Peter Story*, Daniel Smullen, Rex Chen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh*, and Florian Schaub

Increasing Adoption of Tor Browser Using Informational and Planning Nudges

Abstract: Browsing privacy tools can help people protect their digital privacy. However, tools which provide the strongest protections—such as Tor Browser—have struggled to achieve widespread adoption. This may be due to usability challenges, misconceptions, behavioral biases, or mere lack of awareness. In this study, we test the effectiveness of nudging interventions that encourage the adoption of Tor Browser. First, we test an informational nudge based on *protection motivation theory* (PMT), designed to raise awareness of Tor Browser and help participants form accurate perceptions of it. Next, we add an *action planning* implementation intention, designed to help participants identify opportunities for using Tor Browser. Finally, we add a *coping planning* implementation intention, designed to help participants overcome challenges to using Tor Browser, such as extreme website slowness. We test these nudges in a longitudinal field experiment with 537 participants. We find that our PMT-based intervention increased use of Tor Browser in both the short- and long-term. Our coping planning nudge also increased use of Tor Browser, but only in the week following our intervention. We did not find statistically significant evidence of our action planning nudge increasing use of Tor Browser. Our study contributes to a greater understanding of factors influencing the adoption of Tor Browser, and how nudges might be used to encourage the adoption of Tor Browser and similar privacy enhancing technologies.

Keywords: privacy, technology adoption, nudges, protection motivation theory, implementation intentions, Tor Browser

DOI 10.2478/popets-2022-0032
Received 2021-08-31; revised 2021-12-15; accepted 2021-12-16.

***Corresponding Author: Peter Story:** Department of Computer Science, Clark University, E-mail: PeStory@clarku.edu
Daniel Smullen, Rex Chen, Lorrie Faith Cranor: School of Computer Science, Carnegie Mellon University
Yaxing Yao: Department of Information Systems, University of Maryland, Baltimore County
Alessandro Acquisti: Heinz College of Information Systems and Public Policy, Carnegie Mellon University

1 Introduction

Concerns about digital privacy are widespread [11, 34], and can lead to measurable increases in online self-censorship [48]. Privacy enhancing technologies (PETs) can address those concerns. A substantial number of people are already using some form of PET to protect themselves—for example, ad blockers, private browsing, and VPNs are widely adopted [67]. Unfortunately, these tools are somewhat or completely ineffective against the privacy threats people find most concerning, such as online observation by advertisers [67]. Adoption of tools with stronger protections, such as Tor Browser, lag significantly [67]. Some individuals who could benefit from Tor Browser's protections may not be using it due to misconceptions, behavioral biases, or mere lack of awareness [67]. Furthermore, usability challenges associated with Tor Browser may also inhibit adoption [21, 83]. In either case, *nudging* interventions targeting those different hurdles may help end-users adopt Tor Browser. Nudges are designed to help people align their behavior with their expressed preferences [4].

In this study, we tested combining three types of nudging interventions to increase adoption of Tor Browser. First, we used an informational intervention based on protection motivation theory (PMT) [35, 54, 55], designed to raise awareness of Tor Browser and help people form accurate perceptions of it. In addition, we helped some participants form action planning (AP) implementation intentions [12, 60], to help them identify and take advantage of opportunities to use Tor Browser. Finally, we helped some participants form coping planning (CP) implementation intentions [12, 60], to assist them in overcoming challenges associated with using Tor Browser, such as extreme website slowness. We conducted a longitudinal field experiment to test whether

***Corresponding Author: Norman Sadeh:** School of Computer Science, Carnegie Mellon University, E-mail: sadeh@cs.cmu.edu
Florian Schaub: School of Information, University of Michigan

these nudges would increase adoption in the real world (§ 3). We found that our PMT-based nudge made participants 1.8x more likely to use Tor Browser than those in our control group. Furthermore, our coping-planning nudge made participants who reported encountering challenges using Tor Browser 2.6x more likely to use Tor Browser in the following week. However, we did not find statistically significant evidence of our action planning nudge increasing use of Tor Browser.

In addition to these pre-planned hypothesis tests (§ 4.1), we also conducted several exploratory analyses (§ 4.2-4.8). First, we analyzed the effect of our treatments on participants' perceptions of Tor Browser, to better understand the mechanism of our interventions (§ 4.2). Our nudges affected the factors we targeted, although in two areas participants' perceptions changed in directions we did not expect (i.e., threat susceptibility and threat severity). Next, we analyzed participants' reasons for using or not using Tor Browser (§ 4.3), as well as the activities they used Tor Browser for (§ 4.4). Many participants reported using Tor Browser for its privacy protections, and participants reported using Tor Browser to perform a variety of privacy-sensitive activities, including reading the news, accessing Not Safe For Work content (e.g., pornography), and shopping. We also analyzed the challenges encountered by participants when trying to use Tor Browser (§ 4.5). Participants most commonly reported encountering extremely slow websites and websites not working, two challenges explicitly addressed in our coping plan templates (Figure 5). In addition, we trained a logistic regression model to identify factors associated with using Tor Browser (§ 4.7). We found that the most influential factor was participants' expressed intentions to use Tor Browser. Finally, our long-term follow-up survey showed that our PMT-based nudge increased usage of Tor Browser, even after five weeks had passed since participants saw the nudge (§ 4.8).

Overall, our results suggest that nudges can encourage many people to try using Tor Browser, and that some will continue to use Tor Browser long term. However, obstacles to using Tor Browser remain, showing the value of coping planning nudges and other solutions to help overcome those obstacles.

2 Related Work

First, we discuss the state of web browsing privacy (§ 2.1). We explain how Tor Browser may help people protect their privacy, but that misconceptions about Tor Browser and usability challenges associated with Tor Browser are impediments to greater adoption. Next, we describe how nudges have been used to help people protect their privacy and adopt security technologies (§ 2.2). Finally, we draw on the literature to propose three different nudges which might increase adoption of Tor Browser, which are the subjects of our study (§ 2.3).

2.1 Web Browsing Privacy

Digital privacy is a complex topic, in part due to the many entities involved in common online activities. For example, when a website is loaded in a web browser, the website itself has access to the visitor's IP address, which is often associated with a real-world physical location [80]. Additionally, the website may contain advertisements, which give advertisers visibility into the visitor's activities. Some advertisers are embedded on a significant percentage of popular websites [39], allowing them to fingerprint, profile, and target advertisements to users across websites [15, 38]. Network operators (e.g., internet service providers, employers, or schools) also have visibility into traffic metadata, including the identities of websites visited [28]. Finally, other entities may gain access to information about people's browsing activity through various means. For example, a family member with physical access to one's device may view one's browser history, or law enforcement may acquire information about one's browsing via a subpoena to a website operator [27].

In the face of this complexity, effective and usable privacy tools can help ordinary people protect their privacy. Privacy tools have been developed for a variety of use cases (e.g., messaging [59] and payments [70]), but in this study we focus on private web browsing. Tor Browser [73] is a very effective technology for private web browsing, addressing all the privacy threats we listed above. Other privacy tools, such as ad blockers [39] and private browsing mode [19, 29], are more limited in what protections they provide [67]. Tor Browser is designed to make each users' browsing indistinguishable from the browsing of thousands of other users [71]. Tor Browser provides these protections by routing browsing traffic through the Tor network, and by adding various privacy and security enhancements to the open-source Firefox web browser [49]. However, Tor Browser's strong privacy protections come with a cost to usability, and adoption of Tor Browser is lower than that of other privacy tools [67].

Multiple studies have explored the usability of Tor Browser. Norcie at al. tasked participants with using Tor Browser in a controlled environment, in order to identify usability issues [44]. Several common issues were discovered, such as it being difficult to distinguish Tor Browser from users' regular browsers, and Tor Browser taking a long time to launch. The authors and the Tor Project made changes to address these issues, and a subsequent study showed benefits from many of their changes [44]. Gallagher et al. tasked students with using Tor Browser as their primary browser for one week [21]. The researchers used in-situ questionnaires to gather information about usability issues. Some of these issues can be fixed through technical changes to Tor Browser itself, and we contributed a fix for one such issue [65]. However, Tor Browser users themselves can learn to mitigate other usability issues. For example, if a given website blocks traffic from the Tor network, Tor Browser users can switch to an alternative website. In our study, we test helping users cope with such challenges. Gallagher et al. and Story et al. studied common misconceptions about Tor Browser [22, 67]. For example, some people overestimate Tor Browser's security protections, thinking it can protect them from card fraud. We addressed this and other misconceptions when describing Tor Browser to our participants.

In summary, Tor Browser provides strong privacy protections for web browsing, but associated misconceptions and usability challenges present challenges to broader adoption. As we discuss in the next sections, nudging interventions may help people overcome these obstacles and start using Tor Browser.

2.2 Privacy and Security Nudges

There are many situations in which people's behavior doesn't seem to align with their stated preferences. The privacy paradox is a classic example, in which people expose themselves to privacy risks despite expressing a desire for privacy [23, 61], due to uncertainty about risks, the contextual nature of privacy, and dark patterns promoting overexposure [2, 3]. When properly implemented, behavioral *nudges* are a promising way to help people achieve their stated desires for privacy. Nudges originated in the psychology and behavioral economics literature [69], but have been widely applied to privacy and security [4]. For example, Almuhimedi et al. used nudges to show users the data collection behavior of apps on their smartphones [7, 8]. These nudges encouraged some users to restrict apps' access, and similar nudges are now integrated into the iOS platform [40]. Also, Albayram et al. and Al Qahtani et al. used informational videos to encourage people to enable secure smartphone lock screens [5, 6]. As another example, Story et al. used informational and planning nudges to encourage people to adopt secure mobile payment systems like Apple Pay [66]. Each of these studies used different types of nudges, tailored to the particular scenario. In the next section, we explain the types of nudges we used to encourage adoption of Tor Browser.

2.3 Nudging for Browsing Privacy

We used a nudge based on protection motivation theory (PMT) to motivate participants to use Tor Browser [35, 54, 55]. PMT nudges have been successfully used to increase security-related behavior [5, 6, 66]. PMT suggests that people are most likely to protect themselves when they perceive threats to be severe (*threat severity*), they consider themselves to be at risk (*threat susceptibility*), they feel empowered to take protective actions (*self-efficacy*), they think those actions are likely to be effective (*response efficacy*), and they think the actions' costs are low (*response costs*) [42, 82]. We created an intervention to address these factors of PMT. We designed this intervention to help participants form accurate perceptions of these factors, thereby motivating them to follow their implementation intention plans.

However, successfully protecting one's privacy while using Tor Browser is not as straightforward as simply using Tor Browser for all online tasks. For example, a user might reveal their identity when typing their name into a website or logging into their email account [72]. Thus, Tor Browser provides the most privacy benefits when it is used for particular privacy-sensitive activities that do not require revealing one's identity (e.g., searching for health-related information). It might be challenging to remember to switch from one's default browser to Tor Browser for particular activities. Additionally, people are likely to encounter certain usability issues when using Tor Browser (§ 2.1). Implementation intention nudges [24] could help people remember to use Tor Browser and to overcome challenges associated with using it. Implementation intentions are context-activated plans for achieving some goal. They are often specified in an "if-then" format, where a person performs a certain goal-directed action if they are in a certain situation [45, 57]. The literature suggests that implementation intentions work by helping people recognize opportunities for action [1, 79] and by help-

ing people perform the action automatically when the opportunity arises [13, 32]. Implementation intentions designed to help people overcome anticipated obstacles are referred to as *coping plans* [12, 60]. Implementation intentions concerned with helping people initiate actions without special consideration to obstacles are referred to as *action plans*. We study the effectiveness of using coping plans and action plans to encourage Tor Browser use. Our action plans are designed to help participants remember to use Tor Browser when they perform certain privacy-sensitive activities. Our coping plans are designed to help participants overcome the usability challenges they encounter. Story et al. used action plans to increase adoption of Apple Pay [66], but to the best of our knowledge we are the first to test coping plans in the domain of privacy and security.

3 Method

3.1 Overview

The goal of our study was to test whether nudges based on protection motivation theory (PMT), action planning (AP) implementation intentions, and coping planning (CP) implementation intentions could increase real-world adoption of Tor Browser. In total, we had four treatment conditions: Control, PMT, PMT+AP, and PMT+AP+CP. Comparing use of Tor Browser between the treatment conditions allowed us to see the effects of our interventions. The PMT nudge was designed to motivate participants to use Tor Browser, the action planning nudge to help participants identify opportunities to use Tor Browser, and the coping planning nudge to help participants overcome challenges associated with using Tor Browser (§ 2.3). The literature suggests that implementation intention plans are most effective when people are strongly motivated [41, 58], so we tested our implementation intentions together with our PMT nudge. We administered our coping planning nudge one week after the initial interventions, to give participants time to encounter challenges using Tor Browser. Note that the PMT+AP and PMT+AP+CP conditions did not diverge until Survey 3, so for the purposes of describing them in our protocol and in our data analyses we refer to them as the same condition until that point.

Our study used a longitudinal design because we needed to give participants time to use Tor Browser in their everyday lives. After administering each treatment, we checked back with participants one week later to see whether they had used Tor Browser in the intervening week. A week gave participants time to perform activities they might only do on certain days (e.g., weekends). Each type of nudge was administered only once to each participant. Participants could request a link to their nudges.

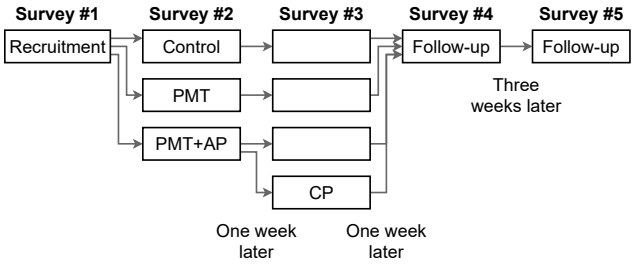

Fig. 1. An overview of the surveys in our study.

Figure 1 shows an overview of the surveys in our study, and complete survey materials are included in Appendix A.1. Next, we describe the contents of each survey in detail.

3.2 Survey Design

Survey 1

We recruited participants from the Prolific crowdsourcing platform [47]. We sought to recruit participants who would be motivated to adopt Tor Browser and who would have the ability to install it on their devices. To identify these participants, we employed a screening survey, Survey 1. To qualify for Survey 1, participants had to live in the United States, speak English, be at least 18 years old, and have a Windows, macOS, or Ubuntu operating-system[1] running on their computer. In Survey 1, we asked about people's use of privacy enhancing technologies, devices, and web browsers. We also asked whether they felt comfortable installing software on their devices and how interested they would be in preventing four threats to their online privacy. Participants had to meet multiple criteria to qualify for our experiment. First, in the past week they must have used either private browsing mode or a VPN, as long as the VPN usage wasn't primarily for work. Second, in the past week they must not have used Tor Browser.

1 Our goal was to measure use of Tor Browser, irrespective of device type. However, we wanted to ensure all participants had devices compatible with Tor Browser. We selected these three operating systems because they were available as prescreening criteria on the Prolific platform.

