Investigating the Effectiveness of Personalized Content in the Form of Videos When Promoting a TOR Browser

Yusuf Albayram
Department of Computer Science
Central Connecticut State University
New Britain, CT, USA
yusuf.albayram@ccsu.edu

David Suess
Department of Computer Science
Central Connecticut State University
New Britain, CT, USA
davidsuess@my.ccsu.edu

Yassir Yaghzar Elidrissi
Department of Computer Science
Central Connecticut State University
New Britain, CT, USA
yassiry@my.ccsu.edu

ABSTRACT

Due to increasing trend of data collection by websites, the use of privacy-enhancing technologies is becoming more and more important in our digital age. However, widespread adoption of tools that provide strongest protection, such as a TOR browser, has been low. Instead of using a "one-size-fits-all" approach when promoting privacy-enhancing technologies as users often vary widely in their perceptions and ways to be persuaded, this study investigated whether using "personalized" content in the form of videos based on decision-making style (GDMS scale) and the level of IT expertise would lead to a higher adoption rate of a TOR browser. Towards that, we designed a study (n = 186) with control and treatment groups. While participants in the control group were randomly given a video raising awareness of the TOR browser, participants in the treatment group were given one of four personalized versions of these videos based on their scores on IT expertise questions and the GDMS scale measuring social influence. Two follow-up surveys, each a week apart, were conducted to determine if the participants installed a TOR browser. We found that only a small percentage of participants started using a TOR browser, and the personalized group did not significantly differ from the control in terms of adoption rate. Though personalized videos did not increase the adoption rate, this study showed that other factors contributed to the low adoption rate and provided insights and recommendations for designing personalized effective videos promoting the TOR browser or similar privacy-enhancing technologies.

ACM Reference Format:
Yusuf Albayram, David Suess, and Yassir Yaghzar Elidrissi. 2022. Investigating the Effectiveness of Personalized Content in the Form of Videos When Promoting a TOR Browser. In *2022 European Symposium on Usable Security (EuroUSEC 2022), September 29–30, 2022, Karlsruhe, Germany*. ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3549015.3554178

1 INTRODUCTION

Due to increasing trend of data collection by websites, the use of privacy-enhancing technologies (PETs) is becoming more and more important in our digital age [17, 34]. However, widespread adoption of tools that provide strongest protection, such as a TOR browser, has been low [34, 39]. The low adoption is often attributed to usability issues (e.g., slowness, complexity) and/or harmful misconceptions about the protections provided by the privacy tools the users know [39, 40]. Thus, designing motivation materials that educate users about the privacy implications of their technology use and correct their misconceptions about these tools is crucial for increasing the adoption of privacy tools such as a TOR browser.

As users often vary widely in their perceptions of risk, level of motivation, and ways to be persuaded, the use of a "one-size-fits-all" approach when creating intervention nudges may not be the best way to persuade end-users to adopt PETs [15, 19]. While recent studies provide some evidence that Protection Motivation Theory (PMT)-based informative treatments are effective in increasing adoption of security and privacy tools [3, 4, 37, 38], the adoption rates are still limited. The effectiveness of content used to promote such tools can be amplified by tailoring materials for specific individuals. For example, the difficulty level of the material can be tailored to the technical proficiency of the individual to whom the material is presented as well as decision-making style of individuals (e.g., social influence) can also be used to personalize the content when it comes to the adoption of PETs. While a growing number of studies in the direction of using personalized nudges based on a person's psychometric traits have shown promising results in the context of security (e.g., improve password strength) [31, 33], no study, to the best of our knowledge, has investigated the effectiveness of using personalized video content in the context of increasing a TOR browser adoption. Towards that, we designed a controlled experiment with personalized video content interventions. Based on participants' scores on IT expertise questions and the GDMS scale measuring social influence, participants were shown one of the four videos. After the initial survey, two follow-up surveys were conducted (one week apart) to evaluate whether participants started using the promoted TOR browser.

Our two follow-up surveys showed that the adoption rate was very low (e.g., 11% in treatment vs. 10% in the control), and the personalized group was not significantly different from the control (i.e, randomized) in terms of adoption rate. Our qualitative data showed that while the majority of those who adopted a TOR browser wanted to "Give it a try", non-adopters did not deem privacy as a major concern for them and would adopt it if they needed more privacy. Though the majority of participants liked the videos and found them very informative, the videos were only effective for those who have higher perceived threat severity (2.2x, p=0.019) and response efficacy (3.1x, p=0.037). Although the personalization of

EuroUSEC 2022, September 29–30, 2022, Karlsruhe, Germany

ACM ISBN 978-1-4503-9700-1/22/09…$15.00
https://doi.org/10.1145/3549015.3554178

content based on IT expertise and social influence was not successful in increasing adoption of the TOR browser, there are a number of possible explanations for our null result, which we discuss in our discussion section.

2 RELATED WORK

The internet has been a major source of personal data collection for governments and businesses, used for data-driven business models to track, surveillance and censor users [17, 34]. While a TOR browser, if properly used, can provide the strongest anonymity and privacy for web browsing, the adoption rate is very low [39]. The low adoption rate can be attributed to a number of factors, such as usability issues (e.g., high latency and complexity of the TOR browser [14, 24, 29]), but some of these issues are psychological, such as optimistic bias, in which a person judges their own risk less than others [18, 25], and a misaligned perception of risk, in which users inconsistently adopt and abandon security and privacy practices depending on their perceived risk level, causing them to follow certain practices only in high-risk situations [40].

One way to promote and overcome the psychological and behavioral barriers can be through effective risk communication. For example, several studies showed that videos developed based on PMT are very effective in encouraging users to enable a secure smartphone lock screen [1, 3], password manager [4] or two-factor authentication (2FA) [2]. In the context of privacy, Story et al. [38] also showed the effectiveness of using PMT-based nudges presented in text form to motivate users to adopt the TOR browser. While these studies provide some evidence that PMT-based informative treatments are effective in increasing adoption of security and privacy tools, the adoption rates are still limited. This may be because the content of these studies was in a "one-size-fits-all" model, meaning the same content was provided to all participants regardless of their individual differences (e.g., decision-making style, computer proficiency etc.). The effectiveness of content used to promote such tools can be amplified by tailoring materials for specific individuals. For example, Peer et al. [31] demonstrated that nudges personalized based on people's decision-making styles lead to 4 times more effective outcomes (e.g., stronger passwords) compared to "one-size-fits-all" nudges designed with an average person in mind. Qu et al. [33] also showed that using a scale measuring users' concerns about future consequences to show them promotion or prevention-based nudges improved users' security attitudes (e.g., stronger passwords). Malkin et al. [27] took into consideration personalization by designing customized HTTP warning based on users' scores on the General Decision-Making Style (GDMS) instrument.

Our study builds on these studies and centers around using personalized content in the form of a video to increase the adoption rate of a TOR browser. Specifically, our study also focuses on increasing a TOR browser similar to the study conducted by Story et. al [38], but with three major differences: which are 1) use of personalized content 2) use of videos rather than text, and 3) use of the Brave Browser, which comes with a TOR connectivity feature [6, 22] rather than the TOR Browser from the TOR project [32].

3 METHODOLOGY

The goal of the study was to evaluate whether "personalized" content in the form of videos based on a person's decision-making style (i.e., social influence) and the level of IT expertise would lead to a higher adoption rate of a TOR browser. Towards this, we designed a study that contained four surveys, (pre-screening surveys, main survey, and two follow-up surveys). Next, we describe the details of each survey.

3.1 Recruitment and Survey Design

3.1.1 Recruitment. To recruit participants for this study, we used Prolific Platform, which is a crowd working platform similar to Amazon's Mechanical Turk with more demographically diverse subjects [30]. We restricted participants to those aged 18 years or older, living in the US, and having at least 95% approval rate.

3.1.2 Pre-screening Surveys. We used a two-part pre-screening process to select participants who have not used a TOR browser and would be motivated to install a TOR browser on their devices.

In the first part, we asked participants 4 multiple-choice questions to determine whether or not they have used a TOR browser. To prevent participants from easily guessing the eligibility criterion, the survey also included 3 more questions: whether they use 1) an antivirus software on their computer, 2) 2FA for at least one of their online accounts, and 3) a password manager to manage their online accounts. Participants who have not used a TOR browser were allowed to proceed directly to the second part.

In the second part, participants were asked more detailed questions and needed to meet the following eligibility criteria to qualify to take our main survey. In particular, eligible participants would be someone who: 1) used private browsing in the past week or a VPN as long as the VPN usage was not primarily for work, 2) used web browser on a laptop or desktop on multiple days in the past week, 3) is comfortable installing software on their laptop or desktop, and 4) is "moderately interested" or "very interested" in preventing at least one of the privacy threats described in the questions (e.g., preventing advertisers from seeing the websites they visit). Similar to the study of Story et al. [38], these criteria allowed us to recruit participants who would be motivated to install and use a TOR browser on one of their devices. Eligible participants were invited to take the main survey.

3.1.3 Main Survey. In the main survey, at first, participants were asked about their level of computer proficiency, IT experience, 6 quiz questions measuring their digital knowledge on security and privacy topics (see section 5.4 in the Appendix), and GDMS-Dependent scale. Participants' answers to these were used to compute their $IT-Expertise_{score}$ and $GDMS-Dependent_{score}$, which will be described in the next section.

