Why Johnny Isn’t (Switching to) Brave

Jonathan Liu
jonliu@uchicago.edu
University of Chicago
Chicago, Illinois, USA

ABSTRACT

Convincing users to adopt a browser with privacy by default is a potent avenue for increasing user privacy. From a technical standpoint, browsers control, load, and (to some extent) vet the data both sent and requested by the user as they interact with the internet, making them a natural domain for protecting the user from both malicious scripts and malicious websites. From an psychological standpoint, users tend to prefer defaults, so a browser that defaults to more privacy-preserving settings will allow users to keep their data more secure without extra consideration, especially as the landscape of the internet evolves. From a social standpoint, browser choice can be an individual decision, in contrast with messaging applications or social media platforms that require peer adoption to provide functionality. Of course, convincing users to change their behavior remains an inherently difficult task, even given promises of increased security.

In this work, we present an introductory investigation into the task of convincing users to adopt a more secure browser. We interview a set of browser users about their usage habits, conceptions of privacy, and beliefs related to the privacy afforded to them by their browser. Next, we present a lightweight intervention intended to clearly demonstrate the privacy protections built into a secure browser, Brave, by default. We aim to demonstrate to users that they can have more privacy with minimal changes in user experience. Through this process, we find that the intervention effectively demonstrates the capabilities of Brave, but that most users find the initial process of logging into accounts on a new browser too large of a cost to make switching browsers worth it. Users indicate awareness of tracking and little perceived threat resulting from it, thus making the benefits of Brave insufficient to outweigh the cost.

CCS CONCEPTS

• **Security and privacy → Browser security**; **Social aspects of security and privacy**; *Usability in security and privacy*.

KEYWORDS

Browser Security, Brave Browser, User Privacy Beliefs and Practices

ACM Reference Format:
Jonathan Liu. 2023. Why Johnny Isn’t (Switching to) Brave. In *Proceedings of CMSC 33250: Introduction to Computer Security V. 1, Winter, 2023, Chicago, IL, US.*. ACM, New York, NY, USA, 9 pages. https://doi.org/00.0000/0000000.0000000

Introduction to Computer Security, Winter 2023, Chicago, IL, US.
© 2023 Association for Computing Machinery.
ACM ISBN 000-0-0000-0000-0/00/00…$0.00
https://doi.org/00.0000/0000000.0000000

1 INTRODUCTION

Users have a well-documented history of not following privacy-preserving practices [15, 22], even when they claim to be generally conscious of privacy. Many users are simply unaware of these better practices or services, but perhaps more telling is the large portion of users aware of secure protocols or applications but unwilling to adopt them. For protocols and services like encryption [4], password managers [3], and secure communication [1, 10, 14], much work has attempted to explain user concerns preventing the adoption of these more secure practices.

The modern web browser serves as the gateway between users and the vast expanse of the internet. Most users nowadays not only frequently use a web browser on their computer but also have access to a web browser through their phone, greatly increasing their interaction possibilities. Browsers also play a crucial intermediary role in sending, receiving, and vetting interactions with the internet requested by the user. With the increased functionality of webpages and accessibility of the internet comes a larger and less-informed attack surface in everyday users, giving the browser much more potential for protecting the user from malicious scripts or adversaries. On the other hand, because these malicious scripts have significant incentive to remain undetected to the user, and browsers serve as a passive, static portal to the internet, privacy threats and protections are likely of low concern to both browser developers and everyday browser users.

We believe browser choice is a potent and understudied avenue for helping users better ensure their privacy on the internet. Unlike other changes that either require peer adoption (e.g. messaging applications) or consistent investment (e.g. disabling cookies, selecting vendors/websites with more protections), a user changing browsers may experience an initial cost in adoption but will likely quickly become familiar with the browser and has no need to convince others to use it or change their browsing habits. Though social factors like popularity of browser will always present a factor in the decision-making progress, they may be more insulated from this due to the lack of interaction between different users’ browsers.

On the other hand, the adoption of a secure browser can provide substantial benefits to a user’s privacy. Though different common browsers provide various levels of privacy protection, Brave has proven itself to be the most security-focused, both with its built-in Ad-blocker and tracker disabling [26], as well as its commitment to not sharing any user data with its own backend servers [19]. More importantly, as the internet landscape changes and tracking methods become more sophisticated, a user on a privacy-by-default browser will remain protected with no extra learning or habit changes necessary on their end.

We explore the possibility of an intervention convincing users to adopt a more secure browser. We first explore user conceptions of privacy especially with relation to their browser, attempting to understand both user threat models on the internet and the extent to which they believe their browser mitigates it. Then, we utilize a simple intervention to demonstrate the effectiveness of the Brave browser in blocking privacy threats while browsing the internet, and analyze the extent to which the intervention motivates users to switch browsers.

Through our interviews, we find that user inertia with their current browser and ambivalence towards trackers for advertisements are the primary impediments to adopting a more secure browser. Though our study participants indicated a general awareness of trackers online, they express only mild annoyance at their existence and view them as generally neutral, occasionally positive and occasionally negative. Furthermore, they expect the process of switching browsers to have high initial cost in the form of being forced to re-authenticate themselves for any service they hope to use. Though users only view an upfront cost for switching browsers, the lasting benefit from Brave's privacy protections do not mitigate enough threat for users to consider a switch worthwhile. That said, users viewed the intervention as illuminating and convincing, and stated that they would strongly consider using Brave if they could overcome the inertia.

In this paper, we describe our research process. First, we provide a summary of notable related research, both in the scope of user privacy decisions and in browser security. Next, we describe our interview protocol and participants. We then present results from our interviews, organized in terms of how they provide insight to the research questions presented above. Finally, we present some key takeaways from our investigation alongside potential future research directions.