Third, on multiple days in the past week, they must have used a web browser on a laptop or desktop. Additionally, we asked which devices they had used at least once in the past week, and compared their responses to those about web browser usage; we required their responses to be consistent, and this served as our attention check. Fourth, participants must have indicated that they were generally comfortable installing software on their laptop or desktop. Finally, participants must have indicated they were "Very interested" in preventing at least one of the privacy threats we described. These criteria were designed to help us recruit participants who we thought would be motivated and able to install and use Tor Browser. Based on their responses to Survey 1, we invited all qualifying participants to our experiment. Our experiment began in Survey 2, and continued in Surveys 3 and 4, which we invited participants to one week after they completed the previous survey.

Survey 2

In Survey 2, we randomly assigned participants to our treatment conditions. Those in the control group only saw a short description of Tor Browser: "Tor Browser is an alternative web browser." Those in the PMT treatment were shown a description of privacy threats (Figure 2), the protection offered by Tor Browser (Figure 3), and instructions for installing and using Tor Browser (Figure 16, in appendix). We also addressed common misconceptions (Figure 18, in appendix) and usability issues (Figure 19, in appendix), and offered technical details to those who were interested (Figure 17, in appendix). Participants in the PMT+AP treatment were given the same information as the PMT treatment, but were also given a chance to form an action plan to help them remember to use Tor Browser for privacy-sensitive browsing activities (Figure 4). Note that the fourth treatment, the PMT+AP+CP treatment, did not diverge from the PMT+AP treatment until Survey 3. Finally, we asked demographic questions and questions related to perceptions of Tor Browser and privacy threats.

Many different organizations can gather information about your browsing activity. Here are just a few examples:

- **Advertisers** can see which websites you visit [81]. By tracking your browsing, advertisers can learn about your interests, and they may show you annoying or embarrassing ads
- **Every website you visit** receives information about you which can be used to infer the city or even neighborhood in which you live [46]
- **Your internet service provider** sees every website you visit, and there are few laws preventing them from selling that information [43]
- **The government** can request that companies give them information [26] about your online activities

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 [31], and some VPNs even spy on their users [25]
- **Ad blockers** only partially hide your browsing from advertisers, and do nothing to protect against other privacy threats

Fig. 2. As part of our PMT-based intervention, we informed participants about threats to their browsing privacy. We primarily focused on threat susceptibility, although we also touched on threat severity [42]. In accordance with Story et al.'s recommendations, we addressed well-defined threats and common misconceptions about other tools' protections [67].

Thankfully, there is a tool called **Tor Browser** which is effective at protecting against these kinds of privacy threats. Tor Browser is a web browser which makes web browsing anonymous. It does this by making each user's browsing indistinguishable from the browsing of thousands of other users around the world. If you use Tor Browser correctly, you can be confident your browsing is hidden from advertisers, your internet service provider, and even the government. Tor Browser also hides your location from the websites you visit. Tor Browser is available for free [74] and is simple to use.

Fig. 3. As part of our PMT-based intervention, we informed participants about the protections offered by Tor Browser. In this text, we addressed response efficacy and response cost [42].

Survey 3

We invited participants to Survey 3 one week later. In this survey, we measured whether people set up and used Tor Browser following Survey 2, and whether they encountered any challenges when trying to use it. We also asked those in the PMT+AP and PMT+AP+CP conditions whether they had followed their action plans for using Tor Browser. Those in the PMT+AP+CP condition who reported encountering challenges using Tor Browser were given the opportunity to form a coping plan to overcome the challenges. We included two predefined plan templates corresponding to two challenges

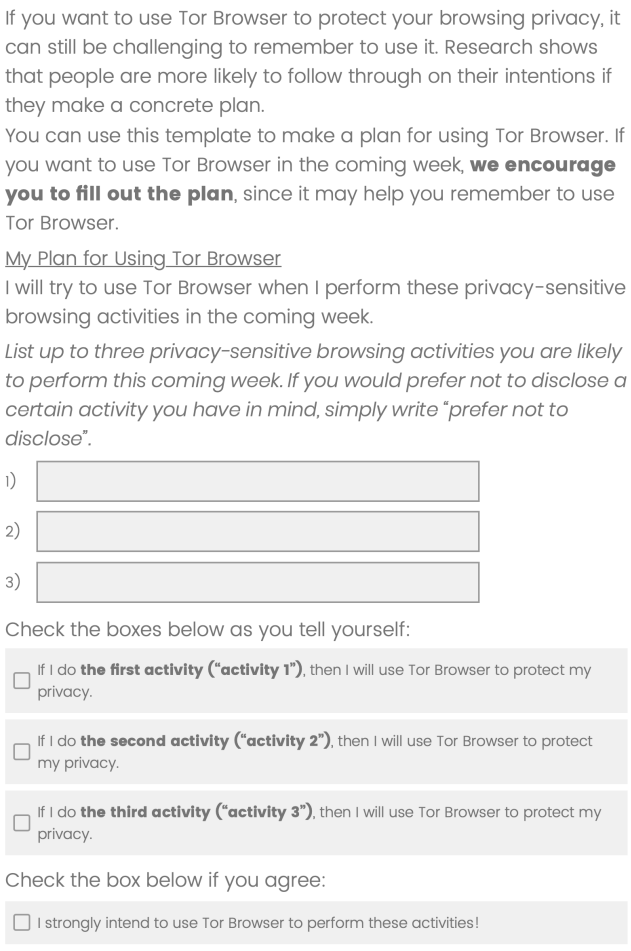

Fig. 4. We encouraged participants in our PMT+AP condition to form an action plan to help themselves use Tor Browser in the coming week. The template is designed to help participants formulate a plan and then mentally rehearse it in an "if-then" format [24, 45, 57]. The template also includes an opportunity for participants to form a strong commitment to their plan [24].

identified by Gallagher et al. [21]. Figure 5 shows our coping plan for participants who reported encountering extremely slow websites, which recommended that participants use the "New Circuit" button to fix this problem. Figure 5 also shows our coping plan for participants who reported encountering websites which didn't work in Tor Browser; in this case, we recommended that participants use alternative websites, and we suggested alternatives for YouTube and Reddit. Both of these challenges were encountered by participants in our pilot study. Finally, Figure 20 in the appendix shows the open-ended template we showed participants who reported encountering other challenges.

Survey 4

One week later, we invited participants to Survey 4. Again, we asked whether participants had set up and used Tor Browser following Survey 3. We also asked again about perceptions of Tor Browser and privacy threats. In addition, we asked those in the PMT+AP and PMT+AP+CP conditions whether they followed their plans, and whether their plans were helpful to them. Finally, we asked whether participants were interested in an optional follow-up survey.

Survey 5

Three weeks after completing Survey 4, we invited participants who had expressed interest to Survey 5. Survey 5 was similar to Survey 4, asking about usage of Tor Browser and Tor Browser-related perceptions.

3.3 Compensation

We estimated survey durations based on the longest treatment (PMT+AP+CP). We estimated Surveys 1, 2, 3, 4, and 5 to take four, eight, six, three, and three minutes, respectively. The median times taken by our participants for each survey were 2.4, 6.8, 2.2, 3.0, and 2.9 minutes, respectively. We aimed to compensate participants at least $12/hour. Thus, we paid $0.80 for Survey 1, $3.50 for successful completion of the experiment, and $1.00 for Survey 5. The actual median rates of compensation were $20.00/hour for Survey 1, $16.48/hour for the experiment, and $20.87/hour for Survey 5. Since our survey questions were time sensitive, we required participants to answer Surveys 2, 3, and 4 within two days of being invited. We allowed up to one week for Survey 5.

3.4 Hypothesis Tests

We pre-planned four one-tailed tests of two independent proportions: First, comparing usage of Tor Browser reported in Survey 3, between the control and PMT groups. Second, comparing usage of Tor Browser reported in Survey 3, between the PMT and PMT+AP groups. Note that this uses data collected before the PMT+AP+CP group diverged from the PMT+AP group. Third, comparing usage of Tor Browser reported in Survey 4, between the PMT+AP and PMT+AP+CP groups. Finally, comparing usage of Tor Browser reported in Survey 4, between the

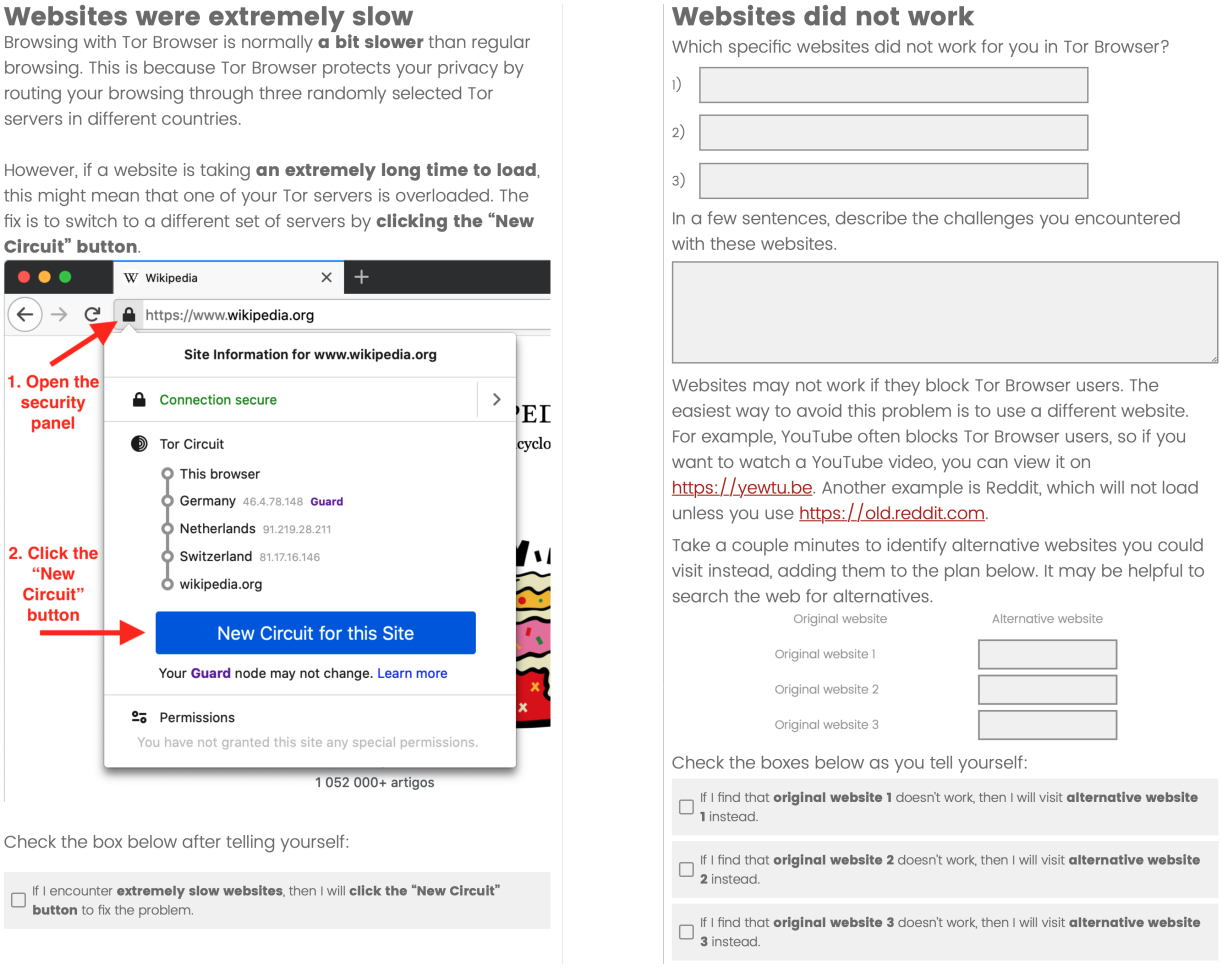

Fig. 5. We encouraged participants in our PMT+AP+CP condition who encountered challenges using Tor Browser to form coping plans to overcome the challenges [12, 60]. The plan on the left was shown to participants who reported encountering extremely slow websites. It explains a possible solution to the problem, and gives participants the opportunity to mentally rehearse the solution in an "if-then" format [24, 45, 57]. The plan on the right was shown to participants who reported encountering websites that did not work. It suggests participants identify alternative websites and visit those if they encounter problems again. Similar to the plan on the left, it also uses an "if-then" format and helps participants mentally rehearse their plan. Note that by the time of publication, the issue with Reddit referenced in the plan appears to have been resolved, and Reddit can now be accessed directly using Tor Browser.

PMT+AP and PMT+AP+CP groups, including only those who reported encountering challenges, since only they were presented with opportunities to form coping plans. Our hypothesis was that each treatment would progressively increase usage of Tor Browser (e.g., that PMT+AP would increase usage to a greater extent than PMT alone).

We conducted a small pilot study (n = 116 completed Survey 1) to test our surveys and to gather data for our power analysis. Based on effect sizes observed in our pilot and budgetary constraints, we determined effect sizes of interest, and used these to determine our sample size. We only describe our power analysis for the final test listed above, since this showed the greatest number of required participants. Our pilot showed that of those in the PMT+AP+CP treatment who reported encountering challenges in Survey 3, 71.4% went on to use Tor Browser in the following week, as reported in Survey 4. Our effect size of interest was 30% (i.e., if 71.4% of those in the PMT+AP+CP treatment use Tor Browser, we want to detect if 41.4% or fewer of those in the PMT+AP treatment use it). This corresponds to $h = 0.62$, a medium to large effect. For 80% power at $\alpha = 0.05$, G*Power showed we need 33 participants in each group. In our pilot, only 28% reported encountering challenges, which suggests that 118 participants are needed in each group in order to have an estimated 33 participants in each group when running the tests.

We pre-registered our protocol on Open Science Framework prior to collecting the data used for our analysis [63, 64].

3.5 Data Collection

We began collecting data in March 2021 and completed collecting data in May 2021. We spread recruitment across multiple days of the week, since participants' behavior might vary by day (e.g., weekday vs weekend). Our goal was for at least 118 participants to complete the experiment in each treatment group. Our pre-registration described weekly recruitment of the *minimum* number of participants needed to replace dropouts. We followed this procedure for two weeks, then used data about our dropout rates to estimate the size of a final batch of replacement participants, sized so that additional batches would not be needed.

Of the 1,870 participants who responded to Survey 1, 689 qualified for our experiment. To ensure high quality data, we reviewed participants' free text responses. We rejected one participant who gave a low-effort response. In total, 537 participants completed our experiment. Of these participants, there were 148 in the control group, 124 in the PMT group, 125 in the PMT+AP group, and 140 in the PMT+AP+CP group.

3.6 Thematic Coding

We analyzed participants' free text responses as part of several exploratory analyses (§ 4.3, § 4.4, and § 4.5) using thematic analysis [14]. For each analysis, the lead annotator began by developing a draft codebook. Next, the lead annotator and another annotator coded a batch of responses from a set of randomly selected participants. Then, the annotators reconciled their codes, and potentially refined the codebook. If they made any changes to the codebook, they reapplied the codes to any earlier batches. The annotators repeated this process until the coding task was complete. The numbers we report in our paper are based on dual-coding, so we have high confidence that we applied our codes consistently.

Comparison	Use of Tor Browser	Odds Ratio	p-value
Control vs PMT	S3: 14.9% vs 24.2%	1.83	**0.026**
PMT vs PMT+AP	S3: 24.2% vs 29.8%	1.33	0.125
PMT+AP vs PMT+AP+CP	S4: 34.4% vs 40.0%	1.27	0.173
Comparison, for those who encountered challenges			
PMT+AP vs PMT+AP+CP	S4: 42.3% vs 65.9%	2.64	**0.027**

Table 1. Our pre-planned tests for the effect of our treatments on participants' self-reported use of Tor Browser. "S3" and "S4" indicate that the Tor Browser usage data came from Surveys 3 and 4, respectively. For odds ratios, 1.5, 2, and 3 are the conventional thresholds for small, medium, and large effect sizes, respectively [68]. Results significant at $\alpha = 0.05$ are bolded.

