( )	( )
I believe the [WebMD/WebDR]website provides useful information	( )	( )	( )	( )	( )

14) Had you ever visited the [WebMD/WebDR] website before (other than in this study)?*
( ) Yes ( ) No ( ) I don't remember

15) How often have you visited the [WebMD/WebDR] website 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

16) Do you have a user account on the [WebMD/WebDR] website?*
( ) Yes ( ) No ( ) I don't remember

17) Have you visited other health or medical-information websites in the past?*
( ) Yes ( ) No ( ) I don't remember

Please read this information carefully. Then answer the questions below.
Many websites, including [WebMD/WebDR], are able to offer free services to their visitors by contracting with online advertising companies. The advertising companies pay websites for every ad they show, allowing the websites to provide free services for users like you.
Imagine that you are experiencing a flaky scalp condition and decide to visit the [WebMD/WebDR] website. [WebMD/WebDR] has contracted with ***[XYZ Advertising Company/Facebook]*,** which collects information about your interactions with the [WebMD/WebDR] website in order t **predict your preferences** and to show you ads that are most likely to be of interest to you. These ads are known as **targeted ads**. For example, if you search for "flaky scalp" or read an article about scalp problems on the [WebMD/WebDR] website, ***[****XYZ Advertising Company/Facebook]* could show you ads for dandruff shampoo or another related product.

In particular, ***[XYZ Advertising Company/Facebook]*** will:
1. Collect your information **only from the** [WebMD/WebDR] website.
2. Use the collected information to show you **targeted ads only on the** [WebMD/WebDR] website.
3. Retain and use collected information for a [**maximum period of one day/indefinite period time]**.

[No text/ In addition: ***[XYZ Advertising Company/Facebook]*** will provide you access to a webpage where you can **review, edit, and delete** the information that is being collected about you. For example, you can confirm that your information and preferences are accurate and remove information that you no longer feel comfortable sharing.]

---

18) Based on the information that you just read, which of the following are examples of the types of targeted ads that might occur as a result of your visit to [WebMD/WebDR]? (Choose any that apply)*
[ ] You see ads for bicycles on [WebMD/WebDR] since studies have found that many visitors to [WebMD/WebDR] are bicycle enthusiasts
[ ] You see ads for Acme cough syrup on Facebook because you read about cough remedies on [WebMD/WebDR]
[ ] You see ads for Acme cough syrup on [WebMD/WebDR] because a friend emailed you information about cough remedies
[ ] You see ads for Acme cough syrup on [WebMD/WebDR] because you read about cough remedies on [WebMD/WebDR]

[ ] You see ads for Acme cough syrup on www.WashingtonPost.com because you read about cough remedies on [WebMD/WebDR]

19) Based on the information that you just read, which of the following statements best explains how [XYZ Advertising Company/Facebook] may use the information that it collects about you?*

( ) To show me non-targeted ads on the websites that I visit
( ) To show me targeted ads only on the [WebMD/WebDR] website
( ) To show me targeted ads on the [WebMD/WebDR] website and other websites that I visit
( ) To show me targeted ads only on Facebook
( ) To show me targeted ads on Facebook and on the [WebMD/WebDR] website
( ) Other [Please explain]: _____*

20) Based on the information that you just read, for how long may [XYZ Advertising Company/Facebook] use the information collected about you?*

( ) One day ( ) One week ( ) One year ( ) Indefinitely

Suppose that you use only your home computer to access the [WebMD/WebDR] website, and that nobody else uses this computer. Based only on the information that your read above, please answer the questions below indicating what information you would allow [XYZ Advertising Company/Facebook] to collect for the purpose of showing you targeted ads [on your Facebook page and the (WebMD/WebDR) website/only on the (WebMD/WebDR) website/on the (WebMD/WebDR) website and other websites you visit]

21) I would be willing to allow [XYZ Advertising Company/Facebook] to use and store the following information about my computer. This information will be retained [indefinitely/one day] [nothing/and you will be able to review, edit, and delete it]*

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
The type of operating system (e.g., Windows, Mac, etc.) of my computer	( )	( )	( )	( )	( )
The IP address of my computer (i.e., a computer identifier assigned by your Internet service provider)	( )	( )	( )	( )	( )
The name and version of the web browser (e.g., Internet Explorer 9, Firefox 18.0.1, Safari 6.0.2, etc.) that I use to visit the [WebMD/WebDR] website	( )	( )	( )	( )	( )

22) I would be willing to allow [XYZ Advertising Company/Facebook] to use and store the following demographic and preference information. This information will be retained [indefinitely/one day[nothing/and you will be able to review, edit, and delete it]*

