Poster: When Brave Hurts Privacy: Why Too Many Choices do More Harm Than Good

Anna Lena Fehlhaber, Yasemin Acar, and Sascha Fahl
Leibniz University Hannover
Email: {lastname}@sec.uni-hannover.de

Marco Gutfleisch, Daniel Theis, and Florian Wallkötter
Ruhr University Bochum
Email: {firstname.lastname}@rub.de

***Abstract*—Private browsing modes offer users various privacy features. However, users have misconceptions about what these privacy features can and cannot accomplish. They generally expect local and network protection, while private browsing modes only offer local protection by e.g., deleting browsing history after closing a browsing session. However, protection against network attackers is in fact provided by Tor. Non-power users are generally unaware of Tor and reluctant to install the Tor browser. As a hybrid, the Brave browser targets privacy-conscious end-users, and, in addition to a private browsing mode, allows users to use Tor-enabled session tabs. We conduct an exploratory online study to investigate users' perceptions of Brave's private mode and Tor-enabled sessions to investigate how much Brave's additional privacy features contribute to (further) misconceptions. We find that Brave's disclosures did not improve comprehension of privacy and security features; however, Help Center information did.**

***Index Terms*—Brave, Private browsing, Web browser privacy, Usable privacy, User study, Misconceptions**

I. Introduction

Private browsing is a standard functionality for many browsers such as Chrome, Edge, Firefox, Safari, and Opera. In most browsers' private modes, browser history is not stored locally and data caching across sessions is prohibited. However, contrary to users' expectations (which include protections offered by Tor), other privacy and security-related features are usually not offered by default in private mode [1]. Firefox, Opera and a relatively new browser named Brave provide additional privacy and security features [2]. The Brave Browser offers two private modes: One is comparable to classic private modes, the other offers additional Tor functionality. In an online study with 283 participants, we study user expectations for the three different Brave modes, and how these expectations change when users are shown Brave's new tab disclosure compares to Brave's Help Center explanation. We find that Help Center information improves comprehension, while the new tab disclosure does not.

II. Main Objectives

1) Considering that general misconceptions about private browsing functionalities are common [3]–[5], we query how end-users understand the different modes of Brave, which is, to the best of our knowledge, not researched.
2) We aim to identify conceptions and misconceptions regarding privacy and security issues for each of Brave's modes (Standard, Private, Private with Tor, cf. Figure 1).
3) Observation of influence of different disclosures on the comprehension of Brave's browser mode functionalities.
4) Observation of influence of official information material on the comprehension of Brave's browser mode functionalities.
5) Understand user's mental models regarding the Brave browser and help to prevent further misconceptions, deriving suggestions about which of the existing information material or disclosure will lead to as most as possible correct conceptions regarding the particular browsing mode.

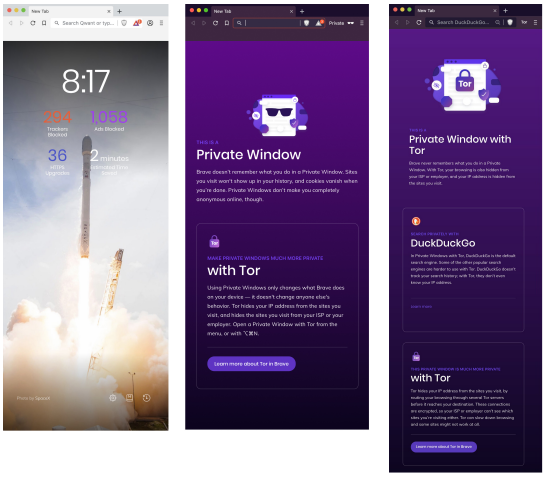

Fig. 1. Disclosures for default, private and private window with Tor mode

III. Materials and Methods

To study conceptions and misconceptions of Brave's different modes, we used the official information material from Brave's Help Section as well as the official disclosure as stimuli material. Accordingly, eight different conditions were assessed.

Within these, we faced our participants with nineteen different everyday scenarios adapted from [3], covering general usage, loading speed, and privacy and security features regarding availability, visibility, and data retention.

For the purpose of our study we cloned the original Brave website (*Home*, *Features*, *Creators*, *About*, *FAQ*, and *Community*) to our own servers and embedded it into an iframe.

Thusly, we were able to give the participants the opportunity to learn something about the Brave browser in a way Brave's developers intended to, while we still had full control and were able to track the participants' behavior.

To assess the data, we have conducted within-subject (for the scenarios) and between-subject (for the experimental conditions) analysis. We pre-tested our design and improved it according to our participants' feedback.

A formal IRB/IEC process was unfortunately not possible due to not being available at our institute. Hence, we used available best practices from the Menlo report, as well as the guidelines for academic requesters outlined by MTurk workers to ensure ethical principles. Additionally, we adhered to the strict German and U.S. data and privacy protection laws and the General Data Protection Regulation in the E.U. whilst designing and conducting the study, and handling the data.