4 Results

4.1 Effect of Nudges on Use of Tor Browser

To determine the effect of our treatments on participants' use of Tor Browser, we conducted four one-tailed tests of two independent proportions. The results are shown in Table 1. Note that our PMT and action planning (AP) interventions were administered in Survey 2, and our coping planning (CP) intervention was administered in Survey 3. Treatments were layered, such that those in the PMT+AP+CP condition saw all three interventions. Also, in each survey we asked about use of Tor Browser since the previous survey.

The results show that our PMT-based informational treatment made participants 1.8x more likely to report using Tor Browser in the week between Surveys 2 and 3 than those in our control condition ($p = 0.026$). Our action planning intervention did not significantly increase use of Tor Browser relative to the PMT-only treatment ($p = 0.125$). For participants who reported encountering challenges using Tor Browser, our coping planning intervention made them 2.6x more likely to report using Tor Browser in the following week ($p = 0.027$). When all participants are analyzed, we do not see a significant effect from our coping planning intervention ($p = 0.173$), which is unsurprising since only those who reported encountering challenges were given the opportunity to form coping plans. In summary, we have statistically significant evidence of a small effect from our PMT-based intervention and a medium effect from our coping planning intervention.

Survey	Variable	p-value	ϵ^2
2	Perception of threat susceptibility	**0.001**	0.027
2	Perception of threat severity	**0.008**	0.018
2	Perception of self-efficacy	**<0.001**	0.041
2	Perception of response efficacy	**<0.001**	0.030
2	Knowledge of how to use Tor Browser	**<0.001**	0.217
2	Expressed intention to use Tor Browser	**<0.001**	0.117
3	Expressed intention to use Tor Browser	**0.001**	0.032
4	Expressed intention to use Tor Browser	0.142	0.010
4	Perception of threat susceptibility	0.661	0.003
4	Perception of threat severity	**0.035**	0.016
4	Perception of self-efficacy	0.490	0.005
4	Perception of response efficacy	0.179	0.009
4	Knowledge of how to use Tor Browser	**<0.001**	0.033
4	Perception of privacy control	0.874	0.001

Table 2. The results of Kruskal-Wallis tests measuring whether these variables differed between our treatment groups. The survey numbers in which the data were collected are shown in the leftmost column. p-values significant at $\alpha = 0.05$ are bolded, representing tests where the null hypothesis was rejected. Effect sizes are estimated as ϵ^2 values where 0.01, 0.08, and 0.26 are conventional thresholds for small, medium, and large effect sizes, respectively [36, 78].

4.2 Perceptions of Tor Browser

We were also interested in the effect of our interventions on participants' perceptions of Tor Browser. We asked about participants' perceptions using Likert scale questions. We analyzed these questions using Kruskal-Wallis tests, testing whether perceptions differed between our treatment groups. The results of our tests are shown in Table 2. For the significant results, we performed pairwise comparisons between the treatment groups using Dunn post-hoc tests, employing the Holm-Bonferroni method to control for Type I error.

The results suggest that our interventions affected participants' perceptions. In Survey 2, after administering the PMT and action plan nudges, the following factors differed significantly between our treatment groups: threat susceptibility (Figure 6), threat severity (Figure 7), self-efficacy (Figure 8), response efficacy (Figure 9), self-reported knowledge of how to use Tor Browser (Figure 10), and intentions to use Tor Browser (Figure 11). In Survey 3, we administered the coping plan nudge and we only asked again about expressed intention to use, finding it still to be significant (Figure 12). In Survey 4, we asked again about all these variables at the end of our experiment. In Survey 4, only changes to threat severity (Figure 13) and knowledge of Tor Browser (Figure 14) remained significant. Graphs of non-significant results are shown in Figures 21-25 in the appendix.

As expected, the results show that our PMT intervention increased perceptions of self-efficacy, response efficacy, knowledge of how to use Tor Browser, and intention to use Tor Browser. Surprisingly, our action planning nudge appeared to negate the increase in perceptions of threat susceptibility from our PMT nudge (Figure 6). Perhaps our participants' plans to use Tor Browser made them feel more protected against online observation. We further discuss this in our limitations section (§ 5). Also, our PMT nudge reduced perceptions of threat severity (Figure 7). This might be because our descriptions of privacy threats did not emphasize the most severe possibilities (Figure 2), and perhaps participants' fears in the abstract are greater than those pertaining to the threats we described. This is not necessarily a problem, since our PMT-based nudge is designed to help participants form accurate perceptions of threats and protective responses, rather than to motivate participants to the greatest extent possible (e.g., by exaggerating threats). It is notable that by Survey 4, we no longer observe significant differences in intention to use Tor Browser or in perceptions of threat susceptibility, self-efficacy, or response efficacy. This suggests that some of our nudges' effects diminish over time, but as we discuss in Section 4.8, our Survey 5 data suggest that use of Tor Browser may persist long-term. We did not ask about perceptions of privacy control in Survey 2; since we do not see differences in Survey 4, it is unclear whether our nudges ever had an effect on these perceptions (further discussed in § 5).

4.3 Why Do or Don't People Use Tor Browser?

At multiple points throughout our study, we asked participants about their reasons for either installing or using Tor Browser, or for not doing so. We collected multiple responses from all 537 participants who completed our experiment. We coded these responses to identify common themes, stopping after reaching code saturation. In total, we coded 558 free text responses from 150 randomly selected participants. Table 6 in the appendix shows our codebook.

Participants most commonly explained that they used or installed Tor Browser because they wanted to test it out. For example, P33 wrote that they installed Tor Browser "To try it out, to see if I would like using it." Participants also commonly mentioned the Tor Browser's privacy protections. For example, P90 used Tor Browser "because I did not want my browsing to

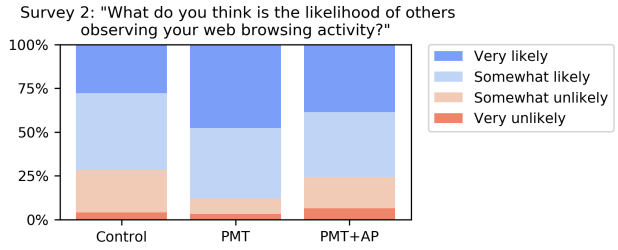

Fig. 6. This question measured perceptions of threat susceptibility. Our PMT nudge increased perceptions of threat susceptibility, but our action planning nudge appears to negate this increase. Post-hoc tests: **Control vs PMT, p<0.001**; Control vs PMT+AP, p=0.072; **PMT vs PMT+AP, p=0.023**.

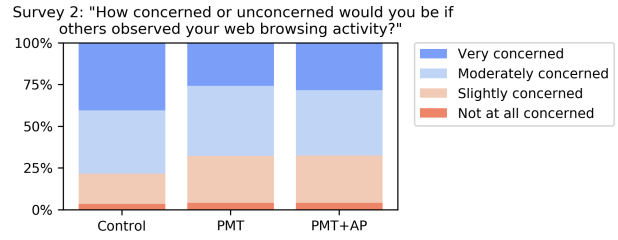

Fig. 7. The question measured perceptions of threat severity. Our PMT nudge reduced perceptions of threat severity. Post-hoc tests: **Control vs PMT, p=0.017**; **Control vs PMT+AP, p=0.014**; PMT vs PMT+AP, p=0.788.

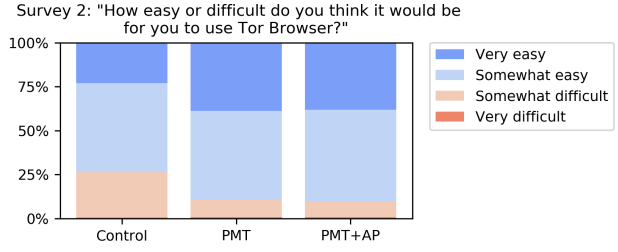

Fig. 8. This question measured perceptions of self-efficacy. Our PMT nudge increased perceptions of self-efficacy. Post-hoc tests: **Control vs PMT, p<0.001**; **Control vs PMT+AP, p<0.001**; PMT vs PMT+AP, p=0.991.

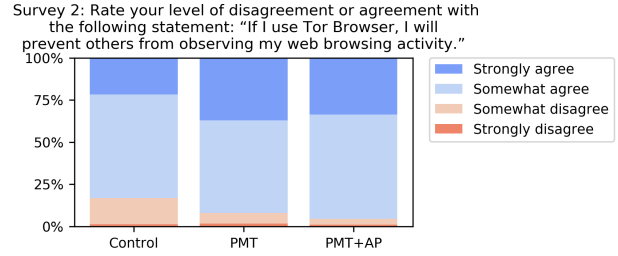

Fig. 9. This question measured perceptions of response efficacy. Our PMT nudge increased perceptions of response efficacy. Post-hoc tests: **Control vs PMT, p=0.002**; **Control vs PMT+AP, p=0.001**; PMT vs PMT+AP, p=0.887.

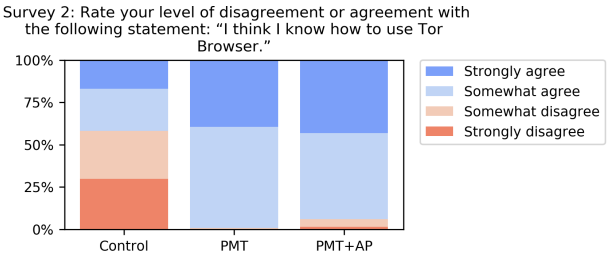

Fig. 10. This question measured self-reported knowledge of how to use Tor Browser. Our PMT nudge increased knowledge of how to use Tor Browser. Post-hoc tests: **Control vs PMT, p<0.001**; **Control vs PMT+AP, p<0.001**; PMT vs PMT+AP, p=0.947.

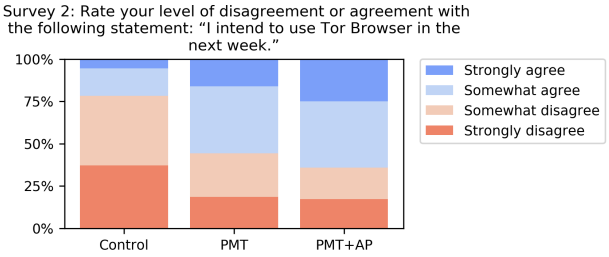

Fig. 11. This question measured intention to use Tor Browser. Our PMT nudge increased intentions to use Tor Browser. Post-hoc tests: **Control vs PMT, p<0.001**; **Control vs PMT+AP, p<0.001**; PMT vs PMT+AP, p=0.096.

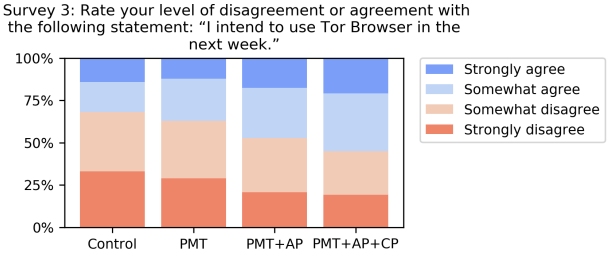

Fig. 12. In Survey 3, we asked again about intention to use Tor Browser. Post-hoc tests: Control vs PMT, p=0.652; **Control vs PMT+AP, p=0.039**; **Control vs PMT+AP+CP, p=0.001**; PMT vs PMT+AP, p=0.200; **PMT vs PMT+AP+CP, p=0.021**; PMT+AP vs PMT+AP+CP, p=0.652.

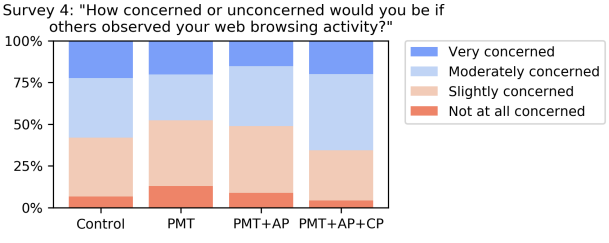

Fig. 13. At the end of the experiment, we asked again about perceptions of threat severity. Although the Kruskal-Wallis test was significant, no post-hoc tests were significant at $\alpha = 0.05$.

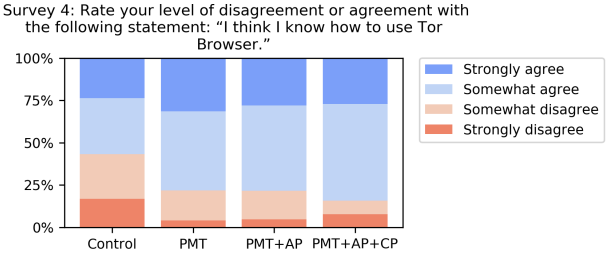

Fig. 14. At the end of the experiment, we asked again about self-reported knowledge of how to use Tor Browser. Our PMT nudge increased self-reported knowledge of how to use Tor Browser, and this persisted to the end of our experiment. Post-hoc tests: **Control vs PMT, p=0.003**; **Control vs PMT+AP, p=0.008**; **Control vs PMT+AP+CP, p=0.002**; PMT vs PMT+AP, p=1.000; PMT vs PMT+AP+CP, p=1.000; PMT+AP vs PMT+AP+CP, p=1.000.

affect my history or be available to my ISP." Similarly, P62 explained that they used Tor Browser "to keep my browsing of adult oriented websites private. If nothing I am doing is illegal [then] the government can keep their nose out of it." Participants also cited our study as an influence on their behavior. For example, P76 installed Tor Browser because "I was interested in trying it, particularly after reading the information provided across the first few surveys on this topic." Also, P42 explained that they wanted to test their coping plan, writing that they used Tor Browser "To check and see if your tip for faster loading speeds by clicking on lock and clicking on 'New Circuit for this Site' works. It was a definite help with faster loading speeds."

Participants gave different reasons for not installing or using Tor Browser as well. Most commonly, participants explained that they did not need Tor Browser. For example, participants gave answers such as "I don't need it" (P15), "I have no use for it" (P100), and "I did not need any extra internet privacy" (P149). This is notable, because we intentionally recruited participants who we thought would be highly motivated to use Tor Browser – recruitment required that participants were recent users of either private browsing or a VPN, and "very interested" in preventing at least one privacy threat we described. It was also common for participants to cite busyness or forgetfulness as reasons for not using Tor Browser. For example, P120 explained that "I forgot to be honest, it's been a busy week."

4.4 What Activities Do People Use Tor Browser For?

In Survey 2, we gave the 265 participants in our PMT+AP treatment group the opportunity to form action plans to use Tor Browser. In their action plans, we invited participants to list privacy-sensitive activities they might perform using Tor Browser. Of these 265 participants, 231 wrote at least one activity in the supplied plan template. In total, participants wrote 598 activities, which we coded to identify common themes. Our codebook is shown in Table 7 in the appendix.