Subsequently, participants were randomly assigned one of two groups: 1) treatment group (i.e., personalized content), and 2) control (i.e., randomized) group (inspired from [31]). In the treatment group, there were 4 sub-groups: 1) PMT, 2) PMT+tech-savvy, 3) PMT+social-influence and 4) PMT+tech-savvy+social-influnce. While participants in the personalized group were assigned to one of these four groups (shown in Table 2) based on their scores, participants in the control group were randomly assigned to one of these four groups regardless of their score (i.e., non-personalized). The participants were then shown a video about the TOR browser and were required to watch the video (ranging between 3:44 and

4:27 minutes long depending on the group they were assigned to). *PMT* content outlined privacy threats, the protection offered by a TOR mode in Brave browser, how they can install and use a TOR mode on this browser and possible misconception about using a TOR browser. $Tech-savvy$ content contained more technical information about how some of privacy enhancing technologies other than a TOR browser would be inefficient for better privacy. The $social-influence$ content included a security expert endorsing the TOR browser.

After the video, the participants were asked to evaluate the video with a set of questions. Finally, participants answered questions about their demographics, SEBIS scale[1] [12] to better understand their security and privacy practices and IUPS scale [26] to determine their awareness of security and privacy issues regarding internet and website usage. Participants who completed the main survey were invited to participate in two follow-up surveys.

3.1.4 Follow-up Surveys. To determine whether participants installed and used a TOR browser, we invited them to participate in two follow-up surveys.

The first follow-up survey was conducted one week after the main survey. To avoid biasing participants' actions, participants were not informed about the follow-up survey during the main survey. The participation was voluntary, and regardless of whether they installed or used a TOR browser, all participants were compensated with the same amount ($0.50). The survey gathered their reasoning for whether to install and/or use a TOR browser.

One week later, the same participants were invited to the second follow-up survey. The goal of the second follow-up survey was to see how many participants continued to use it (if they reported using it in the first follow-up) and whether those who did not install in the first follow-up started using it. Participants were asked the same set of questions as in the first follow-up survey.

We designed all of these surveys by using Django and SurveyJS that allowed us to further customize the surveys (e.g., integrated a feature checking whether the browser is a TOR).

3.2 Data Collection

1124 participants completed prescreening-1 survey. 890 (79.2%) participants were found eligible for the prescreening-2 survey (i.e., the TOR adoption rate was 20.8%). 884 participants completed prescreening-2 survey. 387 participants were found eligible for the main survey. However, we did not invite 8 participants who inconsistently answered two questions in the survey (e.g., in one question, they chose the tablet as a device type they never used, and in the other question, they chose the tablet they used a web browser for last week). Thus, at the end, 33.7% (379/1124) were found to be eligible to participate in our main survey based on our criteria.

The prescreening process lasted 3 days. After these 3 days, we invited eligible participants to the main survey. Out of 379 invited participants, 186 of them completed the main survey. The number of participants in each group are shown in Table 1. As seen in the table, the number of participants in the treatment group is skewed and not homogeneously distributed for each video group, the same pattern was also observed in the personalized nudge study by Peer et al. [31]. For this kind of personalization study, this pattern may be somehow expected as the number of people who fit the grouping criteria may vary depending on the population.

3.2.1 Compensation. Participants took 17.6 minutes on average (median = 15.2 minutes, SD = 7.8 minutes) to complete the main survey, 2.0 minutes on average (median = 1.2 minutes, SD = 2.2 minutes) to complete the first follow-up survey, and 1.9 minutes on average (median = 1.2 minutes, SD = 2.1 minutes) to complete the second follow-up survey.

No compensation was given to participants who failed the first part of the pre-screening survey. Participants who are eligible for the second part of the pre-screening survey received $0.4 for completing this screening survey. Participants who completed the main survey received $1.5 for completing the main survey. Participants received $0.5 for participating in each of the two follow-up surveys. For each of the surveys, an information sheet was first displayed on the survey website for the participants who accepted the task on Prolific and clicked the link of the survey website. Participants who gave consent to participate were then directed to survey questions for each survey. The study was approved by our university's institutional review board (IRB).

3.3 Personalization

To personalize the video content for participants, we used two scales as follows:

1) General Decision Making Style (GDMS) which was designed to assess how individuals approach decision situations [36]. The scale has 5 different decision-making styles: rational, avoidant, intuitive, dependent, and spontaneous. To make our study tractable, we only focused on "dependent" component of this scale. According to this scale, people who have dependent decision-making style often look for advice and direction from others [36]. "Others" can be someone from their social circle or high-status individuals (e.g., experts on the subject matter). In our study context, as high-status individual (i.e., security expert), we selected Kevin Mitnick who recommends using a TOR browser in a Tech Insider video with 3.3M views[2] as the best way to browse anonymously. Obviously, this choice is very subjective. The expert ideally should be someone known by the viewers/users, but finding such an expert may also be challenging. Thus, as an exploratory study, we added a few seconds of Kevin Mitnick video to the video content and only showed this content to those participants who scored high in the formula below based on their ratings of the 5 items of the GDMS-dependent scale.

$$GDMS - Dependent_{score} = \sum_{i=1}^{5} R_i - 3$$

where R_i is the rating for each of the 5 items that participants rated on a scale ranging from Strongly Disagree (1), Disagree to Strongly Agree (5). $GDMS - Dependent_{score}$ gives a measure of whether that person is a dependent decision maker (i.e., influenced by others when making a decision). In this formula, ratings that are either agree (4) or strongly agree (5) get a positive score (+1 or +2, respectively), whereas disagree (2) or strongly disagree (1) is penalized by receiving a negative score (-1 or -2, respectively),

[1] We acknowledge that using a newer version of SEBIS called RSeBIS [35] would be a better option for future studies.

[2] https://www.youtube.com/watch?v=l7KuljR3fJc

	Video				Total
	PMT	PMT+High-social-influence	PMT+High-Tech-savvy	PMT+High-Tech-savvy+High-social-influence	
Control	23	19	31	21	94
Treatment	28	46	10	8	92

Table 1: Number of participants in each of the control and treatment groups.

and neutral (3) does not contribute. Accordingly, the possible score ranges between -10 and +10. A higher score implies that the individual is more inclined to have dependent decision-making style. Although to the best of our knowledge, there is no clear guideline on what the minimum value should be to classify a person as a dependent decision maker, we decided to use a threshold value of +2 to classify the participants into $GDMS - Dependent$ group.

2) IT expertise score: As users often vary widely in knowledge and awareness of security and privacy [5, 19–21], a personalized video targeting that person's level of expertise can be presented to the user to better motivate them when promoting PETs. Towards that, we classified users as low tech-savvy or high-tech savvy using the formula below, and the video contained more technical information (e.g., extra information on the ineffectiveness of private browsing, VPN, and ad blockers in protection against several privacy threats) for participants classified as high-tech savvy. The exact text can also be seen in the transcript of the video with blue color in the Appendix.

$$IT - Expertise_{score} = \mathbf{60} * (quiz_{score}) + \mathbf{30} * (Prior - IT - Experience) + \mathbf{10} * (computer - proficiency)$$

where $quiz_{score}$ represents the number of correct answers (normalized) given by participants to 6 quiz questions (4 of which were adopted from PEW Research's Digital Knowledge Quiz [7]). These questions assess how much participants know about digital topics such as private window, cookies, and ad blockers. The questions can be found in the Appendix. $Prior - IT - Experience$ score indicates whether participants have worked in high-tech job and had formal training in CS or any related technical field. If so, they earned 0.5 for each. $computer - proficiency$ represents participants' self-reported computer proficiency level which was rated on a scale ranging from Novice(1) to Expert(5). The rating was normalized with a minimum value of 0.2 (1/5) and a maximum value of 1 (5/5).

As seen in the formula, the possible $IT - Expertise_{score}$ is between 0 and 100, and the different components are weighted differently. For example, since computer proficiency is self-reported, we assigned a lower weight (10%). On the other hand, a higher weight (60%) was given for their scores in the digital knowledge quiz questions. Also, we decided to use 71 as the threshold value. Our motivation for deciding this threshold value was that even if a user obtains full score in the self-reported proficiency and IT experience parts, they still need to answer more than half of the quiz questions correctly to achieve at least a threshold score.

For example, if a participant answered 5 out of the 6 quiz questions correctly, worked in a high-tech job and rated his/her computer proficiency as proficient (4), the participant's $IT - Expertise_{score}$ would be 73 (60*5/6 + 30*1/2 + 10*4/5). In this case, the participant will be classified as high-tech savvy and the video shown will contain more technical information about a TOR browser.

3.4 Video Design

The video was designed to motivate users to use a TOR browser. The content of the video was inspired by the PMT-based nudge that Story et al. [38] used in their work. Unlike their work, we chose to present the content in video format rather than text format, as there are many studies showing that presenting content in video format is effective in the context of risk communication [4, 10]. We also wanted to increase the adoption rate by personalizing video content for individuals and included some extra content in the video accordingly.

The video first explains the benefits of using a TOR browser, such as to protect oneself from being tracked, surveillance and censored by their internet activities, and the risk of not using a TOR browser, such as being tracked and surveillanced by advertisers, government and ISP providers and why other forms of privacy protection tools like private browsing, VPN and ad blockers cannot provide the same level of protection. This part of the video was the same for all participants.

To personalize video content based on these two scales explained in the previous section, we created four videos which are listed in Table 2. Participants assigned to the treatment group were shown one of these videos based on their score on $GDMS - Dependent_{score}$ and $IT - Expertise_{score}$.

The video for those scored high in $IT - Expertise_{score}$ is more in-depth and explanatory about the existing protection technology. The video for those scored high in $GDMS - Dependent_{score}$ used social influence technique by stating leading security experts recommend using a TOR browser and showing a short video of a security expert "Kevin Micnick" recommending the use of a TOR browser. The next part of the video explains how to install and use a TOR feature in Brave (i.e., self-efficacy). The rest of the video addresses possible misconceptions about using a TOR browser, such as the legality and reputation of being used for illegal activities.