2 RELATED WORK

2.1 Barriers to User Privacy

The Privacy Paradox, introduced by Barnes, describes a sharp disconnect between the degree to which users desire data privacy and the degree to which their actions online actually keep their data private [5]. Barnes explores this through the lens of teen social media participation, but it can be generalized broadly in the modern internet as companies extract more data from their users and policies struggle to protect them. In order to help users make privacy-preserving choices on the internet, users must both be appropriately informed about the potential risks of sharing their data and have the autonomy to make decisions by weighing the risks and benefits.

Exploring how users make decisions about secure procedures, Abu-Salma et al. find that potential users have many misconceptions regarding the security guarantees of cryptographic protocols implemented by secure communication channels, which can limit their interest in adopting said channels [1]. Furthermore, beyond the scope of understanding the protocol, users have many other issues to weigh in their decisions, such as cost and perceived threat [1, 7]. Users also tend to stick to defaults, and providing users with more secure defaults can increase their privacy [2]. Perhaps surprisingly, [24] finds that user confidence in security knowledge affects secure behavior far more than actual knowledge in the area does.

Table 1: User Share among Major Browsers (and Brave) [27]

Browser	% of Total
Google Chrome	65.76%
Apple Safari	18.84%
Microsoft Edge	4.28%
Mozilla Firefox	2.93%
Brave	<0.01%

Even so, it is a worthwhile endeavor to try to convince users to adopt more secure practices. Many studies have explored the adoption of secure messaging systems, largely finding that users maintain misunderstandings and mistrust of secure systems, and prioritize peer adoption over security guarantees [1, 10, 14]. Similarly, in broad security habits [15] and specific settings like encryption [4], differential privacy [8, 12], and multiparty data sharing [16], users maintain incorrect models of their security and value usability or moral factors over privacy concerns.

2.2 Browser Security

Modern internet surfers are tracked by all kinds of scripts and cookies, allowed in order to ensure a smooth web experience but coming with the cost of very low privacy. Users can have their device information, browsing habits, and even location exposed and carried between websites by trackers [20].

To address this, many different privacy-protecting systems have been proposed. To improve browsers, solutions have been developed that address common issues like fingerprinting [6], content blocking [25], and malicious extensions [23]. On a broader scale, systems like Tor [11] and its corresponding browser have been developed to promote user privacy through anonymity.

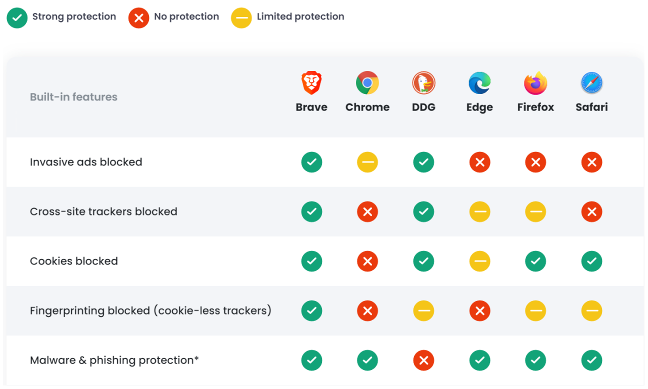
Some research has been done into the user experience with Tor. Studies have found usability issues with the launcher [18], with many UX concerns on the browser like latency and broken websites [13], and lack of understanding of the system [28]. These, coupled with the broad view of Tor as an entry point for criminals, make Tor an unappealing alternative for users, despite its perceived security. Outside of Tor, we could not find any research done on how users select or interact with secure browsers.

2.3 Browser Comparison

The browser market is very top-heavy. In February 2023, an estimated 65.76% of online users were browsing on Google Chrome, and an estimated 18.84% of users browsed on Safari [27]. In the same survey, Brave represented less than 0.01% of users. Brave claims to have 50 million users per year [26]. More can be found in Table 1.

2.4 Brave Browser

The Brave browser is a recent privacy-focused browser. In the pursuit of a more private online browsing experience, Brave has developed many features aimed at ensuring continuity of user experience alongside privacy protection. For example, Brave's browser has shown to have stronger native fingerprinting protection [17], developed robust tracker blocking systems [25], and, in a study with the browsers listed above and Yandex (a browser primarily popular for Russian speakers), was the only browser where no identifiable trackers were being transmitted between an instance of the browser and its backend servers [19]. More privacy features and comparisons with other major browsers can be found in Figure 1.



✓ Strong protection ✗ No protection ⊖ Limited protection

Built-in features	Brave	Chrome	DDG	Edge	Firefox	Safari
Invasive ads blocked	✓	⊖	✓	✗	✗	✗
Cross-site trackers blocked	✓	✗	✓	⊖	⊖	✗
Cookies blocked	✓	✗	✓	⊖	✓	✓
Fingerprinting blocked (cookie-less trackers)	✓	✗	⊖	✗	⊖	⊖
Malware & phishing protection*	✓	✓	✗	✓	✓	✓

Figure 1: Protections Offered by Major Browsers and Brave [26].

3 METHODS

To explore user beliefs and behavior about browser-related privacy, we conduct semi-structured interviews with various browser users.

3.1 Research Questions

Our interviews are guided by the following research questions:

(1) How do users select browsers, and what incentivizes them to switch?
(2) What are users' current conceptions of benefits and threats with regards to internet privacy, and how do these beliefs affect their behavior?
(3) How do users believe browser choice affects online privacy?
(4) To what extent can an interactive demonstration of a secure browser's capabilities affect a user's browser choice?

3.2 Interview Procedure

The author conducted all interviews. Each interview followed the semi-structured format, using a starting set of questions to help guide and provide structure to the interview but allowing the interviewer to either add follow-up questions or omit questions to better obtain information informing conclusions to the research questions. Each interview lasted between 45 and 60 minutes. In this section, we describe the overarching structure to the interview.