First, we note that in 192 cases, participants indicated that they preferred not to disclose details of activities. In these cases, there is no way to determine whether or not the participant actually had an activity in mind. If the participant did have an activity in mind, there is no way to determine the type of activity. This must be considered when interpreting the prevalence of the other themes we discovered, since participants may be less likely to disclose particularly sensitive browsing activities. The next most common theme was online shopping, which applied to 55 activities. For example, P497 wrote that they planned to use Tor Browser for "browsing Amazon to prevent following advertisements." This appears consistent with Mani et al.'s finding that traffic to www.amazon.com accounts for a large percent of Tor network traffic [37]. Other common activities included those related to finance, the news, Not Safe For Work content (e.g., pornography), and medical topics. Watching videos and accessing YouTube were also commonly described.

When we followed up over the course of the experiment, overall we found that participants reported performing 407 of the 598 activities they described (68.1%). Furthermore, of the 407 activities they performed, participants reported using Tor Browser for 180 of these activities (44.2%). Table 7 in the appendix includes a breakdown of which types of activities participants performed and which they used Tor Browser for. Tor Browser was used in at least some cases for nearly all the types of activities participants described.

4.5 What Challenges Do People Encounter When Trying to Use Tor Browser?

In Survey 3, we asked the 244 participants who reported having ever used or tried to use Tor Browser whether they had encountered any challenges doing so. Partici-

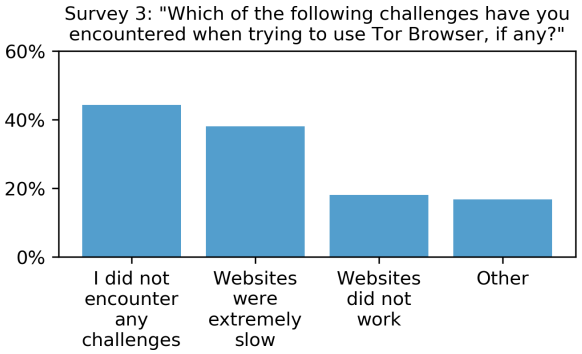

Fig. 15. Challenges encountered by participants trying to use Tor Browser. Note that participants could select multiple challenges. We coded participants' explanations of their "Other" challenges

pants could indicate that they had not encountered any challenges, select a predefined challenge (i.e., "Websites were extremely slow" or "Websites did not work"), or describe an "Other" challenge. The two predefined challenges were identified by Gallagher et al. [21], and we also observed them in our own pilot study. As shown in Figure 15, the majority of participants reported encountering some form of challenge. Additionally, 41 participants described an "Other" challenge. We coded these responses to identify common themes. Our codebook is shown in Table 8 in the appendix. The challenges of websites being slow or not working were common in both participants' multiple choice selections (Figure 15) and in their free text responses (Table 8 in the appendix). This suggests that our coping plan templates (Figure 5) did address participants' greatest challenges. Our findings are also consistent with prior work [21].

4.6 Did Participants Form and Follow Coping Plans?

Of the 138 participants who reported encountering challenges, 44 were in our PMT+AP+CP treatment, and so were offered the opportunity to form a coping plan to address their greatest challenge. 26 completed the "Websites were extremely slow" template, in which we explained how to use the "New Circuit" button. Of these participants, 13 reported clicking the "New Circuit" button when we asked the following week. Two participants completed the "Websites did not work" template. One participant planned to use "Old Reddit" to access Reddit, and the other planned to use Facebook's onion service to access Facebook. When we followed up one week later, the first participant reported successfully using "Old Reddit" in Tor Browser, while the other participant reported not accessing Facebook in the previous week. Finally, 12 participants completed the "Other challenges" template. Participants supplied a diverse set of responses, such as adjusting their mindset, conducting additional research, and employing external tools (e.g., a third-party password manager). We did not think it would be helpful to code such a small number of diverse responses, so we have simply included them all in Table 9 in the appendix. Among these responses, only four participants reported following their plans to overcome "Other challenges."

Our study design did not allow us to directly measure the efficacy of participants' coping plans for overcoming challenges (i.e., because we did not instrument participants' devices). However, we did collect free text responses about perceived helpfulness of the plans. Several participants confirmed that their coping plans helped them overcome the challenges they encountered. For example, P33 wrote: "Using the regular reddit web address didn't work but old reddit did." Also, P42 wrote: "Clicking on 'New Circuit for this Site' works. It was a definite help with faster loading speeds."

4.7 What Factors Are Associated with Using Tor Browser?

Our pre-registered hypothesis tests showed the effect of our treatments on adoption of Tor Browser (§ 4.1). However, we were interested in whether other factors might also influence adoption. Thus, we trained a logistic regression model containing our treatments, demographic factors, and perceptions of Tor Browser. Our model's outcome variable was usage of Tor Browser in either Survey 3 or Survey 4. Our model contains the 20 explanatory variables shown in Table 3. Note that for gender, "Female" is the baseline; for income, "Less than $10,000" is the baseline; for employment, "Working (paid employee)" is the baseline; for education, high school or less is the baseline; for living situation, living alone is the baseline; and for treatment, the control group is the baseline. Also, we included an interaction effect between the "encountered a challenge" factor and the PMT+AP+CP treatment, because our pre-registered hypothesis tests found evidence of this interaction. We encoded our Likert scale questions as binary variables (e.g., "Strongly disagree" and "Somewhat disagree" as 0, "Somewhat agree" and "Strongly agree" as 1). We excluded 18 participants who supplied incomplete demographic information, leaving us with 519 participants to train our model. The Hosmer and

Variable	p-value	e^β
Age	0.593	0.991
Non-female	*0.068*	1.723
Income: $10,000 - $19,999	0.293	0.363
Income: $20,000 - $39,999	0.573	1.616
Income: $40,000 - $59,999	0.892	0.891
Income: $60,000 - $79,999	0.330	0.431
Income: $80,000 - $99,999	0.348	0.440
Income: $100,000 or more	0.645	0.673
Employment: Self-employed	*0.067*	0.384
Employment: Student	0.688	1.220
Employment: Not employed	0.346	0.641
Employment: Retired	0.180	3.483
Education: College or associate degree	0.441	1.303
Education: Graduate degree	0.721	0.859
Computer-related background	0.350	1.283
Living with: Domestic partner	0.338	1.370
Living with: Children	0.449	1.272
Living with: Parents	0.237	0.617
Living with: Other family	0.105	2.043
Living with: Roommates	0.761	1.204
Previously heard of Tor Browser	0.731	1.118
Previously used Tor Browser	0.256	1.490
Knows other users of Tor Browser	0.543	1.220
Installed prior to the study	*0.094*	1.978
S1: Perception of privacy control	0.242	1.348
S2: Perception of threat severity	0.110	1.599
S2: Perception of threat susceptibility	0.322	1.384
S2: Perception of response efficacy	0.307	1.649
S2: Perception of self-efficacy	0.330	1.544
S2: Knowledge of how to use Tor Browser	0.239	1.725
S2: Intention to use Tor Browser	**<0.001**	20.666
S3: Encountered a challenge	0.516	1.249
Treatment: PMT	**0.015**	0.343
Treatment: PMT+AP	**0.013**	0.327
Treatment: PMT+AP+CP	**0.010**	0.284
Treatment: PMT+AP+CP × Challenge	*0.051*	3.298
Constant	**0.001**	0.015

Table 3. Our logistic regression model for predicting use of Tor Browser in either Survey 3 or Survey 4. e^β indicates the change in odds of using the tool for a one unit change in the variable (or when the variable is true). p-values significant at $\alpha = 0.05$ are bolded. p-values significant at $\alpha = 0.10$ are italicized.

	Use of Tor Browser			
Treatment	**In S3**	**In S4**	**In S5**	**Overall**
Control	14.7%	24.3%	15.4%	28.7%
PMT	26.4%	29.1%	27.3%	43.6%
PMT+AP	29.8%	33.0%	32.2%	43.5%
PMT+AP+CP		41.5%	29.2%	49.2%
	Use of Tor Browser, by those who encountered challenges			
Treatment	**In S3**	**In S4**	**In S5**	**Overall**
Control	24.2%	33.3%	15.2%	42.4%
PMT	50.0%	42.9%	35.7%	60.7%
PMT+AP	56.5%	42.9%	47.6%	71.4%
PMT+AP+CP		68.3%	41.5%	78.0%

Table 4. Use of Tor Browser across our study. Note that this table only includes the 491 participants who completed Survey 5, our long-term follow-up survey. Of these participants, 123 reported encountering challenges using Tor Browser. In Surveys 3 and 4, we asked participants whether they had used Tor Browser since the previous survey. Since Survey 5 was sent three weeks after Survey 4, in Survey 5 we instead asked whether participants had used Tor Browser in the past week. The "Overall" column shows the percent of participants who reported using Tor Browser at any time during the study.

Lemeshow goodness of fit test did not find evidence of poor model fit ($p = 0.631$). We did not find evidence of multicollinearity, as all VIFs were less than 10. Our model explains approximately 37.8% of the variance in Tor Browser usage (Cox and Snell $R^2 = 0.378$).

Our model suggests that the most influential predictor of Tor Browser use is intention to use Tor Browser; participants who indicated intention to use Tor Browser in the coming week were 21x more likely to use Tor Browser than those who didn't. The model also suggests that when other factors are controlled for, our treatments make participants *less likely* to adopt Tor Browser than the control condition. However, our earlier tests show that our treatments increased intention to use and actual use of Tor Browser (Figure 11 and § 4.1). Thus, these results simply show that those who intended to use Tor Browser despite being in the control group were even more likely to use it than those we nudged who then expressed intentions to use it.

We have several results which are not significant at $\alpha = 0.05$, but would be significant at $\alpha = 0.10$. First, the model suggests that those in the PMT+AP+CP treatment who encountered a challenge (i.e., who were given opportunities to form coping plans) were 3.3x more likely to use Tor Browser than those in the control group who did not encounter challenges. Next, the model suggests that those who are self-employed may be less likely to adopt Tor Browser. Finally, the model suggests that non-females and those who installed Tor Browser prior to the study may be more likely to use it.

4.8 Will Participants Become Long-term Users of Tor Browser?

We found that our PMT and coping planning nudges increased use of Tor Browser in Surveys 3 and 4, respectively (§ 4.1). However, our exploratory analyses suggest that some of our nudges' effects on participants' perceptions fade over time (§ 4.2). In Survey 5, we collected Tor Browser usage data three weeks after Survey 4, so this data may reveal whether the effects of our treat-

Comparison	Use of Tor Browser	Odds Ratio	p-value
CONTROL vs PMT	S5: 15.4% vs 27.3%	2.05	**0.011**
PMT vs PMT+AP	S5: 27.3% vs 32.2%	1.26	0.211
PMT+AP vs PMT+AP+CP	S5: 32.2% vs 29.2%	0.87	0.691
Comparison, for those who encountered challenges			
PMT+AP vs PMT+AP+CP	S5: 47.6% vs 41.5%	0.78	0.678

Table 5. One-tailed tests of two independent proportions, run on our Survey 5 data. Results significant at $\alpha = 0.05$ are bolded.

ments persist over time. Table 4 summarizes use of Tor Browser across our study.

We reran our hypothesis tests on our Survey 5 data, and the results are shown in Table 5. Weeks after our interventions, the difference between the Control and PMT conditions remains statistically significant ($p = 0.011$), with an effect size similar to what we observed in Survey 3 (Table 1). This suggests that our PMT intervention contributes to long-term adoption of Tor Browser. However, we no longer find our coping planning intervention to significantly increase use of Tor Browser. Although our coping planning intervention temporarily increased adoption of Tor Browser in Survey 4 (Table 1), we do not have evidence that it increases long-term use of Tor Browser. One possibility is that between Surveys 3 and 4, these participants used Tor Browser to test their coping plans; after testing their coping plans, they may not have continued using Tor Browser at higher rates. It is possible their coping plans benefited them in ways that are not reflected in these numbers (e.g., using Tor Browser with the same frequency, but Tor Browser being more pleasant to use).

5 Limitations

Our recruitment method and qualification criteria limit the generalizability of our findings (§ 3.2). For example, our results would likely differ if we recruited from countries where access to Tor Browser is restricted, or if we recruited less tech-savvy participants [53].

A limitation of our study design is that we rely on self-reported use of Tor Browser, making us reliant on participants' honesty and memory. We mitigated this limitation by reassuring participants that it was optional to use Tor Browser. Also, in most cases, we only required participants to recall their behavior in the past week. We considered an alternative design in which we would monitor participants' behavior using an instrumented Tor Browser. However, awareness of our observation might alter participants' behavior, and browser instrumentation might not capture use of Tor Browser across multiple devices.

Dropout in our study was higher than in other studies we have conducted, but we have no evidence to suggest that this negatively impacted our results. Of the 689 people we invited to participate in our experiment, 77.9% completed our entire experimental protocol (i.e., Survey 2, Survey 3, and Survey 4). We lost 6.4%, 9.6%, and 7.9% of participants between Surveys 1 and 2, Surveys 2 and 3, and Surveys 3 and 4, respectively. Of the 537 participants who completed our experiment, all but two requested an invitation to Survey 5, our optional long-term follow-up survey. Of the participants invited to Survey 5, 91.8% completed Survey 5. Our dropout rates may be partly due to our longitudinal study design, which employed multiple surveys over multiple weeks. It may also be partly due to bugs in the Prolific platform which we encountered while running our study [51, 52] which may have interfered with participation. A Pearson Chi-Square test did not find any evidence of dropout differing between our treatment groups ($p = 0.649$), and a Pearson Chi-Square test did not find evidence of Survey 5 completion differing by use of Tor Browser during the experiment ($p = 0.372$).

Another limitation is that our instructions for using Tor Browser were based on a conservative threat model. For example, we recommended that participants not log into online accounts in Tor Browser to avoid deanonymizing themselves. However, it may not be necessary to take this precaution if one is only concerned about protecting one's privacy from one's ISP. We decided against more detailed instructions explaining these nuances, since our intuition was that it might either overwhelm participants or cause them to misunderstand the extent of Tor Browser's protections.

Finally, we identified two instances where improvements to our surveys might make our results clearer. First, we saw that our action planning nudge appeared to negate the increase in perceptions of threat susceptibility from our PMT nudge (Figure 6). Perhaps our participants' plans to use Tor Browser made them feel more protected against online observation, since they anticipated using it. But since we were interested in motivation to adopt Tor Browser, we wanted to measure participants' perceptions of threat susceptibility when they *were not* using Tor Browser. Alternative phrasing could have removed this ambiguity (e.g., "If you do not use Tor Browser, what do you think is the likelihood of others observing your web browsing activity?"). Sec-

ond, we did not ask about perceptions of privacy control in Survey 2; since we do not see differences in Survey 4, it is unclear whether our nudges ever had an effect on these perceptions. It would have been better to ask about privacy control in Survey 2 as well.

6 Discussion and Future Work

Our results suggest that there are opportunities to increase adoption of Tor Browser using nudging techniques, particularly those based on protection motivation theory (PMT). Certainly, not everyone is interested in using Tor Browser (§ 4.3 and Figure 11). However, our nudging techniques show that many people are willing to give it a try (Table 4), and that our PMT-based nudge can encourage a significant percentage to continue using Tor Browser in the long term (§ 4.8). We also tested nudges based on action and coping planning implementation intentions. Although we did not find evidence of these plans further increasing long-term adoption of Tor Browser (§ 4.8), those who were given the opportunity to form coping plans were more likely to use Tor Browser in the subsequent week (§ 4.1).