Depending on the content presented in the videos, the duration of the videos ranged between 3:44 minutes to 4:27 minutes. PMT content was included all the videos as a base. Video-4 (High-Tech-savvy, High-social-influence) was the longest that includes both social influence and tech-savvy content in addition to PMT content, while Video-1 was the shortest that only included PMT content. The videos can be watched on YouTube, and links are provided in Table 2. Also, the transcript of each video can be found in the Appendix.

A native English speaker narrated the video transcript. No other sound was included in the videos. All figures and graphics used in the video, except the part where Kevin Mitnick was shown taken from a YouTube video created by Businessinsider channel, were either selected from copyright-free sources (e.g., freepik.com or pexels.com) or created by us.

In the survey, we used a timer feature where participants had to wait at least for the duration of the video they were assigned before

	Self-Explanatory Label	Content	Video Link
Video-1	PMT	PMT	https://youtu.be/w-24OtR_jqk
Video-2	PMT + High-social-influence	PMT + GDMS-Dependent	https://youtu.be/_iix6JtHoBs
Video-3	PMT + High-Tech-savvy	PMT + IT-Expertise	https://youtu.be/tBQWrFgKa-g
Video-4	PMT + High-Tech-savvy + High-social-influence	PMT + GDMS-Dependent + IT-Expertise	https://youtu.be/B1ISwuvNVSU

Table 2: List of four videos used in the study.

answering subsequent questions. On average, participants took 4.85 minutes to watch the videos (median=4.30 minutes, SD=3.26 minutes).

3.5 Survey Data Analysis

3.5.1 Statistical Analysis. To compare the groups to identify similarities or differences in terms of various factors (e.g., demographics), we used Mann-Whitney tests or Kruskal-Wallis (KW) test for our non-normally distributed ordinal data, Chi-square for nominal data (e.g., the adoption rate of the TOR browser in the control and treatment groups). To explore what factors were associated with adopting a TOR browser, we performed a logistic regression where we included multiple related independent variables and reported odds ratios and standard errors.

3.5.2 Reliability of Scales: Before running the regression analysis, we also verified the reliability of our scales using Cronbach's α. The 3-item IUIPS-Control (α = 0.74), the 3-item IUIPS-Awarness (α = 0.67), and the 4-item IUIPS-Collection (α = 0.92) scales had good or minimally acceptable reliability [16]. We also computed PMT-Response Cost by combining the three items about usability of the TOR browser into a single independent variable (α = 0.71).

3.5.3 Coding Methodology for Qualitative Data. To analyze participants' open-ended responses, we used a bottom-up inductive coding approach [28]. Three researchers were involved in the coding process. Initially, two researchers individually went through all the comments of participants to develop themes and codes. After that, two coders along with a third researcher (who was not involved in the initial coding acted as moderator to help reach agreement) met online several times to finalize a codebook, and the same codebook was subsequently used by the two coders. Finally, one of the researchers consolidated the codes and calculated inter-rater reliability (i.e., Krippendorff's alpha) between the two coders using the ReCal OIR software package [11, 13] for each open-ended response. The average Krippendorff alpha for this study is 0.83, which is within reasonable bounds for agreement [23].

4 EVALUATION

4.1 Sample Statistics

4.1.1 Demographics. Out of 186 participants who completed the main survey, 113 (60.8%) were male, 72 (38.7%) female, and 1 (0.05%) were non-binary. The average age was 37.8 years (Median = 35.0, SD = 13.0). 39.8% reported having a 4-year college degree, 16.1% some level of college education, 13.4% Master's degree, 12.9% high school/GED, 12.9% 2-year college degree, 2.2% Professional/Medical degree, 1.6% had a Doctorate degree, 1.1% less than high school. All but 5 participants reported English as their native language.

In terms of self-reported computer proficiency, 48.9% of the participants indicated their level of knowledge about computers in general as proficient, 39.8% as competent, 7.0% as expert, 3.2% as beginner, and 1.1% as novice. 75.8% reported no formal training in CS or any related technical field, and 85.5% never worked in a "high tech" job.

In terms of employment status, 60.8% reported working full-time, 18.3% working part-time, 5.4% retired and the remaining 15.6% were unemployed or unable to work.

We found no significant difference between the control and treatment groups in terms of gender (p = 0.94), age (U = 3892, p = 0.23), level of education (U = 4093, p = 0.51), level of knowledge about computers in general (U = 4229, p = 0.77), GDMS score (U = 4026, p = 0.41), and knowledge score (U = 4091, p = 0.52). Based on our analysis, we concluded that the two groups were similar in terms of their demographics.

4.1.2 The score frequencies of the participants in each condition. We first looked at score distribution of participants in each condition in terms of $IT - Expertise_{score}$ and $GDMS - Dependent_{score}$. Figure 2 shows the distributional of GDMS-Dependent and IT-Expertise scores for each group in the treatment and control groups. We observed that participants' $IT - Expertise_{score}$ were very similar in all the groups except the ones in "PMT+Tech-savvy" (mean=83.7, SD=10) and "PMT+Tech-savvy+Social-influence" (mean=79.7, SD=7.47) groups in the treatment group as the participants assigned to these groups if their scores were higher than the threshold value (i.e., 71). Thus, the others groups can be fairly comparable in terms of $IT - Expertise_{score}$. However, we did not observe the same for $GDMS - Dependent_{score}$.

While participants in "PMT+Social-influence" (mean=4.48, SD=2.4) and "PMT+Tech-savvy+Social-influence"(mean=4.63, SD=2.56) in the treatment groups obtained higher scores, the participants' $GDMS - Dependent_{score}$ in the "PMT" groups in both the control and treatment were significantly different (mean=-1.14 SD=2.41 (control) vs. mean=2.65 SD=4.5 (control), U = 115, p <0.001), making the PMT group in the treatment and control groups hard to compare in terms of $GDMS - Dependent_{score}$. We will discuss the implication of this in the discussion section.

4.2 Initial Reasons for Not Using a TOR Browser

Participants were asked their reasons for not using a TOR browser before watching the video. We received 186 comments and identified 7 common reasons as explained below.

"Not knowing/not being familiar with TOR" was the most common reason reported by participants (49%). This was followed by "Don't see the need to use a TOR browser" (31%, e.g., *I don't access*

any websites that I would need to keep my visits private). 14% of participants pointed out that they are satisfied with their current browsers or features/tools (e.g., VPN or private browsing) such as *"Mostly because I'm satisfied using incognito along with a VPN"*. 9% of participants stated the "Bad reputation of the TOR browser" as the reason for not using the TOR browser because they thought the TOR browser was only used for dark web or illegal activities. For example, comments such as the following demonstrate this sentiment: *"I do not have anything on the dark web I'm interested in viewing."*, *"To me a TOR Browser seems to have a bad reputation and is often looked upon as a device used by people who are involved with illegal activities. I know that sounds a little like a "cloak and dagger" novel but that is what I feel."* Participants were also mentioned "Inconvenience of using a TOR browser" (e.g., slow connection when accessing sites) , "Too much effort to use/setup" (e.g., *"If I remember correctly, it took quite a lot of effort to set up"*) and "using a TOR browser is not safe" (e.g., *"I don't think that it will work and is not that secure."*). A full list of codes can be found in Table 4 in the Appendix.

4.3 Effect of Interventions on Behavior Change: Two Follow-ups

In this section, we present our findings after the follow-up surveys.

4.3.1 First Follow-up. Out of 186 participants who participated in the main survey, 158 participants (85%) completed the first follow-up survey (82 from the control group, 76 from the treatment group).

In the first follow-up survey, a total of 18 participants (11%) reported that they installed a TOR browser on at least one of their devices. However, only 11 of them (7%) reported that they used their TOR browser while browsing online. Of the 11 participants, 6 (7.3%) were from the control and 5 (6.6%) from the treatment group. Using a chi-square test, we found that there was no significant difference in terms of adoption rate among the two groups (p = 0.85).

4.3.2 Second Follow-up. Out of 158 participants who participated in the first follow-up, 149 participants (94%) completed the second follow-up survey (79 from the control group, 70 from the treatment group).

In the second follow-up, a total of 16 participants (10%) reported that they used a TOR browser while browsing online (8 from the control (10%) and 8 (11%) from the treatment group). In particular, among the 11 participants who reported using a TOR browser in the first follow-up survey, 8 continued to use it. However, 1 participant uninstalled it, 1 stopped using it (i.e., still installed), and 1 participant is unknown as he/she did not participate in the second follow-up survey. Among the 7 participants who reported installing but not using a TOR browser in the first follow-up survey, 3 of them started using it. Moreover, 5 participants who reported not installing in the first follow-up survey started using it.

The results showed that the number of participants who used a TOR browser was very low. However, on the bright side, 8/11 (72%) kept using it and 8 participants started using it after the first follow-up survey, so the usage rate slightly increased from 7% (11/158) to 10% (16/149) in the second follow-up survey. The results are depicted in Figure 1.