3.2.1 Current Browser Usage. The interview begins by establishing some background of each participant as a browser user. We are primarily interested in what browser or browsers they use, whether it depends on device or task, and how often they use their browser(s), as these can provide important context for how they view their relationship with their browser(s).

3.2.2 Web Browser Privacy Beliefs. Next, we explore the participant's beliefs related to privacy, both broadly in the context of the internet as a whole and more specifically with regards to their browser choice.

We begin by evaluating the extent to which each participant's behavior matches the privacy paradox. To do so, we ask the participant how much they value privacy on the internet, the steps they take to protect themselves, and what they believe are best practices for privacy. In doing so, we intend to evaluate the degree to which each user believes they deviate from best practices, and compare it with their own valuation of privacy.

Next, we guide the participant in producing and explaining their perceived threat model with regards to internet privacy. We begin with a baseline threat: that some party is monitoring their browser history. From here, we ask each participant to evaluate the severity of the threat that this provides to their privacy, the potential adversaries or actors that can pose this threat, the frequency of this type of threat, and the likelihood that it could happen to them.

We then focus more specifically on beliefs related to browsers. We explore participant beliefs related to the interaction between privacy and their browsers. We are interested in the extent to which users believe browsers work to either protect or infringe upon their privacy, and the extent to which users believe this varies between browsers. We anticipate users believing that private browsing sessions (e.g. Chrome's Incognito Mode) are a tool provided by the browser to protect the user's privacy, so we also explore each participant's beliefs about the capabilities and limitations of these sessions.

3.2.3 Switching Browsers for Privacy Reasons. A primary goal of this work is to investigate the extent to which privacy concerns would motivate users to switch browsers. In this section of the interview, we explore this from two angles.

First, we explore each participant's habits about selecting and switching browsers. We ask them to recall the last time they switched browsers, why they did so, and what they would do if forced to switch again. We also investigate the considerations they value in different browsers, and the factors preventing them from switching browsers in the present day.

Next, we present participants with a set of four claims, each of which represents a threat to their privacy induced by their current browser but not by Brave. For example, one such claim is "Using your current browser, your device has a "fingerprint" that allows cookies and websites to uniquely identify you even if you are not logged in." For each claim, we ask participants to elaborate on their reaction to the claim and the extent to which it might motivate them to consider switching browsers if there was a usable alternative that did not allow the threat. We ask participants to evaluate the claims separately rather than cumulatively, preventing any effects caused by the ordering of the claims.

3.2.4 Brave Demonstration. In the final part of the study, we ask participants to briefly use Brave, allowing us to demonstrate its security and identify any lasting concerns with the browser not resolved by seeing its use. We ask participants to download Brave, set it up as if they were planning to switch, and open a private browsing window from the original browser alongside the Brave window. First, we ask users to go to a weather website, to demonstrate that location services still work on Brave. Then, we then ask participants to select an item to hypothetically shop for (most selected clothing), and proceed to do the exact same shopping trip on both browsers by searching for the same terms and visiting the same links. When the user has placed an item in their shopping cart in each browser, we ask users to open up the console on each browser and inspect the cookies. In every case, we see that the private browsing window has more cookies than the Brave browser, and many of the cookies have more stored values as well, and the non-Brave browser has cookies clearly designed to track users for ad purposes. In doing so, we provide a clear demonstration that Brave is protecting user privacy with more vigilance than their other browser. We conclude by asking participants about their reaction to their experience, their likelihood of switching to Brave, and their lasting concerns related to switching.

3.3 Interview Analysis

Interviews were recorded, but the author also took brief notes during each meeting, focusing on broad ideas as well as novel insights or recurring themes. After the interviews, the author collated recurring ideas, and identified particularly illuminating insights from participants. For each of these insights, the author referenced the recording to transcribe the exact wording of the participant. The primary goal of this process was to capture recurring themes between participants, but care was also taken to ensure that unique or varied perspectives between participants were not lost.

3.4 Participants

Our study is focused on the beliefs and behaviors of “average" browser users, which we interpret in this context as users who do not have backgrounds in computer science, computer security, or privacy. As such, the author performed convenience sampling to select 7 participants fitting the criterion above. All participants have a college degree, and all participants are either currently employed, or are in school pursuing a higher degree. Three participants identify as female and four participants identify as male, and their ages range from 24 to 60. All browse the web regularly, but none self-identify as experts related to internet browsers or computer security. Furthermore, none are active users of secure browsers. Only two participants were aware of the Brave browser prior to the interview (neither had understanding of its features), and while most had heard of "torrenting" as a practice, none had prior knowledge of the Tor browser.

3.5 Consent

Interviews were all conducted over Zoom. Before the interview started, participants were informed that their participation was completely voluntary and would provide no compensation, that they retained the right to end the interview at any time as well as the right to opt to not answer any particular question. Participants were also informed that the meeting would be recorded, and that data collected from the interviews would remain anonymous. All participants consented to being interviewed.

3.6 Limitations

Though this study aims to provide an exploratory view into user beliefs and behaviors regarding privacy in web browsers, the methodology of this study provides a number of limitations that affect both its broader applicability and the strength of its conclusions.

3.6.1 Size and Homogeneity. The small sample size of participants is a clear limiting factor in the conclusions of the study. Furthermore, all participants are well-educated, live in the US, and a large majority use Google Chrome as their default browser, especially on the web. As such, the population is not a representative sample of “mainstream" browser users, and the study likely does not explore many important perspectives, including different cultures and different levels of access to a browser.