Future work should investigate whether our nudges have effects beyond simply increasing tool usage. First, it is worth testing whether our PMT-based nudge also contributes to more effective use of Tor Browser. For example, our instructions reminded participants that Tor Browser's protections are reduced if one logs in to websites. Future work could confirm that our instructions help people use Tor Browser effectively. Second, although our action planning nudge was designed to help people identify opportunities to use Tor Browser, it did not significantly increase the number of participants who reported using Tor Browser in the previous week. An alternative outcome variable we could not measure was consistency of using Tor Browser: does someone always remember to use Tor Browser for a particular privacy-sensitive activity? A future study could measure whether action plans help in this respect. Also, it should be noted that we intentionally recruited participants who had prior experience with private browsing mode and VPNs (§ 3). Similar to Tor Browser, private browsing mode can be enabled for privacy-sensitive browsing; perhaps our action plan template was less helpful to those already familiar with private browsing, since they might be accustomed to the usage model encouraged by our action plan. Future work could test whether our action plan is more effective for a more general audience. Third, our study showed that participants frequently encountered challenges using Tor Browser (§ 4.5). In particular, it was common for participants to report extreme slowness or websites not working in Tor Browser. To help participants mitigate these and other challenges, we tested several coping plans (Figures 5 and 20). Although we did not find evidence of our coping plans leading to long-term increases in use of Tor Browser, we did see evidence of an effect in the week after participants formed their coping plans, perhaps due to participants using Tor Browser to test their coping strategies (§ 4.3). Combined with participants' positive feedback about their coping plans, it seems worth testing whether coping plans like ours have effects beyond what we measured in our study. For example, coping plans may help people persevere in using Tor Browser when they encounter challenges, rather than simply switching to a different browser after encountering a difficulty. Future work could study how people react to Tor Browser's usability challenges, and whether coping plans have an impact.

Several things should be considered when translating our results to a real-world deployment of nudges. First, our participants knew our nudges were part of a research study. However, how people respond to information depends on which entity delivers that information [18, 33]. Our nudges might be more or less effective depending on how people perceive the entity administering the nudges. Tor Browser itself might serve as a trusted messenger for nudges, perhaps incorporating nudges into the browser's homepage, or displaying them in the UI when various challenges are encountered. For example, if Tor Browser can determine that a website is blocking Tor users, Tor Browser might explain this and recommend using an alternative website. Second, we only recruited participants who we thought would be highly motivated to use Tor Browser (§ 3). Specifically, we recruited participants who had prior experience with other privacy tools, and who expressed a high level of interest in preventing at least one privacy threat Tor Browser can protect against. Our intuition was that it would be easier to detect the effects of our nudges among these participants in our experiment; perhaps similar targeting should be employed when deploying nudges in the wild. Nudging someone to adopt Tor Browser when it does not meet a need for them, or when they are not sufficiently motivated to overcome challenges associated with using it, may be problematic. Most notably, people have limited time to devote to privacy and security, so engaging with advice which is unlikely to be followed has a cost to the recipient [30]. Determining the best way

to target nudges like ours remains a question for future work. As Tor Browser becomes more usable over time, it might make sense to more broadly deploy nudging to encourage adoption.

Multiple stakeholders can increase the usability of Tor Browser. In particular, website operators may benefit from better supporting users of Tor Browser. Our participants shared that they used Tor Browser for many innocuous activities, including shopping, reading the news, and researching medical topics (§ 4.4). Many websites are supported by advertising revenue, and although adoption of ad blockers is widespread [67], Tor Browser actively discourages the use of ad blockers [77]. Thus, websites may have a financial incentive to support Tor Browser users. To support users of Tor Browser, website operators should start by testing that their websites work properly in Tor Browser. If their website is hosted using Cloudflare, they can simply enable Cloudflare's Onion Routing [16] feature. Tor Browser's usability may also be improved through technical enhancements to the Tor Browser and the Tor network [9, 17, 75], and by volunteers contributing computing resources to increase the Tor network's capacity [76].

Finally, future work is needed to test whether PMT, action planning, and coping planning nudges can increase effective adoption of other privacy and security technologies. For example, an action plan might help people remember to use a password manager, and a coping plan might help people persevere if a website does not work properly with their password manager. As another example, an action plan might help people remember to use an encrypted messaging app. If one of the person's friends cannot receive encrypted messages because the friend does not have the app installed, a coping plan could encourage the person to tell their friend to install the app. For both password managers and encrypted messaging apps, a PMT nudge could motivate people to use the tools by helping them form accurate perceptions of the threats the tools protect against, and of the protections the tools can offer.

7 Conclusions

In the face of widespread privacy concerns, privacy enhancing technologies offer the possibility of returning control to users. Privacy tools like ad blockers are widely adopted, but other tools, like Tor Browser, are far less commonly used. Is this due to some inherent property of Tor Browser (e.g., is it too slow?), or is there certain information which might convince more people to adopt Tor Browser? To address this question, we tested whether three nudges could increase adoption of Tor Browser: a nudge based on protection motivation theory (PMT), an action planning implementation intention nudge, and a coping planning implementation nudge. Our longitudinal field experiment showed that our coping planning nudge increased short-term use of Tor Browser (§ 4.1), and our PMT-based nudge increased both short- and long-term use of Tor Browser (§ 4.8). Of course, in the future the usability of Tor Browser might be improved in various ways, but our results suggest that a significant percentage of people are ready to start using Tor Browser today, and that nudges can help them do so. Simultaneously, it is important to realize that Tor Browser only addresses particular privacy needs. For example, it cannot prevent a social media company from sharing information about one's profile, or an email provider from analyzing one's emails. For these and other challenges, a combination of different privacy enhancing technologies and legal regulations may be appropriate. In cases where technologies can help, we hope our nudging research will prove helpful in increasing their adoption.

In particular, the Tor Project and other privacy advocacy groups should consciously incorporate PMT-related factors into their messaging, since our results show that PMT nudges can motivate people to become long-term users of Tor Browser. Our action and coping plans may also help people use Tor Browser more effectively, although further research may be needed to fully understand their effects. Nudging users of Tor Browser to form action plans could help users remember to use Tor Browser more consistently. With some changes in format, an action planning nudge could be deployed on the Tor Browser start page. Coping plans could also be integrated into Tor Browser. For example, if a user of Tor Browser encounters a challenge (e.g., a website blocking Tor traffic), Tor Browser could detect this and help the user respond appropriately (e.g., by suggesting alternative websites). Tor Browser is configured to use DuckDuckGo as the default search engine; in this way, the browser is already nudging users away from using Google, which sometimes blocks Tor traffic. Researchers and privacy advocates should also investigate whether PMT, action planning, and coping planning nudges might help people use other technologies, such as password managers and encrypted messaging apps.

In conclusion, we hope nudges will help increase adoption of Tor Browser and other technologies, giving people greater security and privacy.

Acknowledgments

We thank Yuanyuan Feng, Yixin Zou, and Linda Moreci for their assistance with our research. This research was supported in part by a grant from the National Science Foundation's Secure and Trustworthy Computing program (CNS-1801316) and in part through a fellowship from the CyLab Security and Privacy Institute at Carnegie Mellon University. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF or the U.S. Government.

References

[1] Henk Aarts, Ap Dijksterhuis, and Cees Midden. To plan or not to plan? Goal achievement or interrupting the performance of mundane behaviors. *European Journal of Social Psychology*, 29(8):971–979, 1999.

[2] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. Privacy and human behavior in the age of information. *Science*, 347(6221):509–514, 2015.

[3] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. *Journal of Consumer Psychology*, 30(4):736–758, 2020.

[4] Alessandro Acquisti, Manya Sleeper, Yang Wang, Shomir Wilson, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, and Florian Schaub. Nudges for Privacy and Security. *ACM Computing Surveys*, 50(3):1–41, August 2017.

[5] Elham Al Qahtani, Mohamed Shehab, and Abrar Aljohani. The Effectiveness of Fear Appeals in Increasing Smartphone Locking Behavior among Saudi Arabians. *SOUPS @ USENIX Security Symposium*, 2018.

[6] Yusuf Albayram, Mohammad Maifi Hasan Khan, Theodore Jensen, and Nhan Nguyen. "...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. *Symposium on Usable Privacy and Security*, 2017.

[7] Hazim Almuhimedi. Helping Smartphone Users Manage their Privacy through Nudges. Technical Report CMU-ISR-17-111, December 2017.

[8] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Cranor, and Yuvraj Agarwal. Your location has been shared 5,398 times!: A field study on mobile app privacy nudging. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015.

[9] Mashael Alsabah and Ian Goldberg. Performance and Security Improvements for Tor: A Survey. *ACM Computing Surveys*, 49(2):1–36, November 2016. https://dl.acm.org/doi/10.1145/2946802.

[10] arma. Bittorrent over Tor isn't a good idea, April 2010. https://blog.torproject.org/bittorrent-over-tor-isnt-good-idea.

[11] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information: Pew Research Center*. November 2019.

[12] Ariane Bélanger-Gravel, Gaston Godin, and Steve Amireault. A meta-analytic review of the effect of implementation intentions on physical activity. *Health Psychology Review*, 7(1):23–54, March 2013.

[13] Veronika Brandstätter, Angelika Lengfelder, and Peter M Gollwitzer. Implementation Intentions and Efficient Action Initiation. *Journal of personality and social psychology*, 81(5):946, 2001.

[14] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, January 2006.

[15] Yinzhi Cao, Song Li, and Erik Wijmans. (Cross-)Browser Fingerprinting via OS and Hardware Level Features. *Network and Distributed System Security Symposium*, March 2017.

[16] Cloudflare. Understanding Cloudflare Tor support and Onion Routing, February 2021. https://support.cloudflare.com/hc/en-us/articles/203306930-Understanding-Cloudflare-Tor-support-and-Onion-Routing.

[17] Roger Dingledine and Steven J Murdoch. Performance Improvements on Tor or, Why Tor is slow and what we're going to do about it. Technical report, March 2009. https://svn-archive.torproject.org/svn/projects/roadmaps/2009-03-11-performance.pdf.

[18] P. Dolan, M. Hallsworth, D. Halpern, D. King, R. Metcalfe, and I. Vlaev. Influencing behaviour: The mindspace way. *Journal of Economic Psychology*, 33(1):264–277, February 2012. https://linkinghub.elsevier.com/retrieve/pii/S0167487011001668.

[19] DuckDuckGo. A Study on Private Browsing: Consumer Usage, Knowledge, and Thoughts. Whitepaper, January 2017.

[20] Jim Finkle. Web tools help protect human rights activists. *Reuters*, August 2009. https://www.reuters.com/article/us-column-pluggedin-idUSTRE57I4IE20090819.

[21] Kevin Gallagher, Sameer Patil, Brendan Dolan-Gavitt, Damon McCoy, and Nasir Memon. Peeling the Onion's User Experience Layer. *ACM SIGSAC Conference on Computer and Communications Security (CCS '18)*, October 2018.

[22] Kevin Gallagher, Sameer Patil, and Nasir D. Memon. New Me - Understanding Expert and Non-Expert Perceptions and Usage of the Tor Anonymity Network. *Symposium on Usable Privacy and Security*, 2017.

[23] Nina Gerber, Paul Gerber, and Melanie Volkamer. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, 77:226–261, August 2018. https://linkinghub.elsevier.com/retrieve/pii/S0167404818303031.

[24] Peter M. Gollwitzer. Implementation intentions: Strong effects of simple plans. *American Psychologist*, 54(7), 1999.

[25] Dan Goodin. Majority of Android VPNs can't be trusted to make users more secure | Ars Technica, January 2017. https://arstechnica.com/information-technology/2017/01/majority-of-android-vpns-cant-be-trusted-to-make-users-more-secure/.

[26] Google. Requests for User Information FAQs - Transparency Report Help Center, 2021. https://support.google.com/transparencyreport/answer/9713961?hl=en.

[27] Glenn Greenwald and Ewen MacAskill. NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*, June 2013. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[28] Ilya Grigorik. Networking 101: Transport Layer Security (TLS). In *High Performance Browser Networking*. O'Reilly Media, Inc., 2013. https://hpbn.co/transport-layer-security-tls/.

[29] Hana Habib, Jessica Colnago, Vidya Gopalakrishnan, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, and Lorrie Faith Cranor. Away From Prying Eyes - Analyzing Usage and Understanding of Private Browsing. *SOUPS @ USENIX Security Symposium*, 2018.

[30] Cormac Herley. So long, and no thanks for the externalities - the rational rejection of security advice by users. *NSPW*, pages 133–144, 2009.

[31] Rae Hodge. Why you should be skeptical about a VPN's no-logs claims, July 2020. https://www.cnet.com/news/why-you-should-be-skeptical-about-a-vpns-no-logs-claims/.

[32] Angelika Lengfelder and Peter M Gollwitzer. Reflective and Reflexive Action Control in Patients With Frontal Brain Lesions. *Neuropsychology*, 15(1):80, 2001.

[33] Johanna Catherine Maclean, John Buckell, and Joachim Marti. Information Source and Cigarettes: Experimental Evidence on the Messenger Effect. Technical Report w25632, National Bureau of Economic Research, Cambridge, MA, March 2019. http://www.nber.org/papers/w25632.pdf.

[34] Mary Madden and L. Rainie. *Americans' Attitudes about Privacy, Security and Surveillance*. Pew Research Center, May 2015.

[35] James E Maddux and Ronald W Rogers. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology*, 19(5):469–479, 1983.

[36] Salvatore S. Mangiafico. Kruskal–wallis test, Feb 2020. https://rcompanion.org/handbook/F_08.html.

[37] Akshaya Mani, T. Wilson-Brown, Rob Jansen, Aaron Johnson, and Micah Sherr. Understanding Tor Usage with Privacy-Preserving Measurement. In *Proceedings of the Internet Measurement Conference*, pages 175–187, Boston MA USA, October 2018. ACM. https://dl.acm.org/doi/10.1145/3278532.3278549.

[38] Jonathan R. Mayer and John C. Mitchell. Third-Party Web Tracking: Policy and Technology. *IEEE Symposium on Security and Privacy*, 2012.

[39] Georg Merzdovnik, Markus Huber, Damjan Buhov, Nick Nikiforakis, Sebastian Neuner, Martin Schmiedecker, and Edgar Weippl. Block Me If You Can: A Large-Scale Study of Tracker-Blocking Tools. *IEEE European Symposium on Security and Privacy (EuroS&P)*, March 2017.

[40] Chance Miller. iOS 13 cracks down on location permission settings, June 2019. https://9to5mac.com/2019/06/08/ios-13-location-permissions/.

[41] Sarah Milne, Sheina Orbell, and Paschal Sheeran. Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British Journal of Health Psychology*, 7(2):163–184, May 2002.

[42] Sarah Milne, Paschal Sheeran, and Sheina Orbell. Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory. *Journal of Applied Social Psychology*, 30(1):106–143, January 2000.

[43] Chris Morran. House Votes To Allow Internet Service Providers To Sell, Share Your Personal Information, March 2017. https://www.consumerreports.org/consumerist/house-votes-to-allow-internet-service-providers-to-sell-share-your-personal-information/.

[44] Greg Norcie, Jim Blythe, Kelly Caine, and L. Jean Camp. Why Johnny Can't Blow the Whistle: Identifying and Reducing Usability Issues in Anonymity Systems. *Workshop on Usable Security*, February 2014.