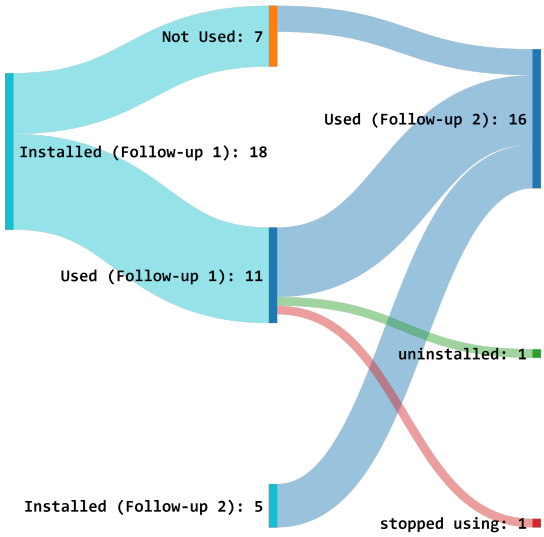

Figure 1: The number of participants who installed/uninstalled or used or stopped using a TOR browser in the two follow-up surveys

To verify whether the participants actually used a TOR browser, we used an API called ipdata[3]. In particular, participants who indicated installing a TOR browser were given a unique link hosted on our survey site to open in their TOR browser, the page checked their IP address and made a query to the API to check it is a TOR. In this way, we verified that 9 out of 16 participants actually installed a TOR browser. The other 7 participants reported either the page was not working, or they installed the TOR browser on another computer. However, we still considered those who did not succeed in our verification process as TOR browser users based on the truthfulness of their statements/comments about the verification process.[4]

4.3.3 Reasons For Choosing to Adopt/Not Adopt a TOR Browser. To understand the rationale behind participants' decisions to adopt or not to adopt a TOR browser, participants were asked to answer the following open-ended questions in the two follow-up surveys. In particular, while participants who installed a TOR browser were asked *"What motivated you to install a TOR browser?"*, participants who chose not to install a TOR browser were asked *"Please explain why you chose not to install a Tor Browser"* as well as *"What might motivate you to start using a TOR Browser?"*. We present the details of each question in detail in the following sections.

4.3.4 Reasons for Installing a TOR Browser. 18 participants in the first follow-up survey and 5 participants in the second follow-up survey stated that they installed a TOR browser. In the first follow-up, we received 18 comments and identified four codes as shown below:

(1) *"Give it a try/curiosity"* with 7 comments (39%),
(2) *"Safety/privacy"* reasons with 5 comments (28%),

[3]https://ipdata.co/
[4]Although the API we use claims to catch most Tor connections, it is not a 100% guarantee as there may be some unofficial exit nodes that are not on the published list https://ipdata.co/blog/tor-detection/.

(3) *"Information in the videos"* with 3 comments (17%),
(4) *"Already had Brave but not aware of the TOR feature"* with 3 comments (17%).

In the second follow-up, we received 6 comments and identified similar codes where *"Give it a try/curiosity"* was mentioned the most (3 comments). A full list of codes can be found in Tables 5 and 6 in the Appendix.

Comments like *"Just to try it out"*, *"It was something new to try out"* and *"just a little curious to see what it was about"* showed that the main motivation to install the TOR browser was due to curiosity and giving it a try. The video seemed to motivate participants by making them curious about the security features and capabilities of the TOR browser for better privacy protection to at least try it.

Some participants also specifically mentioned that they were influenced by the video to install a TOR browser, comments like the following demonstrated this. *"The video describing who could access my data was very motivating."*, and *"The information that I was given made me want to."*.

3 participants also stated that they already had Brave browser installed on their devices, but they did not realize that the Brave browser comes with a TOR feature (i.e., the video seemed to make them aware of this feature). For example, one of the participants provided the following comment: *"I already had Brave installed, I had just never done the TOR browser on it. I've been using Brave for the past four or five years. I didn't realize it could be a TOR Browser, I just thought it was a great browser."*

4.3.5 Reasons for not using after installing a TOR Browser. Of the 23 participants who stated that they installed a TOR browser, 6 of them did not use it. The majority of these participants mentioned that they did not feel the need for using it, which may be due to the low perception of threat severity such as this comment *"I wasn't do any sort of browsing that required to use TOR. None of the websites I visit are sketchy enough to be worth going through a different browser for."*

4.3.6 Reasons for Not Adopting a TOR Browser. Regarding the reason for not installing a TOR browser, we received a total of 140 comments in the first follow-up and 126 comments in the second follow-up surveys. In the first follow-up, we identified the following 8 codes: 1) "No Need", 2) "Forgot", 3) "Too busy", 4) "Other browsers fit my needs", 5) "Need more research", 6) "Work/Job does not allow the usage of TOR", 7) "Inconvenience/need to be logged in", and 8) "I don't feel comfortable/not safe". In the second follow-up, the codes were all the same except for the last code (see Table 7 and 8 in the Appendix).

In the first follow-up, the most common code was "No Need" with 65 comments (46%). Comments like *"There's not a lot that I do on the internet that I'm worried about others knowing."* and *"I have no need to install the [TOR] browser. I do not think I have anything worth hiding from others."* suggest that participants did not worry about security/privacy of their online browsing because they did not think they had data that needed to be kept private or secured while browsing. Comments such as *"I haven't felt like I needed a secondary browser for this reason."* and *"I like using Firefox. And honestly I don't really care as much as I know I should about having extra privacy."* also suggest that the participants did not seem to deem privacy as a major concern for them.

While some of the participants indicated that their current browsers fit their needs (16%), the others used the excuse of being busy (15%) or forgetting about it after the study (14%). For example, participants provided the following comments: *"I like the browser that I currently use and know that programs, extensions and scripts that I use to complete my work are compatible with it."* and *"I honestly forgot about it and Firefox usually fits most of my needs fine."*

Also, 10 participants mentioned about the inconvenience of using a TOR browser or that TOR mode would be troublesome since it is recommended to be used only for non-personal use, not when logging into accounts (this was mentioned in the video). For example, one participant said, *"The hassle of having to switch browsers and also not being able to sign into yours accounts while using a TOR browser put me off."* 5 participants indicated that their job or work may not allow them to use a TOR browser. For instance, participants said *"If my employer caught me with TOR on my laptop, that would be grounds to fire me."* and *"Using a TOR browser would violate the terms of many of the surveys that I complete."*

In the second follow-up survey, we observed that the ranking of the codes was somewhat similar to the first follow-up survey. "No Need" (56%) was again the most common reason, followed by "I forgot", "Too busy" and "Other browsers fit my need", accounting for 42% of comments. Interestingly, the participants who stated the reason for forgetting or being busy still continued to use the same excuse after 1 week (i.e., 2 weeks in a row). This can suggest that, based on the information provided in our study, participants were not willing to make using a TOR browser a top priority, especially if it makes browsing over complex or changes the way they browse the web.

4.3.7 Possible Motivation for Adopting a TOR browser. For participants who chose not to install a TOR browser, we wanted to know what would motivate them to adopt it. For that, we received a total of 140 comments in the first follow-up and 126 comments in the second follow-up. In both follow-ups, we identified 12 codes as shown in Table 9 and 10 in the Appendix. We present the most common themes of both follow-ups below.

In the first follow-up, the most common code was "If I needed more privacy" with 43 comments (30%). Comments like *"If I was doing some sensitive research or looking at stuff that I don't want people to know I looked at"*, *"If my privacy concerns increased"*, and *"If I spent more time and did more things online that made me more conscious of my online activities. Pretty much what I do now are things that I wouldn't be doing on TOR anyway, and the rest of it feels so benign that I don't care who sees."* suggests that these participants had a low perception of threat severity (i.e., they were not concerned about their privacy based on their current browsing habits). There could be two explanations for that. First, their internet usage is very limited and does not require TOR-level security and privacy. Second, they are not aware of the privacy risks of their online browsing habits. The first one is more understandable, but the second one requires effective risk communication to raise their awareness about their browsing activities, which in turn can influence their behavior. Maybe the video was generic for them and did not really address how their certain browsing activities pose a risk for their privacy.

Thus, tailoring motivational material content based on individuals' browsing activities can better motivate such users.

The second most common code was "More explanation" with 21 comments (15%). Comments such as *"If an information PDF was provided that summarized what was told during the video."* and *"Learning more about it and what benefits it would bring to someone like me. It has less of a stigma perhaps."* suggest that participants might be more motivated to install a TOR browser if they had more information about it. Also, some participants pointed out the benefit of providing tangible information such as a PDF with explanations on how to install the TOR browser and how to use it.

The third most common code was "Cannot be motivated" with 21 comments (15%). Some participants stated that nothing would motivate them to install a TOR browser. For example, those participants provided the following comments: *"I really have no interest in using a different browser than the one I currently use."*, and *"Nothing would really motivate me to use the TOR browser and I would actually be scared to be penalized for using it by some of the sites I use for work."*

12 participants (8%) mentioned that they would be motivated to adopt a TOR browser if their data or privacy was breached or more evidence of their personal data being used against them. This shows that these participants had low perceived risk, as they seemed willing to take risks and only take action after an adverse event has occurred. To motivate such participants better, the content of the motivational material could further highlight risk factors.

Also, 6 participants (4%) highlighted the importance of social influence to use a TOR browser. For instance, participants provided the following comments: *"if I hear and see good reviews."*, *"I would feel better if everyone moved to this type of technology before I did it by myself. "*, *"If more people I knew used it and recommended it. "*, and *"recommendations by people I trust."* These indicate that social influence can have an impact on some users' decision-making, and recommendations from trusted people or reviews from other users can be provided to better motivate these users.

In the second follow-up survey, we observed that the top four codes were the same, but the other code ranking was slightly different for certain codes. Additionally, "Reminder/Need more time" was still a theme mentioned by 10 participants (after two weeks of the main survey).

4.3.8 Maintainability of the adopted behavior. In terms of maintaining the adopted behavior, all but one participant indicated "Yes" when asked "Do you plan to continue using it?", and the one participant who said no provided the following comment *"I'll use Brave but not the TOR side of it. Not worth it. I don't think I need the TOR level of security. I have a paid for VPN if I need it."*

Also, 6 participants (37%) reported that they installed a TOR browser on the same day after watching the video in the main survey, and 2 participants indicated that they already installed Brave before participating to our study but were not aware of a TOR feature. Among the participants who used a TOR browser while browsing online, Brave was the most preferred browser (15/16) and 1 participant reported using a TOR browser from the TOR project website after doing his/her own research about TOR browsers.