3.6.2 Mode of Presentation. It is likely that interviewing participants non-trivially affects user perception of the threat posed by privacy concerns. After the interview, P5 remarked "if I had just read [the dangers mentioned by the interviewer] on a website I wouldn’t have cared at all, but this interview format really forced me to think about why I might care about my data being collected online, and made me seriously consider switching." This showcases the potency of an personal, deliberate exploration of privacy concerns in motivating a user to switch, but perhaps also implies that a less personal (and as a result scaleable) intervention like an advertisement will likely face larger barriers in nudging the broader public towards privacy-preserving behavior.

In sampling the author’s personal connections as participants in the study, the trust arising from personal relationships is also introduced as a potential confounding element. The fact that participants were not trained in Computer Science and were speaking with a personally trusted interviewer who they know studies Computer Science means that users were very likely to view the interviewer’s claims as both truthful and well-intentioned. If claims made by the interviewer about the privacy of a practice or browser were instead made by an online website or other source like Brave’s website, participants would likely have dismissed both the benefits of Brave or the dangers of their current browsing as exaggerated.

4 FINDINGS

We present our findings as answers to the research questions posed in Section 3.1.

4.1 How do users select browsers, and what incentivizes them to switch?

4.1.1 Users prefer default browsers, but are willing to switch following sufficiently meaningful experiences or events. Six out of the seven participants use the default browser on their phone, and all attribute this to the fact that it was already downloaded on their phone. Despite this, only P5 uses the default browser on their computer, Edge. For this user, defaults are the only choice in the matter: "*When it comes to technology, I just go with the most straightforward measure. I started with Internet Explorer, and when it went away it was replaced with Edge on my computer, so I used that.* " (P5).

Every other user uses Chrome, and was motivated to switch away from their computer’s default browser to Chrome by a specific personal intervention or experience. P1, P2, P4, and P7 were recommended the browser by a peer, but some cited more specific grievances with their original browser. P2, P6, and P7 noted specific dissatisfaction with the way that their default browser looked and performed, describing slower loading speeds and ugly interfaces, and P3 found that a specific flash game would not work on their original browser but performed well on Chrome. More generally, six out of the seven participants indicate that only a major lapse in functionality would convince them to switch today. On the other hand, P4, P6, and P7 all mention having been recommended a different browser impersonally, either through an advertisement or a video, and dismissing the recommendation without any consideration.

4.1.2 Users view the process of switching browsers as having high upfront cost. In discussing their current browsers, all users indicate that they never consider changing browsers unless directly prompted, describing a sense of inertia from their constant use of the browser that disincentivizes a migration. For P2, P3, and P4, the fact that no issues were being experienced with the current browser was sufficient explanation for not changing. P1, P5, and P7 also described a sense of familiarity with the basic actions and layout of the browser that they did not want to give up: "*It's like if I were to go to a different grocery store, I would shop much slower because I wouldn't know where to find anything*." (P5).

Many participants also worry about needing to transfer all of their credentials over to a new browser. P1, P2, P5, P6, and P7 all describe that logging in to all of their accounts on the new browser would present a major inconvenience, especially for older accounts: "*There are plenty of places where I would hope that the browser remembers my password because I haven't been recently so I can't remember it.*" (P6). The two users who did not bring up this concern, P3 and P4, are the only two participants who use password managers.

4.1.3 Users looking to switch would default to convenience or familiarity, instead of performance-related metrics. In the interview, we asked users to consider the hypothetical where they were forced to switch browsers. Surprisingly, only of the participants responded that they would attempt to evaluate browsers by specifications: P6 mentioned that cross-platform compatibility was important, so that would be their first priority, followed by functionality. The others all deferred to simpler approaches: P1, P3, P4, P5, and P7 all stated that they would use the next browser they were already familiar with, and P2 would ask a knowledgeable friend for their recommendation. For these participants, the motivation was similar to the effects described above - comfort is prioritized over potential benefits, and while some participants later mention metrics of interest like speed and appearance, none indicate willingness to attempt browsers that they were not previously familiar with. Furthermore, participants were explicitly asked if they would consider privacy when selecting a new browser - all said no, though P7 had some sense of a baseline: "*I probably wouldn't download a random browser off the internet because they probably just want my data, a certain level of trust is necessary.*" (P7).

4.1.4 Google's hegemonic position in web services and products plays a major role in retaining users with Chrome. Every participant in the study indicated that they regularly use both Google Search and Google Workspace tools. These factors play a perhaps inordinately large part in user preference for Chrome. P2, P3, P4, P6, and P7 cited the integration between Chrome and Google Workspace as the primary benefit: "*Chrome provides easy access to Gmail, and other interconnected features of internet life*" (P2). P1, P2, and P5 also associate browser quality with search quality: "*What I care more about is the user experience. I like Chrome a lot better, because [the search results] have pictures, and there are images on the side.*" (P1). Interestingly, these preferences seem to reflect relatively minor actualized benefits - the browser-product integration seems to amount to offline access of Gmail and Google Drive [9], which, though convenient, are likely rarely utilized by most users, and users of common competitor browsers can switch their browser's default search engine to Google Search. Discounting here the potential that Google may be discretely throttling their services on competing browsers [21], the benefits cited by users seem to amount to very minor perks and perhaps demonstrate Google's successful coalescence of the internet experience under their banner.

4.2 What are users' current conceptions of benefits and threats with regards to internet privacy, and how do these beliefs affect their behavior?

4.2.1 Users view the possibility of threats to online privacy as correlated with sensitivity of information. For many of the participants, an important factor in the lack of threat posed by the tracking is the belief that their browsing information is not sensitive. For P3, P5, P6, and P7, their lack of public importance greatly diminishes the value of online privacy: "*I would like to think that if I gained significant net value, I would spend more time being conscientious, or maybe going off the grid, but not now. What are they going to do with me? Let's be real.*" (P3).