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
My age	( )	( )	( )	( )	( )
My gender	( )	( )	( )	( )	( )
My highest level of education	( )	( )	( )	( )	( )
My income bracket	( )	( )	( )	( )	( )
My religion	( )	( )	( )	( )	( )
My political preferences	( )	( )	( )	( )	( )
My sexual orientation	( )	( )	( )	( )	( )
My marital status	( )	( )	( )	( )	( )
My hobbies	( )	( )	( )	( )	( )
My credit score bracket	( )	( )	( )	( )	( )

23) I would be willing to allow [XYZ Advertising Company/Facebook] to use and store the following information related to my interactions with the [WebMD/WebDR] website. This information will be retained [indefinitely/one day[nothing/and you will be able to review, edit, and delete it]*

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
The pages I've visited on the [WebMD/WebDR] website	( )	( )	( )	( )	( )
Which search terms I've entered on the [WebMD/WebDR] website	( )	( )	( )	( )	( )
My weight and height	( )	( )	( )	( )	( )
My responses to health-related surveys	( )	( )	( )	( )	( )
The medications I am taking (inferred from my interactions with the site)	( )	( )	( )	( )	( )
How long I spent on each page of the [WebMD/WebDR] website	( )	( )	( )	( )	( )

24) I would be willing to allow [XYZ Advertising Company/Facebook] to use and store the following information related to my location. This information will be retained [indefinitely/one day[nothing/and you will be able to review, edit, and delete it]*

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
The country from which I'm visiting the [WebMD/WebDR] website	( )	( )	( )	( )	( )
The state from which I'm visiting the [WebMD/WebDR] website	( )	( )	( )	( )	( )
The town or city from which I'm visiting the [WebMD/WebDR] website	( )	( )	( )	( )	( )
The zip code from which I'm visiting the [WebMD/WebDR] website	( )	( )	( )	( )	( )
The exact address from which I'm visiting the [WebMD/WebDR] website	( )	( )	( )	( )	( )

25) I would be willing to allow [XYZ Advertising Company/Facebook] to collect the following information. This information will be retained [indefinitely/one day[nothing/and you will be able to review, edit, and delete it]*

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
My name	( )	( )	( )	( )	( )
My email address	( )	( )	( )	( )	( )
My phone number	( )	( )	( )	( )	( )
My address	( )	( )	( )	( )	( )
My social security number	( )	( )	( )	( )	( )
My credit card number	( )	( )	( )	( )	( )

26) How would your willingness to allow [XYZ Advertising Company/Facebook] to collect your information change if it retained your information...*

	I would be less willing	I would be equally willing	I would be more willing
...only for the duration of a single web browsing session	( )	( )	( )
...for one week	( )	( )	( )
...for one month	( )	( )	( )
... for six months	( )	( )	( )
...for one year	( )	( )	( )
...indefinitely	( )	( )	( )

27) How would your willingness to allow [XYZ Advertising Company/Facebook] to collect your information change if it retained your information...*

	I would be less willing	I would be equally willing	I would be more willing
...only for the duration of a single web browsing session	( )	( )	( )
...for one day	( )	( )	( )
...for one week	( )	( )	( )
...for one month	( )	( )	( )
... for six months	( )	( )	( )
...for one year	( )	( )	( )

28) How would your willingness to allow [XYZ Advertising Company/Facebook] to collect your information change if it provided you access to a webpage where you could review, edit, and delete the information that is being collected about you? For example, you could confirm that your information and preferences are accurate and remove information that you no longer feel comfortable sharing.*

( ) I would be less willing
( ) I would be equally willing
( ) I would be more willing

---

29) Imagine that you are a frequent user of the [WebMD/WebDR] website, and that [WebMD/WebDR] offers you the opportunity to pay a monthly fee in exchange for not showing you any ads on the [WebMD/WebDR] website. In this case the information that [XYZ Advertising Company/Facebook] collects from you will not be used to show you ads, but may still be used for other purposes. What monthly fee, if any, in dollars and cents might you be willing to pay?*

30) Please explain how you chose the amount in the previous question.*

31) Imagine that you are a frequent user of the [WebMD/WebDR] website, and that [WebMD/WebDR] offers you the opportunity to pay a monthly fee in exchange for not showing you targeted ads but only generic ads on the [WebMD/WebDR] website. In this case the information that [XYZ Advertising Company/Facebook] collects from you will not be used to show you targeted ads, but may still be used for other purposes. What monthly fee (if an) in dollars and cents might you be willing to pay?*

32) Please explain how you chose the amount in the previous question.*

33) Imagine that you are a frequent user of the [WebMD/WebDR] website, and that [WebMD/WebDR] offers you the opportunity to pay a monthly fee in exchange for stopping [XYZ Advertising Company/Facebook] from collecting any information about you or your online activities on the [WebMD/WebDR] website. What monthly fee (if any) in dollars and cents might you be willing to pay?*