Overall, participants' experience using the TOR browser was good. 14 (88%) participants rated either somewhat or very satisfied when asked to rate their overall experience with using their TOR browser (mean=4.4, median=4, std=0.48, the scaled ranged from 1 (very unsatisfied) to 5 (very satisfied)). The remaining 2 participants, one of whom did not plan to use it, rated it as neither satisfied nor unsatisfied. This indicates that the usability of the TOR browser was found satisfactory by most participants.

4.4 Likes/Dislikes of the Videos

We asked participants two open-ended questions to describe what they liked and disliked in the video they watched. In response to each of these two questions, we received 186 comments. We organized the comments about the likes into 5 codes and the comments about the dislikes into 6 codes, which are discussed below. A full list of codes can be found on Tables 11 and 12 in the Appendix.

107 comments (58%) mentioned that there was nothing they did not like about the video, and the majority of the participants liked the simplicity and quality of presentation. Comments such as *"I really like the breakdown of all the information. It explained things very well with graphic examples, too."*, and *"I liked that the video wasn't overly wordy when it comes to technical terms, only using technical terms when necessary, which I felt makes it easier to understand how TOR works, and what its purpose is. I also liked the graphics that were used, that showed how TOR works by connecting you to different nodes all over the world, it made the process easier to understand. I also liked that the video explained how TOR should be used, such as highlighting that you shouldn't sign into your accounts since it would defeat the purpose of using TOR."* demonstrate that overall design and presentation of the video content was well received by the majority of the participants, and they appreciated that the video was well done and very informative.

On the other hand, there were some dislikes of the videos (e.g., the narrator's voice is monotonous). For instance, some participants noted that the study/video felt more like an advertisement for the Brave browser and so less believable. *"It was clearly trying to get me to use a specific product (Brave browser) so it seemed more like an ad, which makes the information seem less believable."*, and *"How it suddenly felt like an advertisement for Brave."* This may be because of the video that showed only the Brave browser as an example after introducing the concept of how TOR works. However, some participants perceived it as an advertisement, and it seems to cause a decrease in their trust in the source of information. 2 participants in the control group also pointed out that they did not know who Kevin Mitnick was and questioned the reliability of what he said in the video. They provided the following comments: *"I don't know who Kevin Mitnick is, so I didn't need him telling me to use a TOR. He could be anyone."*, *"Kevin Mitnick's bona fides are not given. I have no idea why I should take anything he says as trustworthy."* Thus, this suggests that careful selection of the social influencer and the fact that the chosen person is a known and trusted expert can be an important factor in increasing the effectiveness of the motivational material.

4.5 Types of devices on which participants used a TOR browser

In the first and second follow-up surveys, we asked participants what types of devices they installed and used a TOR browser on. The question was presented in multiple choice selection format where the options were Smartphone, Tablet, Laptop and Desktop. The

results show that the most common device type participants used a TOR browser was the desktop (50%), followed by laptop (29%), smartphone (11%) and tablet (11%). Two participants also reported using the TOR browser on two of their devices (e.g., smartphone and laptop or desktop and laptop).

4.6 Challenges encountered while using TOR browser

In the first and second follow-up surveys, we asked participants if they encountered any challenges while using their TOR browser. The participants were presented with 3 common challenges, which were identified by Peter et al. [38], and along with none and other options (the question was a multiple choice selections). As shown in Figure 3 (see the Appendix), the majority of the participants (44%: 7/16) did not report any challenges. Among those who had, "websites were extremely slow" was reported by 37% (6/16), "websites asked CAPTCHAS to prove you are not robot" was reported by 19% (3/16), and "websites did not work (i.e., you could not access the site)" was reported by 12% (2/16). Consistent with previous studies [14, 38], the challenge of websites being slow was the most common. One of the participants also provided the following comment on this matter. *"There's definitely some slowdown associated with using the TOR Browser (I wouldn't call sites "extremely" slow though). I also can't really use the browser as a daily driver; it's more of a supplemental tool to my normal web browser."*

4.7 Factors Associated with Using a TOR Browser

Though we did not find any significant differences between the control and treatment group in terms of adoption rate, we wanted to explore what other factors are associated with a TOR browser adoption. Towards that, we trained a binary logistic regression model based on data collected in the main survey and two follow-up surveys. The dependent variable of our model was usage of a TOR browser in the two follow-up surveys, and the model predicts the likelihood of a user adopting a TOR browser based on 20 independent variables (e.g., demographic factors and scales measuring participants' perception on various factors). Table 3 shows all these variables along with odds ratios and p-values denoting which independent variables are strong predictors of participants' adoption decision of a TOR browser. The baselines of categorical independent variables are described in the table caption. Our model fits reasonably well according to the Hosmer and Lemeshow goodness-of-fit test ($\chi^2(132) = 106.88$, $p = 0.95$). We also found no evidence for multicollinearity as all VIFs (variance inflation factors) were less than 10 (mean VIF = 1.73). Overall, the model explained 17.6% of the variance in a TOR browser usage decision (Cox & Snell–R^2 is 0.176). Although all the measures we checked indicates a good fit for the regression model, the power of our analysis may be limited due to the small sample size and low number of participants who adopted a TOR browser. Thus, the results presented below should be interpreted with caution due to the aforementioned concerns.

The model suggests that participants who were more concerned about others observing their web browsing activities (i.e., threat severity) were 2.2x (p=0.019) more likely adopt and use a TOR browser. Additionally, participants who agreed more on efficacy of a TOR browser preventing others from observing their web browsing activity (i.e., response efficacy) were 3.1x (p=0.037) more likely use a TOR browser. We also found that male participants were 4.09x (p=0.045) more likely to use a TOR browser compared to female participants.

5 DISCUSSION

In this study, we assess the effectiveness of using "personalized" content in the form of videos based on a person's decision-making style (i.e., social influence) and the level of IT expertise in terms of adoption rate of a TOR browser. Even though the adoption rate in our study was very low, and the personalized group was not significantly different from the control in terms of adoption rate, we believe that our research approach is a contribution, and our findings are still valuable as they can help other researchers work on this problem and improve the shortcomings we observed in our study. Next, we provide a comparison to the study of Story et al. [38], which is closest to the spirit of our study, along with limitations of our study and design recommendations for future work.

5.1 Comparison to Story et al's TOR Browser Study

Our work is somewhat similar to a recent TOR browser adoption study conducted by Story et al. [38] in terms of survey questions, how the study was conducted, and the PMT content that we used in our videos. We adopted things proven to work (e.g., using PMT-based informational treatment) in their work and wished to further improve the TOR browser adoption rate in their study by personalizing the motivational materiel content. However, the TOR browser adoption rate was vastly different, and the treatment group (who watched personalized videos) in our study did not even reach the same level of adoption as the control group in their study who received only one sentence ("TOR browser is an alternative web browser"). In particular, in our study, the adoption rate for the treatment group after the second follow-up (i.e., two weeks after the main survey) was 11%, while it was 14.9% for their control group and 24.2% for their PMT group after the first follow-up. Even though the two studies showed similarities, there were some differences that we believe contributed to the lower adoption rate and can be used to provide recommendations for future studies.

First, we relaxed one of the screening criteria. While Story et al. [38] recruited participants who expressed a high level of interest in preventing at least one of the privacy threats that the TOR browser can protect against, we lowered this bar to medium level of interest. However, after checking our dataset, we did not find any evidence that this was the mere reason for the low adoption in our study. In particular, we identified 35 participants who did not select "very interested" in any of the threats described in the questions. Among those, 2 participants installed and one of them used a TOR browser. Hypothetically, even if we dropped/did not recruit 35 participants who did not select very interested in any of the questions, the usage rate after the second follow-up would still be 13% (149 - 35 = 114 total sample size, 16 - 1 = 15, number of participants adopted, 15 / 114 = 13%), which is still lower than the adoption rate of their control group (14.9% vs. 11%, yet alone it was 24.2% for their PMT group). This is an interesting observation because we expected

using the video version of their PMT-based informative treatments (even in our control group) to be more effective when promoting TOR browser usage compared to simply motivating them with a sentence. We also expected the video used in our PMT groups (both control and treatment) to be as effective as their text-based nudges, given the fact that several studies showed that videos are a more effective delivery method than text in risk communication [4, 10]. One possible explanation for such difference could be the fact that we verified the majority of participants claiming they were using a TOR browser by having them go to a link on our website using their TOR browser, but Story et al. [38] relied on the self-reported use of a TOR browser. In fact, this limitation was also listed as one of the limitations of their study in their paper. On the other hand, it may have been harder for the participants in our study to lie or just say yes because of the verification step/process. Thus, we recommend the future studies to use a similar validation process to address potential self-reported biases.

5.2 Limitations and Design Recommendation for Future Work

This study has some limitations, and there may be several reasons why we failed to see the impact of personalized video content in increasing the adoption rate compared to non-personalized content.

First, the two scales and their threshold values used for personalizing video content were not validated prior to our study. We do realize that personalizing video content when promoting tools like the TOR browser is not a small endeavor and requires careful and iterative design process to be successful. Thus, future studies should first identify characteristics of users and scales, and then verify which contents/materials are more effective and should be administered for specific individuals. Furthermore, personalization can be done based on users' initial reasons for not using a TOR browser and utilize these reasons in the design of the promotional materials to specifically address their concerns.

Second, the small and unbalanced sample size may have impacted negatively to our results. In particular, after the prescreening surveys, we experienced a high attrition rate about 49% (out of 379 invited participants, 186 of them completed the main survey). This also resulted in very few participants in some of the personalized groups (e.g., there were only 10 and 8 in the "PMT+Tech-savvy" and "PMT+Tech-savvy+Social-influence" groups in the treatment group, respectively). Additionally, in the control group, we randomized the group distribution and expected it to be equally balanced for the factors and scores that were not controlled for group assignment. For example, PMT group in both the treatment and control groups had significantly different score, making it hard to compare in terms of $GDMS - Dependent_{score}$. Thus, having a larger and more balanced sample size (in terms of individual characteristics) in future studies will help elicit the effect of personalized content more clearly.