For P1, P2, and P4, the lack of danger comes more from the mundaneness of their browsing habits: "*I don't think I'm looking up anything particularly sensitive.*" (P1). This was accompanied by a broader belief that only relatively non-sensitive information could be drawn from a user's browsing history. When asked about the types of information that could be deduced from a user's browsing history, all participants listed shopping habits and food interests, with three also mentioning their job and two mentioning their rough location. No participants viewed any of these characteristics as particularly sensitive information.

4.2.2 Users understand that they are being tracked online for the purpose of tailoring advertisements, but do not view it as a meaningful threat. All participants describe experience with situations where they are presented with advertisements for products they had been previously browsing for. Though all express mild annoyance, especially when repeatedly being presented with the same advertisement, none consider it to be a serious concern: "*I'm shopping on a website, and all of a sudden next day i see an ad on Facebook for the same thing. Clearly they're trying to use my data to get me to buy something. Sometimes it's a little creepy, but it doesn't really bother me.*" (P4). Some view it as a natural extension of non-internet advertisements: "*If you compare them to TV ads, in sports games half of the ads are tailored to main demographic anyway. It's targeted* *better [online], which is kind of creepy but slay.*" (P3). In fact, P3, P5, and P7 describe appreciation for the personalization: "*Sometimes I kind of like it. They know exactly what I want, even when I don't know I want it.*" (P7).

One particularly surprising attitude towards data privacy was the potential of social cues preventing privacy-ensuring behaviors. We saw above that social effects play a sizable part in influencing how users select browsers, but we also find evidence to suggest that it may cause users to avoid some browsers. P3 knew about DuckDuckGo as a potential safe browser option, but did not use it for social reasons: "I understand why people use DuckDuckGo, but I would not want to be associated with those people. My general social consciousness importance outweighs me using DuckDuckGo... [Using DuckDuckGo] feels like believing a tinhat, stressful conspiracy theory, and even though I know the tracking is real, it's still the conspiracy vibes that make me not use it." (P3). Though only one participant expressed this type of reservation, it still presents a meaningful barrier to adoption.

4.2.3 Users do see some benefits to privacy, especially with regards to more specific individual threats. Participants were not fully reckless online - all participants had a heightened sense of danger regarding financial applications and identity theft, and were willing to take extra precautions to prevent them. P1, P5, and P6 all express wariness about conducting any potentially sensitive business in public settings, expressing fears of eavesdropping both over-the-shoulder and across public networks. Three participants express the importance of remaining private on social media, and three participants take special care with their passwords in situations with sensitive information: "*If someone wants to see what I'm browsing I don't care, if someone wants to use my data I don't really care. I just don't want them to use my data to commit identity theft.*" (P4).

4.2.4 Chrome users view Chrome's Incognito Mode as a sufficient, on-demand privacy-ensuring practice, though they have some understanding of its drawbacks. Though P5 (who used Edge) had never heard of private browsing, all other participants indicated familiarity with the feature. These participants described using Incognito mode when searching for topics that they did not want to appear in their search history, for various reasons. P1 and P6 also indicate a belief that only using incognito mode is a "best practice" for maintaining privacy online. That said, participants also seemed aware of its drawbacks, citing the launch page for new Incognito windows that provide a brief description of the limitations. P1, P2, P3, and P7 all indicated awareness that Incognito still allowed websites and ISPs to track your information, with P3 even mentioning that this warning was what first let them know that they were being track online. P7 also identifies the futility of Incognito Mode for actual privacy: "*When you're on incognito mode, it doesn't automatically save in your history, but I think your ISP still knows, the site still gets your information, so it's not doing much. Maybe it's more of a mental thing.*" (P7).

4.3 How do users believe browser choice affects online privacy?

4.3.1 Users vary widely in the extent to which they believe that browsers provide functionality designed to protect user privacy. Because these are "mainstream" users, we do not expect users to maintain a complete understanding of or interest in the privacy mechanisms of their browsers. Nonetheless, we were surprised to find a spectrum of beliefs about the extent of their browser's protection. On one end, P5 believes that browsers make no attempts to protect your privacy, leaving it up to the user. P1 and P7 believe that browsers do very little, but have worked to give users more overt control over the cookies used on a page, citing the recent uptick in webpage banners related to cookies. Of course, these banners are implemented by the webpage and not the browser, and are likely a result of data regulation laws rather than browser protections. P3, P4, and P6 noticed warnings related to phishing when attempting to visit potentially suspicious websites, and P4 indicated belief that this demonstrated a broader commitment to user privacy. P2 believed that Chrome invested in user privacy for the sake of competition: "*Chrome probably has a lot of protections against external forces, but does not protect you from their internal mechanisms.*" (P2).

4.3.2 Users do not believe that browser choice has a large impact on user privacy. At least, users do not seem to be aware of differences in privacy protections between browsers they use, nor do they expect that any of the major browsers differ in this regard. For P3, P3, P4, and P7, this was a natural consequence of the fact that for-profit companies: "*I'm sure google sells your information, I'm sure Microsoft does it, they're big tech companies that can make a fortune and get away with it so why wouldn't they?*" (P7). Some participants also indicated a sense that the types of privacy violations occuring on each browser are mostly similar, but that the party collecting the data may differ. P2, for example, stated that because a search engine is closer to search inputs than a browser, that the extent to which the browser collected information may be dependent on which search engine was being used.

4.3.3 Users told about fingerprinting had varying reactions, but most found that it was unsettling but not enough so to switch browsers. Participants had mild reactions to learning about fingerprinting, though for varied reasons. For P1, P5, and P7, their belief that they had "nothing to hide" in their browsing history made fingerprinting seem benign, though they did express surprise that it was possible. For P2 and P3, this fit into their conception of how tracking worked, so it did not induce any increased concern - "*I knew about fingerprinting, you can do that with an IP address. I'm sure there's scarier stuff they do to track people anyway.* " (P3). For P6, this was not a concern because the solution was already provided: "*If I wanted [a browser that didn't fingerprint], I would switch to incognito mode, which I think is the same.*" (P6). For P4, however, learning about this was enough: "*that's so creepy, if this was happening I would switch 100 percent.*" (P4).