34) Please explain how you chose the amount in the previous question.*

---

35) How much do you agree or disagree with the following statements. I am interested in receiving targeted ads on the websites that I visit based on my online activities on...*

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree	I don't use them
...health websites	( )	( )	( )	( )	( )	( )
...online banking websites	( )	( )	( )	( )	( )	( )
...travel websites	( )	( )	( )	( )	( )	( )
...employment websites	( )	( )	( )	( )	( )	( )
...arts and entertainment websites	( )	( )	( )	( )	( )	( )
...dating websites	( )	( )	( )	( )	( )	( )
...news websites	( )	( )	( )	( )	( )	( )
...photo sharing websites	( )	( )	( )	( )	( )	( )
...social networking websites	( )	( )	( )	( )	( )	( )

---

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

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

38) Overall, how do you feel about receiving ads that are targeted based on your online activities?*

( ) Strongly dislike
( ) Dislike
( ) Neutral
( ) Like
( ) Strongly like

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

40) How would you feel about seeing ads on Facebook that are targeted based on your activities on other websites that you visit? Please explain.*

41) How much do you agree or disagree with the following statements:*

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
It would be useful to see ads on my Facebook page based on my interactions with the [WebMD/WebDR] website	( )	( )	( )	( )	( )
I would feel comfortable seeing ads on my Facebook page based on my interactions with the [WebMD/WebDR] website	( )	( )	( )	( )	( )
It would be useful to see ads on my Facebook page based on my activities on the [WebMD/WebDR] website and other websites I visit	( )	( )	( )	( )	( )
I would feel comfortable if Facebook shows me ads on my Facebook page based on my activities on the [WebMD/WebDR] website and other websites I visit	( )	( )	( )	( )	( )
It would be useful to see ads on the websites that I visit based on my activities on my Facebook page and other websites that I've visited in the past	( )	( )	( )	( )	( )
I would feel comfortable seeing ads on the websites that I visit based on my activities on Facebook and other websites that I've visited in the past	( )	( )	( )	( )	( )

42) Please state how much you agree or disagree with the following statements.
I would be more willing to allow collection of ANONYMOUS information (i.e., information that cannot be used to identify me or contact me) for the purpose of receiving targeted ads if my web browser...*

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
...allowed me to choose ahead of time what information advertising companies can learn about me	( )	( )	( )	( )	( )
...allowed me to control which advertising companies can collect and use that information	( )	( )	( )	( )	( )
...allowed me to visualize what the advertising companies already know about me	( )	( )	( )	( )	( )
...allowed me to create different "personas" (i.e., fake or real characterizations of me) to show to these advertising companies at different points in time	( )	( )	( )	( )	( )
...allowed me to control on which websites my information can be collected	( )	( )	( )	( )	( )
...showed me on which websites my information has been collected	( )	( )	( )	( )	( )

43) Please state how much you agree or disagree with the following statements.
I would be more willing to allow collection of PERSONAL information (i.e. information that can be used to identify me and contact me) for the purpose of receiving targeted ads if my web browser....*

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
...allowed me to choose ahead of time what information advertising companies can learn about me	( )	( )	( )	( )	( )
...allowed me to control which advertising companies can collect and use that information	( )	( )	( )	( )	( )
...allowed me to visualize what the advertising companies already know about me	( )	( )	( )	( )	( )
...allowed me to control on which websites my information can be collected	( )	( )	( )	( )	( )
...showed me on which websites my information has been collected	( )	( )	( )	( )	( )
...allowed me to create different "personas" (i.e., fake or real characterizations of me) to show to these advertising companies at different points in time	( )	( )	( )	( )	( )

44) Please tell us what functionality would you like to have in your web browser to control the information that online advertising companies collect about you for the purpose of showing you targeted ads.

This is the last page of the survey. Please answer these last questions as accurately as possible.

45) Please indicate whether you have ever done any of the following.*

	Yes	No
Refused to give information to a website because you felt it was too personal or unnecessary	( )	( )
Decided not to use a website or not to purchase something online because you were not sure how your personal information would be used	( )	( )
Read a website's privacy policy	( )	( )
Deleted cookies from your web browser	( )	( )
Turned on the "do not track" option in your web browser	( )	( )

46) How much do you agree or disagree with the following statements:*

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
When websites ask for personal information, I usually think twice about providing it	( )	( )	( )	( )	( )
Consumers have lost all control over how personal information is collected and used by companies	( )	( )	( )	( )	( )
I feel that as a result of my visiting websites, others know more about me than I am comfortable with	( )	( )	( )	( )	( )

47) Do you have any further comments?