[45] Gabriele Oettingen and Gaby Ho. Effective self-regulation of goal attainment. *International journal of educational research*, pages 705–732, 2000.

[46] Office of the Privacy Commissioner of Canada. What an IP Address Can Reveal About You, May 2013. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305.

[47] Eyal Peer, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology*, 70(C):153–163, May 2017.

[48] Jonathon W. Penney. Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Technology Law Journal*, 31(1):117–182, 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645.

[49] Mike Perry, Erinn Clark, Steven Murdoch, and Georg Koppen. The Design and Implementation of the Tor Browser, June 2018. https://2019.www.torproject.org/projects/torbrowser/design/.

[50] Nathaniel Popper. The Tax Sleuth Who Took Down a Drug Lord. *The New York Times*, December 2015. https://www.nytimes.com/2015/12/27/business/dealbook/the-unsung-tax-agent-who-put-a-face-on-the-silk-road.html.

[51] Prolific Support Team. Ineligibility issues, April 2021. https://www.reddit.com/r/ProlificAc/comments/ms114h/ineligibility_issues/.

[52] Prolific Support Team. Ineligibility issues: Fix update, April 2021. https://www.reddit.com/r/ProlificAc/comments/n0f1me/ineligibility_issues_fix_update/.

[53] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. How Well Do My Results Generalize? Comparing Security and Privacy Survey Results from MTurk, Web, and Telephone Samples. *IEEE SP*, 2019.

[54] Ronald W Rogers. A Protection Motivation Theory of Fear Appeals and Attitude Change. *The Journal of Psychology*, 91(1):93–114, 1975.

[55] Ronald W Rogers and Steven Prentice-Dunn. Protection motivation theory. 1997.

[56] Choe Sang-Hun. In Reporting on North Korea, Tech Helps Break Through Secrecy. *The New York Times*, July 2017. https://www.nytimes.com/2017/07/05/technology/personaltech/in-reporting-on-north-korea-tech-helps-break-through-secrecy.html.

[57] Paschal Sheeran, Sarah Milne, Thomas L. Webb, and Peter M. Gollwitzer. *Implementation Intentions and Health Behaviour*. 2005.

[58] Paschal Sheeran, Thomas L. Webb, and Peter M. Gollwitzer. The Interplay Between Goal Intentions and Implementation Intentions. *Personality and Social Psychology Bulletin*, 31(1):87–98, January 2005. https://doi.org/10.1177/0146167204271308.

[59] Signal. Signal Messenger, 2021. https://signal.org/.

[60] Falko F. Sniehotta, Ralf Schwarzer, Urte Scholz, and Benjamin Schüz. Action planning and coping planning for long-term lifestyle change: Theory and assessment. *European Journal of Social Psychology*, 35(4):565–576, 2005.

[61] Daniel J Solove. The Myth of the Privacy Paradox. *George Washington Law Review*, 89:52, 2021.

[62] steph. How Has Tor Helped You? Send Us Your Story., February 2019. https://blog.torproject.org/how-has-tor-helped-you-send-us-your-story.

[63] Peter Story. Tor browser study: Preregistration, Mar 2020. https://osf.io/bc42h.

[64] Peter Story. Tor browser study: Study page, Mar 2020. https://osf.io/t7qe2.

[65] Peter Story. Switch from POST to GET for DDG Searches, January 2021. https://gitlab.torproject.org/tpo/applications/tor-browser/-/issues/40287.

[66] Peter Story, Daniel Smullen, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. From Intent to Action - Nudging Users Towards Secure Mobile Payments. *SOUPS @ USENIX Security Symposium*, 2020.

[67] Peter Story, Daniel Smullen, Yaxing Yao, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. Awareness, Adoption, and Misconceptions of Web Privacy Tools. *Proceedings on Privacy Enhancing Technologies*, 2021(3):308–333, July 2021. https://www.sciendo.com/article/10.2478/popets-2021-0049.

[68] Gail M. Sullivan and Richard Feinn. Using Effect Size—or Why the PValue Is Not Enough. *Journal of Graduate Medical Education*, 4(3):279–282, September 2012.

[69] Richard H Thaler and Cass R Sunstein. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. J. Wiley and Sons, 2008.

[70] The Monero Project. Monero - secure, private, untraceable, 2021. https://www.getmonero.org//index.html.

[71] The Tor Project. Overview, April 2020. https://2019.www.torproject.org/about/overview.html.en.

[72] The Tor Project. Am I totally anonymous if I use Tor?, 2021. https://support.torproject.org/faq/staying-anonymous/.

[73] The Tor Project. Anonymity Online, 2021. https://torproject.org.

[74] The Tor Project. Download, 2021. https://www.torproject.org/download/.

[75] The Tor Project. GitLab, 2021. https://gitlab.torproject.org/tpo/team.

[76] The Tor Project. Relay Operations, 2021. https://community.torproject.org/relay/.

[77] The Tor Project. Should I install a new add-on or extension in Tor Browser, like AdBlock Plus or uBlock Origin?, 2021. https://support.torproject.org/tbb/tbb-14/.

[78] Maciej Tomczak and Ewa Tomczak. The need to report effect size estimates revisited. An overview of some recommended measures of effect size. *Trends in Sport Sciences*, pages 19–25, July 2014.

[79] Thomas L. Webb and Paschal Sheeran. Identifying good opportunities to act: Implementation intentions and cue discrimination. *European Journal of Social Psychology*, 34(4):407–419, 2004. https://onlinelibrary.wiley.com/doi/abs/10.1002/ejsp.205.

[80] WhatIsMyIPAddress.com. How does geolocation work?, November 2020. https://whatismyipaddress.com/geolocation.

[81] Wikipedia. Web tracking. *Wikipedia*, May 2021. https://en.wikipedia.org/w/index.php?title=Web_tracking&oldid=1020976696.

[82] Kim Witte and Mike Allen. A meta-analysis of fear appeals: Implications for effective public health campaigns. *Personality and Social Psychology Review*, 27(5):591–615, 2000.

[83] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices. *CHI*, pages 1–15, April 2020.

A Appendix

A.1 Survey Materials

A.1.1 Survey 1

Researchers at Carnegie Mellon University are conducting a research study to understand people's use of web browsing-related tools.

All participants are asked to answer the screening questions below.

Based on your answers to the screening questions, we will determine your eligibility for our Survey #1. If you are eligible, Survey #1 will take about 4 minutes to complete. Only some of the participants who take Survey #1 will be invited to participate in four follow-up surveys (Surveys #2, #3, #4, and #5).

In what country do you currently reside?
(United States, Other country)

Which operating system does your primary personal computer run?
(Windows, macOS, Ubuntu, Other, I don't know)

Use/Install Code	Description	Number of Occurrences
NOVELTY	Wanting to test out Tor Browser, compare it to other browsers, etc.	36
PRIVACY	Installing/using Tor Browser for its privacy protections. We count "not seeing ads" as a privacy issue (i.e., intrusion upon seclusion). We count listing topics which would commonly be considered privacy-sensitive (e.g., medical).	34
STUDY	Installing/using Tor Browser explicitly because of the study (e.g., if they think we asked them to use it, that it is required, they made a promise to do so, or they explicitly state that their plan or the study information is influencing them).	21
SECURITY	Installing/using Tor Browser for security protections. We count listing topics which would commonly be considered security-sensitive (e.g., logging into your bank account).	10
VAGUE_POSITIVE	Installing/using Tor Browser for vague positive reasons. If their other answers remove the ambiguity, it's okay to use the other answers to inform the choice of a different code.	9
CONTENT	For accessing inaccessible content (e.g., viewing country-specific content, paywalls, censored content, piracy, them accessing dark web sites, etc.).	6
HIGH_SELF_EFFICACY	Thinking it would be easy to install/use.	4
GOOD_REVIEWS	Hearing/reading good things about Tor Browser (aside from those in the survey itself), or knowing others who use it. Not applicable if you heard about it before, but don't specify whether you heard good things or not.	3
JOB	For one's work or school.	1
Not Use/Install Code		
NOT_NEEDED	Not needing Tor Browser, whether stated generally, or for a particular reason (e.g., I don't need that level of protection, my needs are already met by another tool, etc.).	80
NOT_INSTALLED	Not using Tor Browser because it's not installed.	53
BUSY	Not having time to install/use Tor Browser (e.g., general busyness, vacation, being away from devices, etc.).	32
FORGOT	Forgetting to install/use Tor Browser.	30
LOW_SELF_EFFICACY	Thinking it would be difficult, inconvenient, etc. to install/use. More vague than the explicit difficulties mentioned for USABILITY.	19
USABILITY	Usability challenges, such as Tor Browser being slow, websites not working, not functioning or opening (e.g., due to antivirus software), etc.	16
SAFETY_DOUBTS	Doubting that Tor Browser is safe to install/use.	15
RESEARCH	Needing to do more research before installing/using Tor Browser.	13
VAGUE_NEGATIVE	Not installing/using Tor Browser for vague negative reasons. For example, writing just "I'm not interested," or "I'm lazy". If their other answers remove the ambiguity, it's okay to use the other answers to inform the choice of a different code.	13
DEVICE	Device-related limitations discouraging installation/use of Tor Browser (e.g., workplace prohibitions on installation, lack of disk space, a slow computer, etc.).	7
LOW_RESPONSE_EFFICACY	Doubting that Tor Browser is effective at protecting one's privacy, or doubting that anything can be done to protect one's privacy.	5
LOGINS	Tor Browser not being useful for activities that require logging in.	4
BAD_REVIEWS	Hearing/reading bad things about Tor Browser from sources that are clearly other than the survey itself, or finding it suspicious that they've heard nothing about it before.	4

Table 6. Throughout our study, we asked participants whether they had installed or used Tor Browser, and their reasons for either doing so or not doing so. We collected multiple responses from all 537 participants who completed our experiment. We stopped coding after reaching code saturation; in total, we coded 558 free text responses from 150 randomly selected participants. Note that codes are not mutually exclusive, and that we count each code at most once per participant.

Activities Code	Description	Described	Performed	Performed Using Tor Browser
PNTD	Either the literal text "prefer not to disclose," or something close to it.	192	100	33
SHOPPING	Looking up information about consumer products, regardless of intention to purchase.	55	39	13
FINANCIAL	Looking up information about financial products (e.g., stocks, bitcoin), mortgages, banking, insurance, salaries, applying to jobs, etc.	49	35	8
VAGUE	A vaguely defined activity, such as "using a search engine" or "researching things."	49	41	25
NEWS	Looking up information about politics, celebrities, current events, document leaks, etc.	40	29	17
NSFW	Pornography or other "Not Safe For Work" content.	36	29	15
MEDICAL	Accessing medical information. Includes personal care and cannabis.	33	21	11
VIDEOS	Watching videos, movies, or streaming. We don't assume that all pornography is video-based. Since there is a "community" aspect to YouTube, simply mentioning "YouTube" isn't enough to assume this code applies.	26	18	10
YOUTUBE	Using YouTube.	25	22	12
SNOOPING	Looking up information about non-celebrities (e.g., ex's, friends, background checks) or similar entities (e.g., employers, competitors).	20	11	4
OTHER_ENTERTAINMENT	Websites about hobbies (e.g., emulation, listening to music), reading stories, blogs, etc.	16	10	7
N_A	Not plans or activities. For example, "none". Or "I will install Tor Browser."	16	0	0
MISC	Activities which are well-described but difficult to categorize.	14	11	4
TRAVEL	Travel-related browsing.	12	7	4
OTHER_SOCIAL	Using a generically specified social media website (e.g., "social media," "dating website," "forums," "anonymous messaging").	12	8	4
GOOGLE	Using Google search.	11	9	7
LOCAL	Apartment hunting, researching schools, wedding venues, etc.	10	9	9
REDDIT	Using Reddit.	9	8	6
OTHER_NAMED	Using another named website.	9	7	4
PIRACY	Pirating music, software, etc.	7	5	2
WIKI	Using Wikipedia or other wikis. Wikileaks doesn't count, since it isn't actually a wiki.	7	5	4
EMAIL	Accessing email.	7	6	0
AMAZON	Using Amazon.	4	3	1
FACEBOOK	Using Facebook.	4	3	2
DARK_WEB	Accessing the dark web.	2	2	2
TWITTER	Using Twitter.	2	2	1
RELIGION	Accessing religious information.	2	0	0
LEGAL	Accessing legal information.	2	0	0
LINKEDIN	Using LinkedIn.	1	1	0
PINTEREST	Using Pinterest.	1	0	0

Table 7. In Survey 2, we gave participants in our PMT+AP treatment group the opportunity to plan to use Tor Browser for privacy-sensitive activities. Each participant was given the option to list up to three activities, so in some cases they contributed multiple times to the counts of the same codes. Also, note that codes were not mutually exclusive; for example, it was common for the VIDEOS and YOUTUBE codes to occur together. The "Described" column shows the number of activities with each code described in participants' plans. The "Performed" column shows the number of activities participants reported performing in either Survey 3 or Survey 4. The "Performed Using Tor Browser" column shows the number of activities participants reported performing using Tor Browser in either Survey 3 or Survey 4.

Challenges Code	Description	Number of Occurrences
BIT_SLOW	Websites were somewhat slow, but not extremely slow.	9
VAGUE	A vaguely defined challenge, or it's unclear whether there was a challenge at all. For example, "It didn't work."	7
SEARCHING	Difficulty finding pages (e.g., poor results from DuckDuckGo).	5
NOT_WORKING	An answer substantially the same as the predefined "Websites did not work" option (e.g., CAPTCHAs). Problems likely originating from the website, rather than the browser.	4
N_A	Clearly not a challenge "encountered when trying to use Tor Browser." For example, "I don't need it," or using the free text fields to explain other responses (e.g., "I made a mistake earlier in the survey").	4
FEATURES	Lacking features (e.g., bookmarks, ad blockers, login persistence, etc.).	4
CONNECTION	Tor Browser taking time or failing to connect to the Tor network.	3
CONFUSED	Expressing confusion about how to use Tor Browser, or what it is for.	2
EXTREMELY_SLOW	An answer substantially the same as the predefined "Websites were extremely slow" option (e.g., that might be mitigated by creating a new circuit).	2
IP_RELATED	IP address-related issues. Don't make inferences when coding (e.g., don't assume that a CAPTCHA is IP-related, unless the participant explicitly makes that connection).	2
LANGUAGE	Pages appearing in the wrong language.	2
LOW_RESPONSE_EFFICACY	The participant doesn't believe Tor Browser can protect their privacy.	1
CONFIGURATION	Configuration being a challenge.	1
NO_CHALLENGE	An answer substantially the same as the predefined "I did not encounter any challenges" option.	1
COST	Tor Browser costing money.	1
SPACE	Lack of space on one's device.	1
NOT_ALLOWED	Not being allowed to install or use Tor Browser due to company policies, etc.	1

Table 8. In Survey 3, we asked participants whether they had encountered challenges when trying to use Tor Browser. Some participants indicated that they had encountered a challenge other than those we listed. All participants were given a free text field to explain these challenges, and those in the coping planning treatment were asked to explain further. We coded such responses from 41 different participants, 3 of whom we determined not to have actually encountered a challenge (i.e., their free text responses were only coded with as "N_A"). Note that codes were not mutually exclusive, and if participants gave two free text responses, their responses might have different codes. However, we count each code at most once from each participant.