IV. Analysis and Results

We recruited 283 participants from MTurk and were able to gain 233 valid datasets from it. We erased datasets of participants who claimed to be dishonest or inattentive, as well as those with a completion rate less than 80%. For our analysis, we further prepared our dataset and checked for outliers before doing inductive statistics.

We investigated the reasons and preferences regarding the usage of privacy and security enhancing features and asked our participants their personal reasons for doing so. Our participants claimed that NSA surveillance is a more relevant motive to use private browsing than monitoring at workplace. Noteworthy, Tor network renown is variant. Nearly half of our participants at least agreed with the statement, that they are familiar how the Tor network works. Surprisingly, that are more participants than the amount who stated to have heard, but made no experience with Tor.

To analyse the conceptions and misconceptions, we summed up the correct answers given for the scenarios and analysed 1.) the correctness of privacy and security assumptions within a scenario 2.) the correctness of assumptions within an experimental condition, e.g., normal, private, and Tor mode as well as with/without disclosures or additional information.

We used a random effect model and Pearson's χ^2 with Kruskal-Wallis (α=0.05) as well as Pearson's r for the contigency analysis to determine effect size. We corrected for multiple testing with Bonferroni-Holm. We found a highly significant correlation of Brave's mode and correct answers given (Kruskal Wallis' Chi-squared = 21.307, df = 7, p-value $<$ 0.01). We compared the same for conditions and found a less clear indication (Kruskal-Wallis chi-squared = 1.2677, df = 2, p-value = 0.53). Thus, the differences between each modes are more probable than a general difference for all conditions. Further analysis revealed that the indicated significance of Kruskal Wallis can be explained with Mann-Whitney-Wilcoxon post-hoc, which showed more correct answers for participants in normal and Tor conditions (W = 3818, p-value = 0.01 and W = 7951, p-value $<$ 0.01). When we modelled the scenarios as random intercepts we picked best-fitting models (AIC less than 1142.409, BIC less than 1166.566) for our random effect model to optimize further. The final random effect model included condition (disclosure/Help Center information material/control), browsing mode (normal/private/private with Tor), and prior touch points (heard about the assigned Brave mode/experienced the assigned Brave mode) with robust standard errors for the parameter estimates and recalculated p-values.

We found several misconceptions and non-misconceptions throughout the scenarios: Most existing misconceptions seem to persist for modified cookies visible in a default Brave session. Additionally, chi-square-testing revealed a significance for hiding the IP address from visited websites and the online shopping scenario when comparing private without anything and private with disclosure (chi-square 0.044 and 0.048). For non-misconceptions, the relatively high correctness of answers for meta stored data (cookies) takeover from a default browsing session, IP accessibility of the service provider, and website's tracking behavior through different browsing modes indicate a correct mental model.

We analysed these misconceptions compared between our experimental conditions and thereby were able to identify that there was no significant improvement of presenting the mode's corresponding disclosure on user's mental model correctness, thus, users were not able to gain or process the information needed to correct their assumptions about browsing modes. Even worse, the private mode disclosure showing up when opening a new tab in a Brave's private browsing session significantly decreased our participant's mental model correctness (p=0.0001). Hence, we suggest to redesign the disclosure to avoid further misconceptions. While the disclosures had no or a negative impact, the relatively new Help Section's additional and short explanations were able to significantly improve the correctness of answers regarding the mode's functionalities, indicating a revision of respective mental models. We tested for the overall effect of showing Help Center information and found degree of freedom and chi-square test to be significant ($p < 0.01$), indicating the Help Center information to be a statistical significant predicTor. Accordingly, integrating the Help Section's content into the existing disclosures or even replace the disclosures could improve the user's understanding of Brave's modes and enhance the correctness of conceptions about Brave's private browsing modes.

References

[1] A. Rao, F, Schaub, N. Sadeh, A. Acquisti, and R. Kang.; Expecting the Unexpected: Understanding Mismatched Privacy Expectations Online.; SOUPS'16.

[2] E. Bursztein. "Understanding how people use private browsing." https://elie.net/blog/privacy/understanding-how-people-use-private-browsing/, 2017.

[3] Wu, Justin and Zappala, Daniel, "When is a Tree Really a Truck? Exploring Mental Models of Encryption," SOUPS'18.

[4] Gao, Xianyi and Yang, Yulong and Fu, Huiqing and Lindqvist, Janne and Wang, Yang; Private Browsing: an Inquiry on Usability and Privacy Protection.; CCS'14

[5] Abu-Salma, Ruba and Livshits.; Evaluating the End-User Experience of Private Browsing Mode.; CHI'20