Third, we decided to promote the Brave browser's TOR mode [22] in this study, rather than the TOR Browser from "The TOR Project" [32]. The Brave browser offers a private window with TOR connectivity and contributes to the TOR network by running TOR relays [32]. We were aware that the TOR feature in Brave may not offer the same level security and privacy as the TOR Browser from the TOR project, which is also acknowledged by Brave (see [6] "If your personal safety depends on remaining anonymous, we highly recommend using TOR Browser instead of Brave TOR windows."). On the other hand, Brave offers better usability as it is like a conventional browser that comes with the TOR feature, especially considering that the TOR browser had various usability issues such as lag while browsing, difficulty in installation and setup etc. [15, 24, 29]. This decision was made so that participants can easily switch from other browsers such as Chrome or Firefox as it would provide participants with three easy levels of privacy that could easily be switched to normal browsing, private browsing, and private browsing with TOR connectivity depending on the site they are accessing. In fact, in our study, several participants who were currently using Brave, but were not aware of the TOR feature in Brave appreciate us for introducing this feature, and overall participants' overall experience using it was also high (mean=4.4 on a scale of 1-5). However, some participants disliked the video and pointed out that study/video felt more like an advertisement for the Brave browser and so less believable and credible. Thus, researchers/practitioners promoting the adoption of PETs such as the TOR browser should introduce the spectrum of tools available and highlight the pros and cons of each and leave it to the users to choose which option they decide. Also, although the video mentioned the use of Brave's normal or private window to log into accounts and the use of TOR for privacy sensitive information, it is possible that some of the participants had impression that the use of TOR and other windows in Brave is exclusive. Future work should explicitly demonstrate the possibility of simultaneous use of TOR and normal or private windows to avoid potential confusion some participants may have.

Finally, while the focus of the study was to evaluate the effect of personalized video content on the adoption of a TOR browser, getting users to watch a video promoting a privacy tool is not yet an easy task, let alone getting some information from users before watching to tailor the content of it. Therefore, more research is needed to identify ways to use videos and personalize their content. One possibility could be implemented in conjunction with promoters such as social influencers on social networks or family and friends who would be personally connected to the potential user [8, 9]. These online promoters would provide the personal credibility and social influence necessary to promote the TOR browser. In this way, users can be directed to a site where a personalized video can be shown after asking a few questions about the user to better motivate the user to adopt it. Furthermore, future work should investigate whether personalized video content based on IT expertise and social influence is effective in increasing adoption of other security and privacy technologies. For example, the effect of material promoting 2FA or password manager used in prior studies (e.g., [2, 4, 10]) can be amplified by personalizing the content and presenting the materials in the most effective way (e.g., text vs. video) for that individual. In particular, a video can be used for those who prefer watching a video over text in addition to dynamically changing the presented material content (e.g., using a social influencer that the user knows and trusts, and aligning the content based on the IT expertise of that individual, and presenting the material based on the person's psychometric traits).

ACKNOWLEDGMENTS

This work was supported by the Central Connecticut State University Faculty & Student Research Grant (No. AFALBR).

REFERENCES

[1] Elham Al Qahtani, Mohamed Shehab, and Abrar Aljohani. 2018. The effectiveness of fear appeals in increasing smartphone locking behavior among Saudi Arabians. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 31–46.

[2] Yusuf Albayram, Mohammad Maifi Hasan Khan, and Michael Fagan. 2017. A study on designing video tutorials for promoting security features: A case study in the context of two-factor authentication (2fa). *International Journal of Human–Computer Interaction* 33, 11 (2017), 927–942.

[3] Yusuf Albayram, Mohammad Maifi Hasan Khan, Theodore Jensen, and Nhan Nguyen. 2017. "... better to use a lock screen than to worry about saving a few seconds of time": Effect of Fear Appeal in the Context of Smartphone Locking Behavior. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*. 49–63.

[4] Yusuf Albayram, John Liu, and Stivi Cangonj. 2021. Comparing the Effectiveness of Text-based and Video-based Delivery in Motivating Users to Adopt a Password Manager. In *European Symposium on Usable Security 2021*. 89–104.

[5] Maria Bada, Angela M Sasse, and Jason RC Nurse. 2019. Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672* (2019).

[6] Brave. 2020. What is a Private Window with Tor Connectivity? Retrieved June 5, 2022 from https://support.brave.com/hc/en-us/articles/360018121491-What-is-a-Private-Window-with-Tor-Connectivity-

[7] PEW RESEARCH CENTER. 2019. Digital Knowledge Quiz. Retrieved June 5, 2022 from https://www.pewresearch.org/internet/quiz/digital-knowledge-quiz/

[8] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A Dabbish, and Jason I Hong. 2014. The effect of social influence on security sensitivity. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. 143–157.

[9] Sauvik Das, Adam DI Kramer, Laura A Dabbish, and Jason I Hong. 2014. Increasing security sensitivity with social proof: A large-scale experimental confirmation. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*. 739–749.

[10] Sanchari Das, Shrirang Mare, and L Jean Camp. 2020. Smart storytelling: Video and text risk communication to increase mfa acceptability. In *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*. IEEE, 153–160.

[11] Ph.D. Deen Freelon. 2020. ReCal2: Reliability for 2 Coders. Retrieved June 10, 2022 from https://http://dfreelon.org/utils/recalfront/recal2/

[12] Serge Egelman and Eyal Peer. 2015. Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. 2873–2882.

[13] Deen Freelon. 2013. ReCal OIR: Ordinal, interval, and ratio intercoder reliability as a web service. *International Journal of Internet Science* 8, 1 (2013).

[14] Kevin Gallagher, Sameer Patil, Brendan Dolan-Gavitt, Damon McCoy, and Nasir Memon. 2018. Peeling the Onion's User Experience Layer: Examining Naturalistic Use of the Tor Browser. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. 1290–1305.

[15] Kevin Gallagher, Sameer Patil, and Nasir Memon. 2017. New Me: Understanding Expert and {Non-Expert} Perceptions and Usage of the Tor Anonymity Network. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. 385–398.

[16] Joseph A Gliem and Rosemary R Gliem. 2003. Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales. In *Midwest Research-to-Practice Conference in Adult, Continuing, and Community Eduction*. Midwest Research-to-Practice Conference in Adult, Continuing, and Community Eduction.

[17] David Harborth, Sebastian Pape, and Kai Rannenberg. 2020. Explaining the Technology Use Behavior of Privacy-Enhancing Technologies: The Case of Tor and JonDonym. *Proc. Priv. Enhancing Technol.* 2020, 2 (2020), 111–128.

[18] Marie Helweg-Larsen and James A Shepperd. 2001. Do moderators of the optimistic bias affect personal or target risk estimates? A review of the literature. *Personality and social psychology review* 5, 1 (2001), 74–95.

[19] Adele E Howe, Indrajit Ray, Mark Roberts, Malgorzata Urbanska, and Zinta Byrne. 2012. The psychology of security for the home computer user. In *2012 IEEE Symposium on Security and Privacy*. IEEE, 209–223.

[20] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "... no one can hack my mind": Comparing Expert and Non-Expert Security Practices. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*. 327–346.

[21] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. {"My} Data Just Goes {Everywhere:"} User Mental Models of the Internet and Implications for Privacy and Security. In *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*. 39–52.

[22] Ben Kero. 2020. Brave.com now has its own Tor Onion Service, providing more users with secure access to Brave. Retrieved June 5, 2022 from https://brave.com/new-onion-service/

[23] Klaus Krippendorff. 2009. Testing the Reliability of Content Analysis Data. *The Content Analysis Reader* (2009), 350–357.

[24] Linda N Lee, David Fifield, Nathan Malkin, Ganesh Iyer, Serge Egelman, and David A Wagner. 2017. A Usability Evaluation of Tor Launcher. *Proc. Priv. Enhancing Technol.* 2017, 3 (2017), 90.

[25] Sarah Lichtenstein, Baruch Fischhoff, and Lawrence D Phillips. 1977. Calibration of probabilities: The state of the art. *Decision making and change in human affairs* (1977), 275–324.

[26] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research* 15, 4 (2004), 336–355.

[27] Nathan Malkin, Arunesh Mathur, Marian Harbach, and Serge Egelman. 2017. Personalized security messaging: Nudges for compliance with browser warnings. In *2nd European Workshop on Usable Security. Internet Society*.

[28] Matthew B Miles and A Michael Huberman. 1994. *Qualitative data analysis: An expanded sourcebook*. SAGE.

[29] Greg Norcie, Jim Blythe, Kelly Caine, and L Jean Camp. 2014. Why Johnny can't blow the whistle: Identifying and reducing usability issues in anonymity systems. In *Proceedings 2014 Workshop on Usable Security. https://doi. org/10.14722/usec*.

[30] Stefan Palan and Christian Schitter. 2018. Prolific. ac—A subject pool for online experiments. *Journal of Behavioral and Experimental Finance* 17 (2018), 22–27.

[31] Eyal Peer, Serge Egelman, Marian Harbach, Nathan Malkin, Arunesh Mathur, and Alisa Frik. 2020. Nudge me right: Personalizing online security nudges to people's decision-making styles. *Computers in Human Behavior* 109 (2020), 106347.

[32] Tor project. 2022. Tor Project. Retrieved June 5, 2022 from https://www.torproject.org/

[33] Leilei Qu, Ruojin Xiao, Cheng Wang, and Wenchang Shi. 2021. Design and Evaluation of CFC-targeted Security Nudges. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–6.