4.3.4 Users told about potential eavesdropping over HTTP and protection through HTTPS are unnerved by the potential of eavesdropping, but most still did not view it as a reason to switch. For P2, P6, and P7, this felt like a potential invasion of privacy, but the perceived magnitude of threat was low: "*That's a pretty big deal, but the odds of someone wanting to do it are low so it's not at the front of my mind.*" (P7), and P2 placed trust in the websites: "*if the information was important, I trust that my personal information would be handled well by the websites anyway.*" (P2). P5 was not convinced that this could be different between browsers, viewing browsers as a passive UI for accessing the internet with no other functionality. Both P1 and P4 indicated that it would convince them to switch if the magnitude of HTTP websites was high enough: "*My activity isn't necessarily incriminating, but... when people have access to that level of information, and know what you're trying to learn or trying to do, it feels like an invasion of my personal thoughts.*" (P1).

4.3.5 Users told that their browser was tracking and selling their data are largely ambivalent, mostly because it was known information. When participants were told that they were being tracked on their browsers at this point in the interview, every participant had already discussed knowledge of trackers used to target advertisements for users. With that in mind, every participant agreed that the use of trackers did not pose enough of an incentive for them to switch browsers.

4.4 To what extent can an interactive demonstration of a secure browser's capabilities affect a user's browser choice?

4.4.1 In the process of testing a browser, users can overcome some of the qualms about the initial cost of switching browsers. All users indicated that setup of the Brave browser was surprisingly easy, particularly because the browser allows the user to port default settings and bookmarks from other websites. Users did not seem particularly disappointed that extensions could not be ported over, and P3 even indicated that it would be a good opportunity to sort through their extensions and only keep the important ones. That said, the need to log in to every website again remains, particularly for those without password managers, which still presents a key barrier to users who want to switch.

In terms of user experience, users generally noticed no changes in functionality with Brave. Because six of the seven participants are currently Chrome users, the fact that Brave is built on Chromium allows for continuity of interfaces switching from Chrome to Brave: "*The user experience seemed very similar to Chrome. If anything, it seems more straightforward in terms of naively what you would expect there to be in a browser.*" (P2).

4.4.2 Our procedure for demonstrating Brave was successful in conveying the security benefits. All participants were impressed by the sharp contrast between the volume of trackers in an private browsing tab as opposed to on the Brave browser, and indicated that the demonstration was convincing in showcasing Brave's strengths: "*You can clearly see that [Chrome] is sending information to outside sources, like for ads, that Brave definitely doesn't have*" (P5).

Of the seven demonstrations, only one - P7 - had an instance where Brave's performance lagged significantly behind Chrome's: when visiting a storepage, Brave took around 20 seconds to load the page, whereas Chrome took less than 1 second. Though we could not replicate the performance issues, a glance at the error logs suggests that a tracker removed by Brave was causing loading issues. Though this annoyed the participant, when the interviewer guided the participant through the error logs on Brave and indicated the errors that were being caused by Brave blocking trackers, the participant appeared impressed with the outcome and noted that a pause for this reason was acceptable as long as it was not too frequent.

4.4.3 The demonstration made users more conducive to Brave, but largely did not fully convince them to switch. Though we are generally pleased with the outcome of the demonstrations, it still remains the case that users did not view privacy as enough of a concern to make any changes. For P1 and P3, the benefits were clear but not enough: "*This is very good if i want to keep my life more private, but I don't really care.*" (P1), "*Nothing bad has happened to me yet, but it's good to know.*" (P3). For P2 and P7, the cost of switching still seemed higher than the benefit: "*I would consider it if I had the willpower to move logins over.*" (P2), "*I don't notice who's tracking me or who's getting my information when I'm browsing. I may be fearful of change, and the threats just are not clear enough.*" (P7). More promisingly, P4, P5, and P6 indicated a willingness to stick with Brave, at least on a more extended trial run, all citing a sufficient presentation of the benefits: "*This is a good way to educate people - a real-world demonstration of the cookies and the tracking was very convincing.*" (P5).

5 DISCUSSION

In this section, we present key takeaways from our interviews, especially centered around how the results differ from those about how the results may be applied to encourage users to adopt more secure browsers.

5.1 Reception of Brave

Perhaps the most promising result from the interviews was the success of the demonstration in illustrating the privacy protections afforded by Brave. The intervention was short, flexible, and provided convincing real-world proof that trackers were following users and that Brave prevented this. Participants came out of the interview with a greater awareness of the trackers that followed them around, and the knowledge of an alternative that could prevent this from occurring. Participants also felt that the interface was familiar and intuitive, likely because of the similarities with Chrome.

No participants voiced concerns about functionality. That said, Brave's anti-tracker mechanisms have the potential to disrupt website functionality, as one participant witnessed during their interview. This participant did not leave doubting the general functionality of Brave, but it remains to be seen whether this kind of disruption would occur more commonly upon adoption and the extent of the chilling effects that it may have on potential users.