Challenge	Coping Plan	Reencountered Challenge?	Followed Plan?
I thought it was only for .onion sites and got confused! I was under the impression it was only for accessing hidden sites on the internet, like .onion domains and the silk road as was discussed in the first studies	I will engage with more tutorials and review the previously provided guide on actually using the tor browser.	No	Mostly yes
I was not always able to open websites, even when they had "are you a human?" checks because they somehow saw me as not a legitimate access request	I think I will just have to open those sites in another browser	No	No
It was very difficult for me to save images from my search. viewing the image or image source only worked half the time. The web was a little slow but nothing bad. It was just frustrating to try and download images	It looks like its a somewhat common issue for android users, which is where I used Tor. An image would only have the "save image" option half the time.	No	No
I used Tor the only time several years ago. I vaguely recall it being a bit slower, but don't know that this reflects the current situation.	When I re-download it I'll keep in mind the security benefits the browser offers and how this outweighs any lag.	No	Mostly no
I tried to use TOR on my phone, even with the work-arounds offered it simply didn't work. I wasn't able to get it to function on my phone.	I plan to keep researching and see if there is a different method to get TOR on my smartphone. Also I plan to try to download TOR on my laptop just to see what my options for private browsing when I'm not working are.	Yes	Yes
Functionality is limited because privacy protection is based so much on individual sites' policies (e.g. if I go to Google Maps or YouTube) that it doesn't actually help that much	Sorry, to be honest, you cannot get around this. It's not a matter of my individual will.	Yes	No
Migrating bookmarks and other personalization such as passwords was either difficult or not present (which I understand the password portion). It was frustrating using it for any activities that required usage of account or cookie-based websites. This is because the passwords and accounts don't save, for obvious reasons.	The best next step would be to use an independent password manager if I ever want to use Tor Browser again. Services like 1Password exist for a solid reason, so it might not be a bad idea to look into it.	Yes	Mostly no
The browser itself is not stable. When I launched the browser the popup screen to load it got stuck a couple of times. Then when I finally did "search" it took so long I gave up and looked up the information on Google Chrome instead.	I have no idea how to cover come this since it's a tech issue that I don't have control over.	Yes	Mostly no
Sometimes some sites were slow but it was manageable. No challenges, just slower than usual. Videos play back just fine, the initial load time is just slow.	So if it becomes a real big issue, I would look at disconnecting from TOR, and relaunching. Perhaps I could find a faster Peer to connect to that isn't as slow. Worst case, if say watching a video, I could pause it, let it buffer and then proceed.	No	Yes
I don't really like DuckDuckGo so I was trying to use Google but every time I did it was in German. I have a hard time remembering to use it and when I do remember, I am usually not willing to wait for it to load. I like using Google search, but I see why they use DuckDuckGo as the default. The results on DuckDuckGo aren't terrible but I know there are some times when its hard to find what I'm looking for.	I can add the Tor browser to my task bar next to the other browsers so I will remember to use it. I could also leave it open so that it is ready for me to use when I need it.	Yes	Mostly yes
It seemed a little slower than my other browsers but I wouldn't describe it as "extremely slow."	Any additional challenges that I encountered I'd search in DuckDuckGo to learn more about.	Yes	No
It wouldn't let me install it because it said I was lacking space on my computer.	Buy a new computer? But that would cost a lot of money. I don't know what I could delete that I don't need.	Yes	Mostly no

Table 9. In Survey 3, we gave participants in our PMT+AP+CP treatment group who reported encountering challenges using Tor Browser the opportunity to form coping plans to overcome their challenges. Participants who did not select a listed challenge (i.e., "Websites were extremely slow" or "Websites did not work") were given an open-ended plan template (Figure 20). This table contains these participants' responses, lightly edited for clarity. In Survey 4, one week later, we checked whether participants reencountered the challenges they described, and whether they followed their plans to overcome the challenges.

Do you speak English?
(Yes, No)

What is your age in years?
____

Based on your answers to our screening questions, we have determined that you are eligible for Survey #1. Please review the details below:
[Consent form]

Have you read and understood the information above?
(Yes, No)

Do you want to participate in this research and continue with the survey?
(Yes, No)

Private Browsing
Note that "private browsing" is referred to as "Incognito" in Google Chrome and "InPrivate" in Microsoft Edge.

Have you **heard of** private browsing before?
(Yes, No, Unsure)

[If Yes]
Have you **used** private browsing before?
(Yes, No, Unsure)

[If Yes]
When did you most recently use private browsing?
(Today, In the past week, In the past month, In the past year, More than a year ago)

VPNs
Have you **heard of** VPNs before?
(Yes, No, Unsure)

[If Yes]
Have you **used** a VPN before?
(Yes, No, Unsure)

[If Yes (i.e., used a VPN before)]
Do you use a VPN **primarily for work purposes**?
(Yes, primarily for work purposes; No, primarily for other purposes; About equally for work and other purposes)

[If Yes (i.e., used a VPN before)]
When did you most recently use a VPN?
(Today, In the past week, In the past month, In the past year, More than a year ago)

Tor Browser
Have you **heard of** Tor Browser before?
(Yes, No, Unsure)

[If Yes]
Have you **used** Tor Browser before?
(Yes, No, Unsure)

[If Yes]
When did you most recently use Tor Browser?
(Today, In the past week, In the past month, In the past year, More than a year ago)

In the past week, which of the following types of devices did you **use at least once**?
(Smartphone, Tablet, Laptop computer, Desktop computer)

In the past week, how often did you **use a web browser** on each of the following devices?
[Answer options are shown in a response matrix. Rows are labeled with device types: Smartphone, Tablet, Laptop computer, Desktop computer, Other device(s). Columns are labeled with the answer options: Every day, On multiple days, On one day, Never.]

[If a response other than Never was selected for Laptop or Desktop]
In general, are you comfortable installing software on your [laptop or desktop]?
(Yes, No, Unsure)

Rate your level of **disagreement or agreement** with the following statement:
"I think I have control over my online privacy."
(Strongly disagree, Somewhat disagree, Somewhat agree, Strongly agree)

How interested or uninterested would you be in **preventing advertisers from seeing the websites you visit**?
(Not at all interested, Slightly interested, Moderately interested, Very interested)

How interested or uninterested would you be in **preventing the websites you visit from seeing what physical location you are browsing from**?

(Not at all interested, Slightly interested, Moderately interested, Very interested)

How interested or uninterested would you be in **preventing your internet service provider from seeing the websites you visit**?
(Not at all interested, Slightly interested, Moderately interested, Very interested)

How interested or uninterested would you be in **preventing the government from seeing the websites you visit**?
(Not at all interested, Slightly interested, Moderately interested, Very interested)

A.1.2 Survey 2

Researchers at Carnegie Mellon University are conducting a research study to understand people's use of web browsing-related tools.

This survey is Survey #2 in the "Research Study for Internet Users" that you previously gave your consent to participate in. It will take up to 8 minutes to complete this survey. If you complete Survey #2, Survey #3, **and** Survey #4 **within 2 days of each survey invitation**, you will be compensated $3.50 total. We will invite you to each survey one week after you complete the previous survey.

There are no right or wrong answers to any of our questions, so please answer honestly. Also, **please take the time to read the information in this survey carefully**. All links to external resources are optional: your compensation will not be affected by whether you follow them.

[Control Group]
Tor Browser is an alternative web browser.

[PMT, PMT+AP, and PMT+AP+CP Groups]
[Threat information: Figure 2]
[Response information: Figure 3]
Please review these materials about Tor Browser.
[Usage and installation instructions: Figure 16]
[Optional technical details: Figure 17]
[Frequently asked questions: Figure 18]
[Common Problems: Figure 19]
If you want to use Tor Browser, we encourage you to install it now [74]. It only takes a minute to install Tor Browser. However, you do not have to install Tor Browser if you do not want to: your compensation will not be affected.

[PMT+AP and PMT+AP+CP Groups]
[Action plan: Figure 4]
For your convenience, here is a link to the information about Tor Browser that we showed you earlier:
Tor Browser Setup, Use, and FAQ
If you want to use Tor Browser in the coming week, we encourage you to fill out the plan, since it may help you remember to use Tor Browser. However, you do not have to use Tor Browser if you do not want to: your compensation will not be affected. Do you want to continue without writing any activities?
(Yes, I would like to continue without writing any activities)

[PMT, PMT+AP, and PMT+AP+CP Groups]
Thank you for reviewing this information about Tor Browser.

What do you think is **the likelihood** of others observing your web browsing activity?
(Very unlikely, Somewhat unlikely, Somewhat likely, Very likely)

How **concerned or unconcerned** would you be if others observed your web browsing activity?
(Not at all concerned, Slightly concerned, Moderately concerned, Very concerned)

Rate your level of **disagreement or agreement** with the following statement:
"I think I know how to use Tor Browser."
(Strongly disagree, Somewhat disagree, Somewhat agree, Strongly agree)

How **easy or difficult** do you think it would be for you to use Tor Browser?
(Very difficult, Somewhat difficult, Somewhat easy, Very easy)

Rate your level of **disagreement or agreement** with the following statement:
"If I use Tor Browser, I will prevent others from observing my web browsing activity."
(Strongly disagree, Somewhat disagree, Somewhat agree, Strongly agree)

Do you know anyone who uses Tor Browser?

(Yes, No, I'm not sure)

Is Tor Browser currently installed on one of your devices?
(Yes, No, I don't know)

[If Yes (i.e., Tor Browser is installed)]
When did you install Tor Browser?
(Prior to taking this survey, While taking this survey)

[If Yes (i.e., Tor Browser is installed)]
Please explain why you installed Tor Browser.

_____

[If I don't know (i.e., whether Tor Browser is installed)]
Please explain why you do not know whether you have Tor Browser installed.

_____

[If No or I don't know (i.e., whether Tor Browser is installed)]
Rate your level of disagreement or agreement with the following statement:
"I intend **to install** Tor Browser in the next week."
(Strongly disagree, Somewhat disagree, Somewhat agree, Strongly agree)

Rate your level of disagreement or agreement with the following statement:
"I intend **to use** Tor Browser in the next week."
(Strongly disagree, Somewhat disagree, Somewhat agree, Strongly agree)

What is your overall opinion of Tor Browser? (Please write a few sentences)

_____

[PMT, PMT+AP, and PMT+AP+CP Groups]
This is a link to the information about Tor Browser that we showed you earlier:
Tor Browser Setup, Use, and FAQ
Would you like us to send you a message on Prolific containing this link?
(Yes, No)

[PMT+AP and PMT+AP+CP Groups]
This is a link to your plan for using Tor Browser:
My Plan for Using Tor Browser
Would you like us to send you a message on Prolific containing this link?
(Yes, No)

What gender do you identify with?
(Male, Female, Non-binary, Other: _____, Prefer not to answer)

What best describes your employment status?
(Working, paid employee; Working, self employed; Student; Not employed; Retired; Prefer not to answer)

Have you ever worked in or studied in a computer-related field? (Computer Science, IT support, etc.)
(Yes, No)

What is the highest level of school you have completed or degree you have earned?
(Less than high school, High school or equivalent, College or associate degree, Master's degree, Doctoral degree, Professional degree, Other: _____, Prefer not to answer)

Please estimate what your total household income will be for this year:
(Less than $10,000; $10,000 - $19,999; $20,000 - $39,999; $40,000 - $59,999; $60,000 - $79,999; $80,000 - $99,999; $100,000 or more; Prefer not to answer)

Please indicate which other people, if any, live in your household.
(Domestic partner, e.g., spouse, boyfriend/girlfriend, etc.; Children; Parents; Other family; Unrelated roommates; I live alone; Other: _____, Prefer not to answer)

A.1.3 Survey 3

Researchers at Carnegie Mellon University are conducting a research study to understand people's use of web browsing-related tools.

This survey is Survey #3 in the "Research Study for Internet Users" that you previously gave your consent to participate in. It will take up to 6 minutes to complete this survey. If you complete **both** Survey #3 and Survey #4 **within 2 days of each survey invitation**, you will be compensated $3.50 total. We will invite you to Survey #4 one week after you complete this survey.

There are no right or wrong answers to any of our questions, so please answer honestly. Also, **please take the time to read the information in this survey carefully**.

[If not installed, or unsure whether installed]

How do I use Tor Browser?

Tor Browser works just like a regular web browser, with a few key differences:

- **You should not log into accounts when using Tor Browser**. If you log into an account, you will reveal your identity.
- Every time you quit Tor Browser, it erases your browsing history. **You should quit Tor Browser periodically**, so your browsing patterns do not identify you.

So you should not completely replace your regular browser with Tor Browser, since you should use your regular browser to log into your email, social media, etc. Instead, we recommend using Tor Browser for specific, privacy-sensitive activities, such as for viewing sensitive information on Wikipedia or YouTube.

How do I install Tor Browser?

Tor Browser is a free tool run by a non-profit and volunteers. If you would like to use Tor Browser, please download and install it from this webpage: https://www.torproject.org/download/

Fig. 16. As part of our PMT-based intervention we informed participants about how to use and install Tor Browser. We also reminded participants that Tor Browser is free. This text was designed to increase participants' perceptions of self-efficacy and to reduce perceptions of response cost [42].

How does Tor Browser work? (Optional: Click here to reveal)

Tor Browser works by making you look the same as the thousands of other Tor Browser users. It combines several technologies to do this. For example, it uses encryption to hide your browsing from your internet service provider **and from the operators of the Tor network itself**. Also, by automatically erasing browsing history each time it is closed, Tor Browser prevents tracking cookies from connecting your browsing sessions. You can read more about Tor Browser's technology here [71].

This is a simple diagram showing how websites load in Tor Browser. Your browsing goes through three randomly selected servers in the Tor network. This is done so that no single server in the Tor network can connect you to the websites you are browsing. Also, websites see the Tor network instead of your home internet connection, so they cannot connect your browsing back to you.

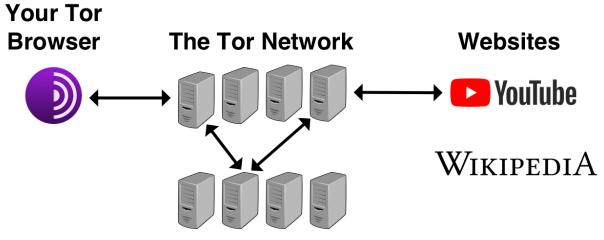

Fig. 17. For more technically inclined participants, we offered technical details about how Tor Browser works. To avoid overwhelming participants, this information was hidden until the heading was clicked.

Frequently Asked Questions

Who uses Tor Browser?

Citizens avoiding government censorship [20], journalists [56], and many other people [62] use Tor Browser.

Is it legal to use Tor Browser?

Yes: In the United States, free speech laws mean that it is completely legal to use Tor Browser. However, Tor Browser is blocked in countries which employ censorship, like China.

Is Tor Browser useful for torrenting files?

No: Tor Browser is intended for loading websites, and the similarity in name of Tor and BitTorrent is purely coincidental. Torrenting files over Tor is not recommended [10].

*Does using Tor Browser **protect me from malware or hackers**?*

No: Tor Browser provides no additional protections against malware or hackers.

*Does using Tor Browser **guarantee** that I will be **anonymous**?*

No: Tor Browser initially provides anonymity, but if you log into internet accounts (e.g., your email account) or identify yourself through other ways (e.g., Googling your name) in Tor Browser, you will reveal your identity. But when used correctly, Tor Browser provides strong privacy protections: law enforcement has successfully caught some criminals who commit crimes using Tor Browser [50], but such investigations are time-consuming and expensive.