[34] Lee Rainie and Mary Madden. 2015. Americans' privacy strategies post-Snowden. (2015).

[35] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. 2017. Self-confidence trumps knowledge: A cross-cultural study of security behavior. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 2202–2214.

[36] Susanne G Scott and Reginald A Bruce. 1995. Decision-making style: The development and assessment of a new measure. *Educational and psychological measurement* 55, 5 (1995), 818–831.

[37] Peter Story, Daniel Smullen, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2020. From intent to action: Nudging users towards secure mobile payments. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. 379–415.

[38] Peter Story, Daniel Smullen, Rex Chen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2022. Increasing Adoption of Tor Browser Using Informational and Planning Nudges. *Proceedings on Privacy Enhancing Technologies* 2 (2022), 152–183.

[39] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2021. Awareness, adoption, and misconceptions of web privacy tools. *Proceedings on Privacy Enhancing Technologies* 2021, 3 (2021), 308–333.

[40] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. 2020. Examining the adoption and abandonment of security, privacy, and identity theft protection practices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–15.

APPENDIX

5.3 Video transcript

In the text below,
–Text in *Red and italics* represents the extra content shown to participants who were classified as high-tech savvy.
–Text in **Blue and bold** represents the extra content shown to participants who scored high on $GDMS - Dependent_{score}$.

Hello! This video is designed to explain how you can better protect yourself from being tracked, surveillanced and censored by your internet activities. Did you know that many different organizations can gather information about your browsing activities? Here are just a few examples: Advertisers can see which websites

you visit. By tracking your browsing, advertisers can learn about your interests, and they may show you annoying or even embarrassing ads. Every website you visit receives information about you which can be used to infer the city, even neighborhood in which you live. This information can be used by government or organizations to censor or even surveillance your activity. Your internet service provider sees every website you visit, and there are few laws preventing them from selling that information or providing them to the government and there are few laws preventing them from selling that information or providing them to the government. And unfortunately, most browsing tools offer only partial protection against these privacy threats. *For example, Private browsing only partially hides your browsing from advertisers, and does nothing to hide your location from websites or your browsing from your internet service provider or the government. Most VPNs do nothing to hide your browsing from advertisers, many VPNs keep logs which can be accessed by the government, and some VPNs even spy on their users. Ad blockers only partially hide your browsing from advertisers, and do nothing to protect against other privacy threats.*

Thankfully, you can use a TOR browser. TOR is an acronym for "The Onion Router," which is a technology to protect your anonymity and privacy while browsing the internet. Normally without TOR you directly connect to a site like youtube.com. Whereas TOR obscures this connection by adding 3 randomly selected nodes so that your browsing activities go through these 3 nodes contributed by volunteers. Each node is operated independently and chosen randomly each time so none of the nodes know the full traffic. A new path is built randomly every 10 minutes or whenever you start a new TOR session. By using a TOR browser, your browsing will be indistinguishable from the browsing of thousands of other users around the world.

Using a TOR browser is recommended by leading security experts such as Kevin Mitnick. For example, Brave is a browser that offers Tor connectivity in addition to regular web browsing and there are 50 million monthly active Brave users. Brave makes using a TOR browser very easy!! You just need to go to Brave website, download and install Brave just like any other regular browser. If you are switching from other browsers like Chrome or Firefox, moving over to something like Brave will feel the most comfortable. You can enter TOR mode by clicking the menu button and selecting the "New private window with TOR". Once you see the TOR status as connected you can now access the website privately. Under TOR Mode, Brave works just like a regular web browser, with a few key differences: You should not log into accounts such as email, social media, etc. when using a TOR browser. If you log into an account or Google your name, you will reveal your identity which defeats the purpose of being private. So, you should not be using a TOR browser for accessing all the websites, but for non-personal usage or, specific privacy-sensitive activities, such as for viewing sensitive information on Wikipedia or YouTube. For logging into accounts, you can use your regular browser or Brave's normal or private window mode. We also recommend quitting the TOR mode browser periodically, so your browsing patterns do not identify you, since quitting erases your browsing history. There might be some concerns or misconceptions with using a TOR browser. For instance, you might be thinking that TOR browser is only for people who do illegal activities like hackers or criminals. Using a TOR browser in the United States is completely legal, and it is such an important tool in our digital age to hide information and activity that is personal to you, like closing the blinds in your house to keep your privacy from external prying eyes. We hope that this video helped you to realize the importance of being private while surfing online and will encourage you to give TOR browser a shot! Thank you for taking the time to watch this video!

5.4 Survey Items

The following questions were adapted from PEW Research Knowledge Quiz [7].

-**Q1:** Many web browsers offer a feature known as "private browsing" or "incognito mode." If someone opens a webpage on their computer at work using incognito mode, which of the following groups will NOT be able to see their online activities?
• The group that runs their company's internal computer network • Their company's internet service provider • A coworker who uses the same computer • The websites they visit while in private browsing mode • Not sure

-**Q2:** When a website has a privacy policy, it means that the site...
• Has created a contract between itself and its users about how it will use their data • Will not share its users' personal information with third parties • Adheres to federal guidelines about deceptive advertising practices • Does not retain any personally identifying information about its users • Not sure

-**Q3:** If a website uses cookies, it means that the site...
• Can see the content of all the files on the device you are using • Is not a risk to infect your device with a computer virus • Will automatically prompt you to update your web browser software if it is out of date • Can track your visits and activity on the site • Not sure

-**Q4:** What does it mean when a website has "https://" at the beginning of its URL, as opposed to "http://" without the "s"?
• Information entered into the site is encrypted • The content on the site is safe for children • The site is only accessible to people in certain countries • The site has been verified as trustworthy • Not sure

The following questions were also used, but they are not from the above source.

-**Q5:** Which of the following is correct about Ad blockers?
• Ad blockers only partially hide your browsing from advertisers • Ad blockers hide your IP • Ad blockers hide your browsing history from your ISP • Ad blockers hide only inappropriate advertisements • Not sure

-**Q6:** Which of the following is correct if you are accessing a website through a VPN?
• VPNs prevent your ISP from seeing the websites you visit • Your Internet service provider (ISP) cannot see that you are connected to an IP owned by a VPN service • Free VPN companies cannot sell your browsing information • If you log on to an account through VPN, the system administrator cannot correlate your identity and IP address • Not sure

5.5 Figures and Tables

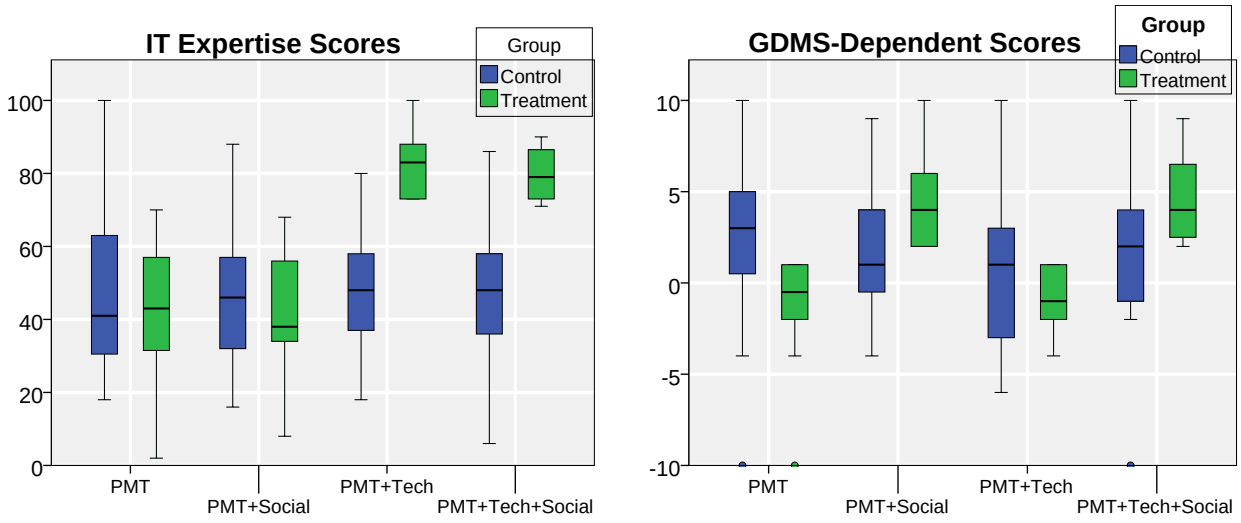

Figure 2: The Box plots showing the distribution of GDMS-Dependent and IT-Expertise scores for each group in the treatment and control groups.

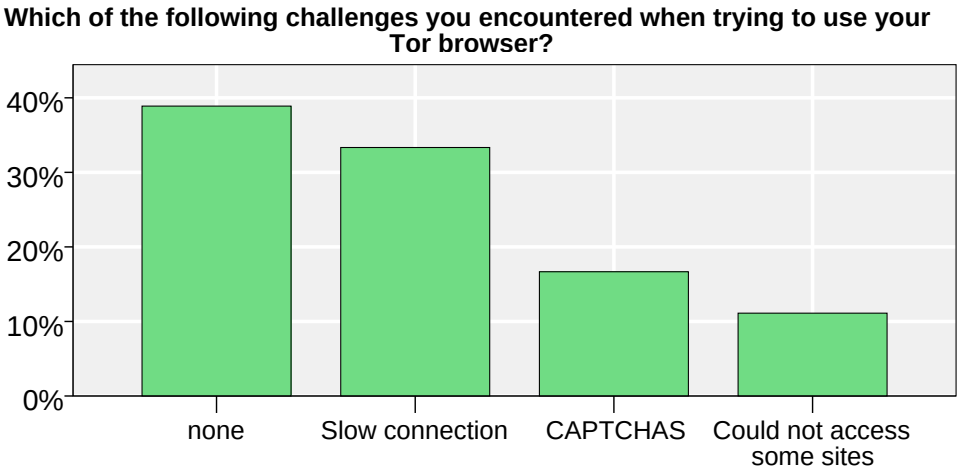

Figure 3: Challenges encountered by participants who used a TOR browser. Multiple selection was possible.