5.2 High Cost of Switching

We find that the most important barrier for users in switching browsers is the inertia with their current browser and the perceived high cost of switching to a new browser, especially in the form of re-authentication into all services. Even prior to the Brave demonstration, users generally did not believe that browsers would offer different levels of usability or security, with the exception of a couple of participants who disliked Internet Explorer and Edge. The fact that the barrier lies heavily in the user's individual incentives and interests contrasts with other similar user studies, like that of secure communication, where [1, 10] find that users are willing to switch to more private alternatives but find that peer adoption is a primary barrier. Furthermore, these studies find that many users view the pursuit of security as a futile endeavor, in the sense that even End-to-End Encryption is not sufficient to prevent capable adversaries from eavesdropping. Our results mirror this to some extent - we find indications that users view tracking as an inescapable part of the internet experience, but also seem convinced that Brave greatly limits the effectiveness of these trackers. As such, assuming applicability of the results in secure communication, we believe our results demonstrate that the cost of switching browsers is the only pertinent barrier.

That said, this does not make the task any easier, at least given current user password habits. Transferring passwords between browsers can be made much smoother if users rely on a password manager, but a 2017 study found that only 12% of Americans do [22]. For the users that don't, the adoption of a password manager can present even more of a habit-changing issue than simply changing browsers, and does not solve the problem of users hoping to rely on their browser for logins to websites long-forgotten.

On the other hand, this finding does present a potential, albeit narrow, opportunity for intervention. We find that users tend to stick with their default browser until a personal experience convinces them otherwise, and even users convinced to switch to Chrome on their computers largely remain on Safari on their phones. Thus, we believe it likely that users who are given Brave as a default browser would be inclined to continue using it, especially if they do not experience significant performance issues with the browser. At this point, it seems that Chrome users getting a new computer would default to downloading Chrome anyway, but for undecided or uncommitted users like P5 this would be a potential method to make them use Brave.

5.3 Lack of Privacy Concern

By and large, users did not view the usage of trackers for the purposes of advertisements as a substantial threat. Our interview avoided suggesting that it was a threat for fear of asking leading questions, but as a result we did not get a clear understanding of why users felt this way. Even so, we can draw some more nuanced conclusions from user approaches towards discussions about their browser history. Though users did not express any concern for the types of information that may be gleaned from their browsing history, some nonetheless expressed that the ability to eavesdrop fully on a user's browser history would be uncomfortable. Similarly, some users follow private habits on social media. As such, it should not be concluded that users have no concern for privacy - it is simply that tracking for the purposes of advertisement does not pose any immediate harm or danger. We speculate that this may be due to the facelessness of the tracker and the advertising company, as opposed to the threat imagined by real individual stalking another person online or reading another person's browsing history.

Users also indicated that a bad or dangerous experience would convince them to switch, but targeted advertisements will never do so. It is not clear that even a dangerous experience would fully do so - being part of a major password breach has shown not to influence a user's likelihood to take more secure measures with their passwords [22]. Participants in the study who use this data for their job indicated that they have access to details about users much more specific than they had expected - future work in the area may look at whether users outside of this industry believe that this is possible, and whether this threat of a specific employee at a company knowing one's attributes is enough of a realized privacy violation to justify switching browsers.

6 CONCLUSION

In order to ensure the privacy and security of everyday users, we must not only focus on protective measures but also develop interventions centered around encouraging user adoption. While the development and release of new technologies for insertion into default browsers can allow some progress, competing influences can still hinder their integration. For example, browsers interested in revenue through selling advertisements have a vested interest in enhancing the effectiveness of their advertisements through deployment and permission of trackers, at the cost of user privacy and data. This inherent conflict precludes the setting of browser choice from having a secure default, so it is important to investigate the potential for motivating users away from the hegemonic default. In this study, we find that users foresee a large activation energy in switching browsers, and though they are aware of the tracking present in their current browser, do not see it as damaging enough to warrant switching to a browser that actively prevents it. Yet, we present promising evidence that, following our intervention, users see Brave as a viable alternative with clearly increased security and no downsides in terms of user experience. All of our participants cited a specific, personal event that motivated them to switch to their current browser - it remains to determine if this kind of event can be imitated on a larger scale, or can occur naturally as a result of a privacy violation. We believe the adoption of a browser with security as its default allows the user to protect their privacy with minimal change in experience, and hope future work explores both barriers and incentives for users to better protect their privacy.

ACKNOWLEDGMENTS

We would like to thank Bailey Kacsmar, Blase Ur, and David Cash for their assistance guiding, shaping, and informing the research project.

REFERENCES

[1] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. 2017. Obstacles to the Adoption of Secure Communication Tools. In *2017 IEEE Symposium on Security and Privacy (SP)*. 137–153. https://doi.org/10.1109/SP.2017.65

[2] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. 2017. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Comput. Surv.* 50, 3, Article 44 (aug 2017), 41 pages. https://doi.org/10.1145/3054926

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

(Karlsruhe, Germany) *(EuroUSEC '21)*. Association for Computing Machinery, New York, NY, USA, 89–104. https://doi.org/10.1145/3481357.3481519

[4] Erinn Atwater, Cecylia Bocovich, Urs Hengartner, Ed Lank, and Ian Goldberg. 2015. Leading Johnny to Water: Designing for Usability and Trust. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security* (Ottawa, Canada) *(SOUPS '15)*. USENIX Association, USA, 69–88.

[5] Susan B Barnes. [n. d.]. A privacy paradox: Social Networking in the United States. https://firstmonday.org/ojs/index.php/fm/article/view/1394/1312

[6] Peter Baumann, Stefan Katzenbeisser, Martin Stopczynski, and Erik Tews. 2016. Disguised Chromium Browser: Robust Browser, Flash and Canvas Fingerprinting Protection. In *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society* (Vienna, Austria) *(WPES '16)*. Association for Computing Machinery, New York, NY, USA, 37–46. https://doi.org/10.1145/2994620.2994621

[7] Alastair R. Beresford, Dorothea Kübler, and Sören Preibusch. 2012. Unwillingness to pay for privacy: A field experiment. *Economics Letters* 117, 1 (2012), 25–27. https://doi.org/10.1016/j.econlet.2012.04.077

[8] Brooke Bullek, Stephanie Garboski, Darakhshan J. Mir, and Evan M. Peck. 2017. Towards Understanding Differential Privacy: When Do People Trust Randomized Response Technique?. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 3833–3837. https://doi.org/10.1145/3025453.3025698

[9] Google Chrome. 2023. Discover Chrome's Built-in Browser Tools. https://www.google.com/chrome/browser-tools/

[10] Alexander De Luca, Sauvik Das, Martin Ortlieb, Iulia Ion, and Ben Laurie. 2016. Expert and Non-Expert Attitudes towards (Secure) Instant Messaging. In *Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security* (Denver, CO, USA) *(SOUPS '16)*. USENIX Association, USA, 147–157.

