

(Draft): Perceived User Benefits of Competing Ad-Blocking Strategies

Francis Djabri
Mozilla Corporation

Abstract – *Ad-blocking adoption has seen phenomenal levels of increase globally over the past several years. The advertising and technology industries have started to coalesce and respond to this threat by devising ad-blocking strategies that will block the most annoying forms of advertising by default. However, this approach only partially addresses the threats that Internet users perceive from online behavioral advertising, which is indicated by a long-standing and growing body of research. This research has demonstrated the complex and contextual nature of users' preferences and norms for how they disclose personal information, which points to an opportunity for browser technologies to offer a more nuanced approach in managing the data exchange between users and advertisers. This research attempts to directly inform the design of privacy protecting tools in the browser that go further towards meeting users' privacy preferences. 15 participants were recruited to evaluate and provide feedback on different ad-blocking approaches in the browser. The results indicated some commonly perceived bad advertising practices that users desire protection from that includes: interrupting and annoying ads, retargeted ads, malvertising and dishonest and misleading advertising.*

Index Terms – *online behavioral advertising, retargeted advertising, privacy protecting technology, ad-blocking, perceived privacy benefits.*

INTRODUCTION

Ad-blocking adoption has seen phenomenal levels of increase globally in the past few years. As of December 2016, there were over 600 million devices running ad-block software globally, 62% of which were on mobile devices (PageFair, 2017). There has been extensive research around the motivations behind ad-block usage, with interruptive ad formats and security and privacy concerns being the primary motivating factors [e.g., see PageFair report].

The rise in ad-block usage poses a threat to the advertising business model of the web and we are starting to see the industry responding to save it. For example, Google has partnered with the [Coalition for Better Ads](#), a

consortium of ad, publishing, and tech companies, with the aim of pre-installing selective ad-blockers on Chrome to purge the most annoying forms of advertising from the Internet and to stem the rise of more general ad-blockers or those with tracking protection features.

An ad-blocking strategy that focuses solely on alleviating annoyance based on interruption only goes so far, however, in protecting users. Such an approach still leaves users exposed to online tracking from site to site and does nothing to address their concerns around targeted advertising. Previous studies have consistently shown that people find the concept of targeted advertising to be invasive (McDonald and Cranor, Pew, Turow et al, other refs). A majority of American adults (66%) do not want marketers to tailor advertisements to them based on their interests (Turow et al, 2009). Attitudes are particularly negative towards the industry practice of *retargeting*, where ads are shown to users for products that they have encountered, either in the same browsing session or in a previous browsing session. These ads thereby appear to follow people around the web and are perceived as being more invasive and consequently cause greater negative reactions in Internet users than ads that are targeted based on demographics or interest (Barnard, 2014).

Nevertheless, previous research has also shown that people's attitudes and preferences towards behavioral advertising are complex, being perceived as being both useful and invasive at the same time (Ur et al.). Targeted ads can have the benefits of helping people discover novel products and furthermore many people are aware of the role that Internet advertising has in supporting free content, but at the same time they are uncomfortable for their data to be part of the exchange (McDonald and Cranor). Further research has shown that Internet users' preferences and norms for which data they are willing to share as part of the exchange are nuanced, highly individual and contextual (Leon et al).

The accumulated research suggests that binary approaches towards ad-blocking are unlikely to capture to complexity of Internet users' preferences. For example, Agarwal et al. reported that the overwhelming majority of their research participants preferred an ad-blocking approach that would still allow ads to be shown that

matched topics of their choice over one that blocked all ads indiscriminately, or that only blocked certain annoying ads (pop-up, pop-unders and distracting ads). An opportunity therefore exists for browsers to offer tools that better meet Internet users' preferences towards behavioral advertising – tools that allow for the benefits of behavioral advertising while still respecting users' privacy norms.

In summary, there has been extensive survey-based research done that shows that the existence of Internet users' concerns around being tracked by online advertisers, and some recent qualitative research that has revealed the nuanced, contextual and individualized nature of users' privacy preferences (Leon et al,) towards these advertisers. This research has suggested at the potential of privacy protecting tools that could better assist users in meeting their preferences over what data is exchanged to advertising networks, but there is a need for more research that directly informs the design of these tools and evaluates them from a user perspective. The research presented in this paper attempts to address this gap.

A range of potential approaches and strategies for managing the data exchange between Internet users and online advertisers exist. The goal of this research is to investigate how users perceive the relative value of these different approaches, and how they perceive the different trade-offs between utility, cost and privacy for each variant.

METHODOLOGY

In August 2017, we recruited 15 participants for a group-based card-sorting study and focused group discussion that investigated the relative value of different browser-based tools for managing online advertising. All the participants lived in Tulsa, OK, where the study was also conducted.