Variables	Odds Ratio	Std. Error	p-value
Treatment vs. Control(base)	1.57	1.55	0.649
Video: Social	1.11	1.31	0.929
Video: Technical	0.61	0.58	0.604
Video: Social & Technical	1.79	2.14	0.625
Age	1.02	0.04	0.623
Male vs. Female(base)	4.09	2.87	0.045*
Education: College or associate degree	0.94	1.07	0.956
Education: Graduate degree	2.05	2.65	0.577
Computer Proficiency	1.18	0.78	0.798
GDMS-score	0.92	0.12	0.541
SEBIS-score	1.89	1.13	0.283
UIUPS-Control	0.91	0.47	0.848
UIUPS-Awareness	0.90	0.65	0.882
UIUPS-Collection	1.10	0.27	0.701
PMT-Perceived Response Cost	1.59	1.11	0.505
PMT-Perception of threat susceptibility	1.58	0.49	0.145
PMT-Perceived threat severity	2.20	0.74	0.019*
PMT-Response efficacy	3.10	1.68	0.037*
Worked in high-tech job	0.78	0.84	0.818
Received formal training in CS	0.68	0.66	0.693
Employment: Working (part/full time)	1.55	1.77	0.698
Employment: Retired	9.81	15.81	0.157
Knows other users of TOR browser	0.30	0.29	0.210
Intercept	< 0.01	< 0.01	0.001**

** $p \leq 0.01$, * $p \leq 0.05$.

Table 3: Coefficients for the binary logistic regressions predicting participants' decision to use a TOR browser in either first or the second follow-up surveys (n=157). The odds ratio for each variable represents the likelihood of binary outcome (i.e., use of a TOR browser) when the variable is increased by one-unit while controlling all other numerical variables at their mean values and categorical variables at their baseline. Std. Errors of coefficients are listed in the second column. Significant variables are shown in bold. Female is the baseline for gender, high school or less is the baseline for education, Not employed is the baseline for employment, the video without technical and social themes is the baseline for video condition. Cox & Snell–R^2 is 0.176.

5.6 Coding Tables

In the tables below, Video-1 represents PMT group, Video-2 represents PMT + High-social-influence, Video-3 represents PMT + High-Tech-savvy, and Video-1 represents PMT + High-Tech-savvy + High-social-influence.

Reason	**Control**				**Treatment**				**Total**
	1	**2**	**3**	**4**	**1**	**2**	**3**	**4**	
Not knowing/not being familiar with TOR	11	6	15	9	19	27	2	2	**91**
Don't see the need to use a TOR browser	9	6	12	6	4	13	6	1	**57**
I use private browsing/VPN/other browsers	3	2	4	5	2	6	2	2	**26**
Bad reputation of the TOR browser	0	2	4	3	1	2	2	3	**17**
Too much effort to use/setup	1	3	3	1	3	2	0	0	**13**
Inconvenience of using a TOR browser	1	0	1	2	2	2	0	0	**8**
Using a TOR browser is not safe	1	1	0	1	0	1	0	1	**5**

Table 4: Codes' frequency of occurrence in participants' responses to: "Why do you choose not to use a TOR browser?". Krippendorf's Alpha: 0.766

Factor	Control				Treatment				Total
	1	2	3	4	1	2	3	4	
Give it a try/Curiosity	2	1	1	3	0	0	0	0	**7**
Safety/Privacy	1	0	1	0	1	1	0	1	**5**
Already had Brave but not aware of the TOR feature	1	0	0	0	0	1	0	1	**3**
Information in the videos	0	0	0	0	1	1	1	0	**3**

Table 5: Codes' frequency of occurrence in participants' responses in the first follow-up to: "What motivated you to install a TOR browser since completing the main survey?". Krippendorf's Alpha: 0.911

Reason	Control				Treatment				Total
	1	2	3	4	1	2	3	4	
Give it a try/Curiosity	0	1	0	0	1	1	0	0	**3**
Already had Brave but not aware of the TOR feature	0	0	1	0	0	0	0	0	**1**
Needed some time to research it	0	0	1	0	0	0	0	0	**1**
The previous iterations of the study (i.e., follow-ups)	0	0	0	0	0	1	0	0	**1**

Table 6: Codes' frequency of occurrence in participants' responses in the second follow-up to: "What motivated you to start using a TOR browser?". Krippendorf's Alpha: 1

Reason	Control				Treatment				Total
	1	2	3	4	1	2	3	4	
No need	7	5	13	9	10	14	5	2	**65**
Other browsers fit my needs	1	2	2	4	2	9	2	1	**23**
Too busy	3	0	4	2	3	7	0	2	**21**
Forgot	2	3	3	2	4	4	0	1	**19**
Need more research	2	3	2	0	4	2	0	0	**13**
Inconvenience/Need to be logged in	0	0	4	2	2	2	0	0	**10**
I don't feel comfortable/not safe	1	1	1	0	0	1	2	0	**6**
Work/Job does not allow the usage of TOR	1	0	2	0	1	1	0	0	**5**

Table 7: Codes' frequency of occurrence in participants' responses in the first follow-up survey to: "Please explain why you chose not to install a TOR browser?". Krippendorf's Alpha: 0.763

Reason	Control				Treatment				Total
	1	2	3	4	1	2	3	4	
No need	8	5	14	10	14	13	4	3	**71**
Forgot	1	2	3	3	4	6	0	0	**19**
Too busy	1	2	1	2	3	6	0	2	**17**
Other browsers fit my needs	1	3	2	4	0	4	2	1	**17**
Work/Job does not allow the usage of TOR	3	1	4	0	2	0	0	0	**10**
Inconvenience/Need to be logged in	0	0	2	2	1	2	0	0	**7**
Need more research	1	0	1	0	0	3	1	0	**6**

Table 8: Codes' frequency of occurrence in participants' responses in the second follow-up survey to: "Please explain why you chose not to install a TOR browser?". Krippendorf's Alpha: 0.801

Reason	Control				Treatment				Total
	1	2	3	4	1	2	3	4	
If I needed more privacy	1	1	8	5	8	15	4	1	**43**
More explanation	4	2	4	1	4	3	1	2	**21**
Cannot be motivated	2	1	8	2	5	2	1	0	**21**
Security/privacy breach	2	1	3	2	2	2	0	0	**12**
Ease of Use	0	0	1	2	0	5	0	2	**10**
Incentives	0	3	1	3	1	1	1	0	**10**
If TOR is more popular/Reviews	2	2	0	0	1	2	1	0	**8**
Need for another computer to use	1	1	3	0	1	1	0	0	**7**
Reminder/Need more time	0	3	1	0	0	2	0	1	**7**
Recommendations from trusted people	2	3	0	0	0	1	0	0	**6**
Other browsers support TOR	0	0	0	1	0	2	0	0	**3**
Involvement in illegal activities	1	0	0	0	0	0	1	0	**2**

Table 9: Codes' frequency of occurrence in participants' responses in the first follow-up survey to: "What might motivate you to start using a TOR browser?". Krippendorf's Alpha: 0.880

Reason	Control				Treatment				Total
	1	2	3	4	1	2	3	4	
If I needed more privacy	2	4	8	6	7	7	6	2	**42**
Cannot be motivated	1	2	7	0	3	3	0	0	**16**
More explanation	2	1	2	1	1	5	0	1	**13**
Security/privacy breach	2	0	3	3	2	3	0	0	**13**
Ease of Use	0	1	1	2	0	5	0	1	**10**
Reminder/Need more time	1	1	1	0	2	4	0	1	**10**
Incentives	0	1	2	3	3	1	0	0	**10**
Need for another computer to use	1	1	3	0	2	0	0	0	**7**
Recommendations from trusted people	2	2	0	1	0	0	0	0	**5**
If TOR is more popular/Reviews	1	1	0	0	0	0	1	0	**3**
Involvement in illegal activities	1	0	0	0	0	0	1	0	**2**
Other browsers support TOR	0	0	1	0	0	1	0	0	**2**

Table 10: Codes' frequency of occurrence in participants' responses in the second follow-up survey to: "What might motivate you to start using a TOR browser?". Krippendorf's Alpha: 0.879

Aspect	Control				Treatment				Total
	1	2	3	4	1	2	3	4	
Good and informative content	15	12	22	10	16	24	8	4	**111**
Easy to follow/Clear Explanation/good pace	11	7	12	10	12	21	4	5	**82**
Visual demonstration/Graphics	4	6	6	2	6	5	1	2	**32**
None	0	0	3	1	2	2	0	0	**8**

Table 11: Codes' frequency of occurrence in participants' responses to: "What aspects of the video did you like?". Krippendorf's Alpha: 0.703

Aspect	Control				Treatment				Total
	1	**2**	**3**	**4**	**1**	**2**	**3**	**4**	
No dislikes	15	9	17	12	19	26	5	4	**107**
Long/boring	3	6	5	1	1	7	0	1	**24**
Needs more examples/explanation needed	2	3	4	1	1	5	2	2	**20**
Skeptical in information	1	0	4	5	3	5	1	0	**19**
Other not capturing video	2	1	0	2	4	3	2	1	**15**
Too technical	1	0	1	0	0	1	0	0	**3**

Table 12: Codes' frequency of occurrence in participants' responses to: "What aspects of the video did you not like?". Krippendorf's Alpha: 0.768