*What if I **accidentally log into an account** using Tor Browser?*

To become anonymous again, you should clear Tor Browser of all account-related data by either quitting Tor Browser or by clicking the "New Identity" button.

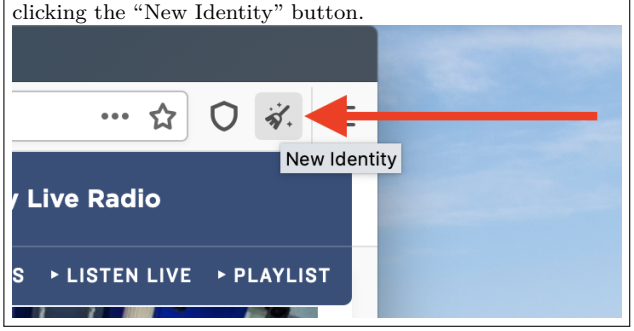

Fig. 18. We use an FAQ to address common misconceptions about Tor Browser, particularly those identified by Story et al. [67].

Common Problems
- Browsing with Tor Browser will be **a bit slower**. This is because Tor Browser protects your privacy by routing your browsing through different servers around the world.
- **Some websites block Tor Browser users**, since spammers sometimes use Tor Browser. If this happens, we recommend trying to use a different website.

Fig. 19. We briefly addressed two common challenges to using Tor Browser [21, 83]. Norcie et al. and Gallagher et al. suggest that making users aware of such usability issues may make users more willing to tolerate them in exchange for greater privacy [21, 44]. Awareness of these issues may also help participants form accurate perceptions of response cost [42].

In Survey #2, you indicated that you [did not have][did not know whether you had] Tor Browser installed on any of your devices.

Since completing Survey #2 on $DATE, **have you installed Tor Browser**?
(Yes, No)

[If Yes] Please explain why you installed Tor Browser.
_____

[If No] Please explain why you did not install Tor Browser.
_____

If you are interested in installing Tor Browser but require technical assistance, you are welcome to message us on Prolific to request help.

Rate your level of disagreement or agreement with the following statement:
"I intend **to install** Tor Browser in the next week."
(Strongly disagree, Somewhat disagree, Somewhat agree, Strongly agree)

Since completing Survey #2 on $DATE, **have you used Tor Browser**?
(Yes, No, I don't know)

Since completing Survey #2 on $DATE, **on which days did you use Tor Browser**, if any?
($DATE, $DATE - 1, $DATE - 2, . . .)

[If Yes (i.e., used Tor Browser)]
Please explain why you used Tor Browser.
_____

[If No (i.e., did not use Tor Browser)]
Please explain why you did not use Tor Browser.
_____

[If I don't know (i.e., whether they used Tor Browser)]
Please explain why you do not know whether you used Tor Browser.
_____

[PMT+AP Group, if wrote at least one activity]
In Survey #2, you made a plan to protect your privacy when performing privacy-sensitive browsing activities.

Since completing Survey #2 on $DATE, which of the following privacy-sensitive activities **have you performed**, if any?
($ACTIVITY_1, $ACTIVITY_2, $ACTIVITY_3)

[If performed $ACTIVITY_N]
When performing the [first/second/third] activity ("$ACTIVITY_N"), **did you use Tor Browser**?
(Yes, No, I don't know)

[If No (i.e., did not use Tor Browser) or I don't know (i.e., whether they used Tor Browser)]
Have you ever **tried to use** Tor Browser?
(Yes, No, I don't know)

[If used or tried to use Tor Browser]
Which of the following challenges have you encountered when trying to use Tor Browser, if any?
I did not encounter any challenges, Websites were extremely slow, Websites did not work, Other:_____)

[If multiple choices were selected]
Which of these challenges was the greatest obstacle to using Tor Browser?
(Websites were extremely slow, Websites did not work, Other: "$OTHER_CHALLENGE")

[If PMT+AP+CP Group, and Websites were extremely slow]
[Figure 5, left]

[If PMT+AP+CP Group, and Websites did not work]
[Figure 5, right]

[If PMT+AP+CP Group, and Other]
[Figure 20]

Other challenges

In a few sentences, describe the other challenge(s) you encountered when trying to use Tor Browser.

———

Take a couple minutes to identify ways to overcome the challenge(s). It may be helpful to search the web for solutions.

In a few sentences, write a plan to overcome the challenge(s).

———

Check the box below after telling yourself:
[ ] If I **encounter challenges**, then I will **follow my plan** to overcome them.

Fig. 20. We encouraged participants in our PMT+AP+CP condition who encountered challenges using Tor Browser to form coping plans to overcome the challenges [12, 60]. This plan template was shown to participants who reported encountering a challenge other than those we listed. The template gives participants the opportunity to mentally rehearse their plan in an "if-then" format [24, 45, 57].

If you want to use Tor Browser in the coming week, we encourage you to fill out the plan, since it may help you overcome challenges associated with using Tor Browser. However, you do not have to fill out or use the plan if you do not want to: your compensation will not be affected. Do you want to continue without filling out the plan?
(Yes, I would like to continue without filling out the plan)

Rate your level of disagreement or agreement with the following statement:
"I intend **to use** Tor Browser in the next week."
(Strongly disagree, Somewhat disagree, Somewhat agree, Strongly agree)

[If PMT+AP+CP Group, and reported a challenge]
This is a link to your plan(s) for using Tor Browser:
My Plan(s) for Using Tor Browser
(Information about your latest plan will appear shortly after you submit this survey)
Would you like us to send you a message on Prolific containing this link?
(Yes, No)

A.1.4 Survey 4

Researchers at Carnegie Mellon University are conducting a research study to understand people's use of web browsing-related tools.

This survey is Survey #4 in the "Research Study for Internet Users" that you previously gave your consent to participate in. It will take up to 3 minutes to complete this survey. If you complete this survey **within 2 days of the survey invitation**, you will be compensated $3.50 total for participating in our study.

There are no right or wrong answers to any of our questions, so please answer honestly. Also, **please take the time to read the information in this survey carefully**.

[Installation and usage checkup, the same as in Survey #3]

[Action plan checkup, the same as in Survey #3]

[If PMT+AP+CP Group, and made the "Websites were extremely slow" plan]
In Survey #3, you made a plan to click the "New Circuit" button if you encountered extremely slow websites when using Tor Browser.

Since completing Survey #3 on $DATE, did you encounter extremely slow websites when using Tor Browser?
(Yes, No, I don't know)

[If I don't know]
Please explain why you do not know whether you encountered extremely slow websites when using Tor Browser.

———

Since completing Survey #3 on $DATE, did you click the "New Circuit" button?
(Yes, No)

[If PMT+AP+CP Group, and made the "Websites did not work" plan]
In Survey #3, you made a plan to use alternative websites if particular websites did not work for you in Tor Browser.

Since completing Survey #3 on $DATE, which of the following websites did you **try to visit with Tor Browser**, if any?

($ORIGINAL_WEBSITE_1,
$ORIGINAL_WEBSITE_2,
$ORIGINAL_WEBSITE_3)

[If $ORIGINAL_WEBSITE_N]
Since completing Survey #3 on $DATE, did **$ORIGINAL_WEBSITE_N** work when you tried to visit it with Tor Browser?
(Yes, every time I tried to visit it; Yes, but only some of the times I tried to visit it; No, it never worked)

Since completing Survey #3 on $DATE, which of the following **alternative websites** did you try to visit with Tor Browser, if any?
($ALTERNATIVE_WEBSITE_1,
$ALTERNATIVE_WEBSITE_2,
$ALTERNATIVE_WEBSITE_3)

[If PMT+AP+CP Group, and made the "Other" plan]
In Survey #3, you described the challenge(s) you encountered when trying to use Tor Browser:
"$CHALLENGE"

Since completing Survey #3 on $DATE, did you encounter the challenge(s)?
(Yes, No, I don't know)

[If I don't know]
Please explain why you do not know whether you encountered the challenge(s).

____

In Survey #3, you described your plan to overcome the challenge(s):
"$PLAN"

Since completing Survey #3 on $DATE, did you follow your plan?
(Yes, Mostly yes, Mostly no, No)

[If formed an action or coping plan]
Were your plans helpful or not helpful? Please explain in a few sentences.

____

Rate your level of **disagreement or agreement** with the following statement:
"I think I have control over my online privacy."
(Strongly disagree, Somewhat disagree, Somewhat agree, Strongly agree)

What do you think is **the likelihood** of others observing your web browsing activity?
(Very unlikely, Somewhat unlikely, Somewhat likely, Very likely)

How **concerned or unconcerned** would you be if others observed your web browsing activity?
(Not at all concerned, Slightly concerned, Moderately concerned, Very concerned)

Rate your level of **disagreement or agreement** with the following statement:
"I think I know how to use Tor Browser."
(Strongly disagree, Somewhat disagree, Somewhat agree, Strongly agree)

How **easy or difficult** do you think it would be for you to use Tor Browser?
(Very difficult, Somewhat difficult, Somewhat easy, Very easy)

Rate your level of **disagreement or agreement** with the following statement:
"If I use Tor Browser, I will prevent others from observing my web browsing activity."
(Strongly disagree, Somewhat disagree, Somewhat agree, Strongly agree)

Rate your level of disagreement or agreement with the following statement:
"I intend **to use** Tor Browser in the next week."
(Strongly disagree, Somewhat disagree, Somewhat agree, Strongly agree)

Would you like to share any other thoughts about this study or about Tor Browser?

____

You are eligible to complete a final, optional survey (Survey #5), which would take up to 3 minutes to complete. If you complete Survey #5 **within 7 days of being invited**, you will be compensated **an additional $1**. You would receive your invitation in three weeks.

Your compensation will not be otherwise affected: you will receive $3.50 of compensation shortly after completing this survey (Survey #4).

Would you like to be invited to Survey #5 in three weeks?
(Yes, No)

A.1.5 Survey 5

Researchers at Carnegie Mellon University are conducting a research study to understand people's use of web browsing-related tools.

This survey is Survey #5 in the "Research Study for Internet Users" that you previously gave your consent to participate in. It will take up to 3 minutes to complete this survey. If you complete this survey **within 7 days of being invited**, you will be compensated $1.

There are no right or wrong answers to any of our questions, so please answer honestly. Also, **please take the time to read the information in this survey carefully**.

[Installation checkup, the same as in Survey #3]

[Note that for the use and plan checkups, we only ask about activity in the past week, since multiple weeks had passed since Survey #4. See an example below.]
In the past week, **have you used Tor Browser**?
(Yes, No, I don't know)

[Use checkup, the same as in Survey #3]

[Action plan checkup, the same as in Survey #3]

[Coping plan checkups, the same as in Survey #4]

Rate your level of **disagreement or agreement** with the following statement:
"I think I have control over my online privacy."
(Strongly disagree, Somewhat disagree, Somewhat agree, Strongly agree)

What do you think is **the likelihood** of others observing your web browsing activity?
(Very unlikely, Somewhat unlikely, Somewhat likely, Very likely)

How **concerned or unconcerned** would you be if others observed your web browsing activity?
(Not at all concerned, Slightly concerned, Moderately concerned, Very concerned)

Rate your level of **disagreement or agreement** with the following statement:
"I think I know how to use Tor Browser."
(Strongly disagree, Somewhat disagree, Somewhat agree, Strongly agree)

How **easy or difficult** do you think it would be for you to use Tor Browser?
(Very difficult, Somewhat difficult, Somewhat easy, Very easy)

Rate your level of **disagreement or agreement** with the following statement:
"If I use Tor Browser, I will prevent others from observing my web browsing activity."
(Strongly disagree, Somewhat disagree, Somewhat agree, Strongly agree)

Rate your level of disagreement or agreement with the following statement:
"I intend **to use** Tor Browser in the next week."
(Strongly disagree, Somewhat disagree, Somewhat agree, Strongly agree)

What is your overall opinion of Tor Browser? Has your opinion changed since the beginning of the study?
(Please write a few sentences)

_____

Would you like to share any other thoughts about this study or about Tor Browser?

_____

A.2 Insignificant Effects on Perceptions of Tor Browser

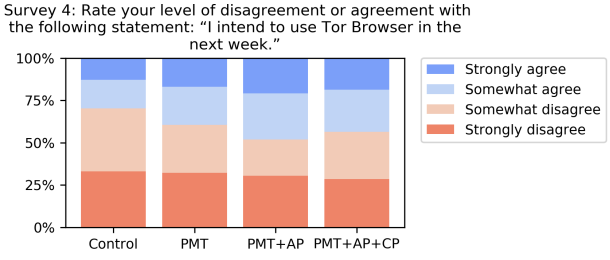

Fig. 21. This question measured intention to use Tor Browser. We did not find statistically significant differences in Survey 4.

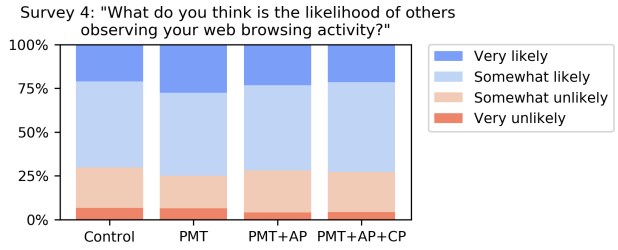

Fig. 22. This question measured perceptions of threat susceptibility. We did not find statistically significant differences in Survey 4.

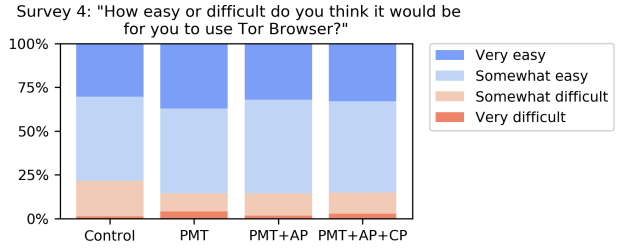

Fig. 23. This question measured perceptions of self-efficacy. We did not find statistically significant differences in Survey 4.

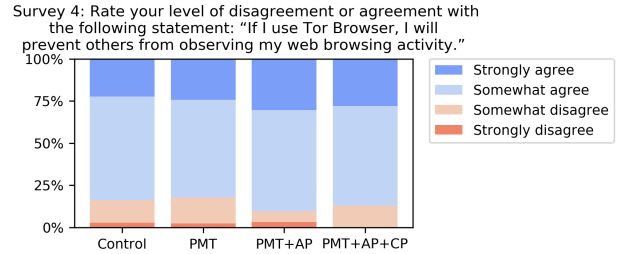

Fig. 24. This question measured perceptions of response efficacy. We did not find statistically significant differences in Survey 4.

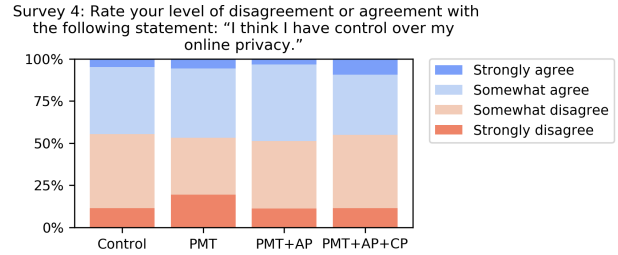

Fig. 25. This question measured perceptions of privacy control. We did not find statistically significant differences in Survey 4.