I. Card-Sorting Study

In this study, small groups of 3-4 participants are presented with different browser features that are shown on "feature cards". Each card describes a feature with a short name, a description that outlines the benefits of the feature, and a putative cost. The cost of each feature was calculated based on its relative implementation complexity, which was estimated by a team of Security engineers working at Mozilla Corporation on the Firefox browser.

Participants in each group are asked to imagine that they have subscribed to a premium Mozilla service and they have an allocation of credits with which to "buy" different features from the cards presented. Each group is given 1500 credits in total, which is enough to buy about around a third of the features on offer. The number of credits is deliberately limited in order to force the groups

to make decisions about which features are the most valuable to them. Each group must buy features for the group as a whole – the groups must therefore collaborate as a team to discuss the relative features and decide which features to buy.

After outlining the process to the group, the different features are presented on feature cards in a random order. The facilitator acts as a "shopkeeper" during each session and collects credits from the team as they buy features. The shopkeeper is permitted to answer questions that participants may have about the different features.

The study session continues until all the credits have been collected or all desired features have been bought. There is no requirement for the team to use all their credits if they so wish. Following this, key points from the earlier discussion are revisited and probed into further by the facilitator.

The following features cards were shown to participants:

Ad-Blocker

Description: Advertising has gone too far on the web – it's time to take action to stop it. This feature will block advertisements so that you no longer see them while browsing.

Cost: 100 credits

Selective Ad-Blocking

Description: Support the websites you care about. Part of your subscription fees will go directly to your favourite 10 websites and in return, Firefox will block all advertising on the sites that you include.

Cost: 1000 credits

Tracking-Blocker

Description: Make ads respectful of your privacy again. This feature will protect your privacy so that advertisers can't follow your movements around the web.

Cost: 375 credits

Firefox "Flow"

Description: Advertising has its place but it's ruining the web by interrupting and getting in the way of your browsing. This feature stops websites from showing ads that interrupt you – we put advertising back in its place.

Cost: 150 credits

Ad-Swapper

Description: Replace ads that you see on the web with ads from categories that interest you.

Cost: 1000 credits

Speed Booster

Description: Ads that track you on the web don't just invade your privacy, they also slow your browser down.

This feature prevents advertising from hogging your resources so that you can browse faster.
Cost: 100 credits

Total Privacy

Description: Ads in the real world know nothing about you. They don't know who you are, or anything about your habits or interests. Firefox will protect your privacy to make ads on the web just as dumb as ads in the real world.
Cost: 750 credits

Malvertising Protection

Description: Some ads on the web are not what they seem – they can be a way of spreading malware on your computer or phone, even on reputable websites. Firefox will help prevent threats from malware delivered by ad networks.
Cost: 750 credits

Community Moderation

Description: Firefox will block advertising from websites that receive complaints from the Mozilla community, so that you can browse in peace.
Cost: 750 credits

Escape Hatch

Description: If you block ads on your browser, then websites can ask you to pay for content instead. With Escape Hatch, you can temporarily allow ads to be shown, but in a way that protects your safety and privacy.
Cost: 150 credits

II. Participants

The 15 participants that were recruited were divided into 3 groups of 4 and 1 group of 3. Ages of the participants ranged between 21-69 years and the gender split was 7 males:8 females. The participants were chosen to provide a broad range of income levels and Internet usage.

RESULTS

I. Selected Features

The features selected by each group were quite uniform, with all 4 groups selecting the following 4 features: **Tracking-Blocker**, **Speed Booster**, **Firefox “Flow”** and **Malvertising Protection**. TABLE 1 shows which features each group selected in the order that they were selected.

TABLE 1. FEATURE SELECTION BY GROUP

Group 1	Group 2	Group 3	Group 4
Malvertising Protection	Tracking-Blocker	Firefox “Flow”	Malvertising Protection

Ad-Blocker	Speed Booster	Speed Booster	Firefox “Flow”
Tracking-Blocker	Firefox “Flow”	Escape Hatch	Speed Booster
Speed Booster	Escape Hatch	Tracking-Blocker	Tracking-Blocker
Firefox “Flow”	Malvertising Protection	Malvertising Protection	

II. Perceived Benefits of Behavioral Advertising

Firstly, it is noticeable that only 1 group selected the **Ad-Blocker** feature, which is revealing of the fact that most participants saw the value of being exposed to at least some form of advertising online, although not necessarily behavioral advertising that tracks online behavior.

The main perceived benefit of advertising was that it could help the participants find novel products that either matched their interests or that could be of interest to the participants’ friends and family.

Advertising makes my life easier. My information is out there already, I'd rather advertisers are able to figure out what I like. I'd rather see that than seeing the same car commercial 10 times every morning. – Participant 3

Following earlier studies (McDonald and Cranor), many participants were also quite knowledgeable about the role online advertising has to play in keeping the Internet free and providing revenue to smaller players.