[11] Roger Dingledine, Nick Mathewson, and Paul Syverson. 2004. Tor: The Second-Generation Onion Router. In *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13* (San Diego, CA) *(SSYM'04)*. USENIX Association, USA, 21.

[12] Daniel Franzen, Saskia Nuñez von Voigt, Peter Sörries, Florian Tschorsch, and Claudia Müller-Birn. 2022. Am I Private and If So, How Many? Communicating Privacy Guarantees of Differential Privacy with Risk Communication Formats. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (Los Angeles, CA, USA) *(CCS '22)*. Association for Computing Machinery, New York, NY, USA, 1125–1139. https://doi.org/10.1145/3548606.3560693

[13] Kevin Gallagher, Sameer Patil, Brendan Dolan-Gavitt, Damon McCoy, and Nasir Memon. 2018. Peeling the Onion's User Experience Layer: Examining Naturalistic Use of the Tor Browser. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (Toronto, Canada) *(CCS '18)*. Association for Computing Machinery, New York, NY, USA, 1290–1305. https://doi.org/10.1145/3243734.3243803

[14] Nina Gerber, Verena Zimmermann, Birgit Henhapl, Sinem Emeröz, and Melanie Volkamer. 2018. Finally Johnny Can Encrypt: But Does This Make Him Feel More Secure?. In *Proceedings of the 13th International Conference on Availability, Reliability and Security* (Hamburg, Germany) *(ARES 2018)*. Association for Computing Machinery, New York, NY, USA, Article 11, 10 pages. https://doi.org/10.1145/3230833.3230859

[15] Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 327–346. https://www.usenix.org/conference/soups2015/proceedings/presentation/ion

[16] Bailey Kacsmar, Kyle Tilbury, Miti Mazmudar, and Florian Kerschbaum. 2022. Caring about Sharing: User Perceptions of Multiparty Data Sharing. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 899–916. https://www.usenix.org/conference/usenixsecurity22/presentation/kacsmar

[17] Pierre Laperdrix, Nataliia Bielova, Benoit Baudry, and Gildas Avoine. 2020. Browser Fingerprinting: A Survey. *ACM Trans. Web* 14, 2, Article 8 (apr 2020), 33 pages. https://doi.org/10.1145/3386040

[18] Linda Lee, David Fifield, Nathan Malkin, Ganesh Iyer, Serge Egelman, and David Wagner. 2017. A Usability Evaluation of Tor Launcher. In *Proceedings on Privacy Enhancing Technologies - Volume 3* (Minneapolis, MN) *(PoPETs)*. 90–109.

[19] Douglas J. Leith. 2021. Web Browser Privacy: What Do Browsers Say When They Phone Home? *IEEE Access* 9 (2021), 41615–41627. https://doi.org/10.1109/ACCESS.2021.3065243

[20] Farhad Manjoo. [n. d.]. I Visited 47 Sites. Hundreds of Trackers Followed Me. *The New York Times* ([n. d.]). https://www.nytimes.com/interactive/2019/08/23/opinion/data-internet-privacy-tracking.html

[21] Johnathan Nightingale. 2019. [Tweet on Twitter:] But Google as a whole is very different than individual googlers. Google Chrome ads started appearing next to Firefox search terms. gmail & gdocs started to experience selective performance issues and bugs on Firefox. Demo sites would falsely block Firefox as "incompatible.". https://twitter.com/johnath/status/1116871243301625856

[22] Kenneth Olmstead and Aaron Smith. 2017. *Americans and Cybersecurity.* Technical Report. Pew Research Center.

[23] Nikolaos Pantelaios, Nick Nikiforakis, and Alexandros Kapravelos. 2020. You've Changed: Detecting Malicious Browser Extensions through Their Update Deltas. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (Virtual Event, USA) *(CCS '20)*. Association for Computing Machinery, New York, NY, USA, 477–491. https://doi.org/10.1145/3372297.3423343

[24] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. 2017. Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 2202–2214. https://doi.org/10.1145/3025453.3025926

[25] Michael Smith, Pete Snyder, Benjamin Livshits, and Deian Stefan. 2021. SugarCoat: Programmatically Generating Privacy-Preserving, Web-Compatible Resource Replacements for Content Blocking. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security* (Virtual Event, Republic of Korea) *(CCS '21)*. Association for Computing Machinery, New York, NY, USA, 2844–2857. https://doi.org/10.1145/3460120.3484578

[26] Brave Software. 2023. Secure, Fast, & Private Web Browser with Adblocker | Brave Browser. https://brave.com/

[27] statcounter GlobalStats. 2023. Browser Market Share Worldwide. https://gs.statcounter.com/browser-market-share

[28] Philipp Winter, Anne Edmundson, Laura M. Roberts, Agnieszka Dutkowska-Zuk, Marshini Chetty, and Nick Feamster. 2018. How Do Tor Users Interact with Onion Services?. In *Proceedings of the 27th USENIX Conference on Security Symposium* (Baltimore, MD, USA) *(SEC'18)*. USENIX Association, USA, 411–428.