I used to be an ad-blocker, I don't use it anymore because I know it's what keeps the lights on for a lot of people. I used to subscribe to a lot of magazines and would pay them directly. Now there's a thousand times more content and it's all free, so I'm not going to complain about ads. – Participant 11

II. Freedom from Annoyance and Interruption

Despite the majority of the discussion in the groups centering on privacy issues and concerns, it is worth noting that the **Firefox “Flow”** and **Speed Booster** features was picked universally across all groups and, furthermore, these feature are ones that the groups could agree on most easily and with minimum conflict. This indicates that speed, convenience and freedom from annoyance and interruption are the benefits that users value the highest and most commonly. Any ad-blocking strategy that has the aim of protecting users’ privacy should also ensure that these core needs are met.

III. Freedom from Being Followed

Another issue that became clear in the course of the card-sorting exercises and discussion was the deep unpopularity of retargeted ads. Echoing previous studies, the participants in this study displayed diverse attitudes towards behavioral advertising. Some perceived clear benefits and were more prepared to exchange some of their personal data in exchange for these benefits, whereas others preferred not receive any behavioral advertising of any kind.

Nevertheless, all participants could agree that they had at least some negative experiences of retargeted advertising that led to them feeling harassed, annoyed or mischaracterized. For some participants, retargeted ads could feel creepy, invasive, or even bring hurtful reminders of painful past events. For others, they were merely annoying. It was therefore relatively easy for all groups to agree on the value of the **Tracking-Blocker** features, in that it would prevent retargeted ads, but still allow for some other forms of targeted advertising, such as targeting by interest or demographics, that would not be possible with a stronger form of tracking protection, such as that provided by the **Total Privacy** feature, which was not chosen by any group.

Interestingly, however, in discussing of the **Total Privacy** feature, some participants could see some benefits to stronger levels of tracking-protection, but these benefits were actually more associated to receiving more interesting and relevant advertising, rather than in the protection of their privacy per se. If advertisers know nothing about your demographics or your behavior, then they are forced to find other ways to make their ads relevant to the consumer. Participants spoke of how advertising that is *contextual* to the website is generally the most interesting and relevant to them. For example, being shown ads for beauty products while visiting a beauty website, or hearing an advertisement in a podcast that matches the topic of the podcast. The interest in the **Total Privacy** feature is therefore more revealing of a perception about the higher quality of contextual advertising, rather than necessarily a need for privacy.

IV. Protection from Illegitimate and Misleading Advertising

The final feature that was chosen unanimously across groups was the **Malvertising Protection** feature. This result is revealing of the contextual nature of people's privacy norms. As mentioned, the participants in this study displayed a diverse range of attitudes about which of their personal data they were willing to share with advertisers. Nevertheless, the participants commonly shared a desire to protect their data from harmful entities and a need to be able to discern reputable from less reputable advertisers online.

This need for protection applied not just to obviously harmful entities, such as malware, but also to other forms of advertising that may still be legitimate but still misleading, such as clickbait that lures people to pages that are designed just to show them advertising. Several participants asked about whether the Malvertising Protection feature would cover such use cases. When it was explained that it was not, the groups still selected the feature since the threat perceived from malware was so high.

DISCUSSION

I. Safeguarding Against Bad Advertising Practices

The participants in this study did not reveal an aversion to advertising per se. Participants had different attitudes with the respect to how willing they were to share their personal data with advertisers, with some participants wanting to remain completely private and some happy to share some information in certain circumstances. However, the participants could find agreement in protecting themselves against what they commonly perceived as bad advertising practices, which they defined in the following ways:

- Ads that interrupt the user or get in the way of content
- Irrelevant retargeted ads, that are at best annoying, and at worst creepy and invasive
- Malvertising
- Dishonest or misleading advertising

II. Implications for Ad-Blocking Strategies

This research provides support that a binary approach to blocking ads is not optimal for many of Internet users. The majority of participants in this study are not against online advertising per se, and in some cases see tangible benefits in sharing their data with advertisers in return for more personalized ads. It is hypothesized that the majority of Internet users would be better served with a more balanced approach that still allows for the benefits that advertising while protecting users from some of the privacy threats they can bring.

Finding the right balance and flexibility in privacy protecting tools is hard task given the highly contextual, individualized and complex nature of users' data sharing preferences and norms. However, this study has clarified areas of commonality that an ad-blocking strategy should address. This includes ensuring that, at a minimum, annoying ads that interrupt or block the user should be handled as a priority for any ad-blocking strategy. Beyond that, there are opportunities to devise solutions that prevent retargeted ads from harassing users and that protect users from illegitimate and misleading advertising.

Such solutions will depend on the ability to connect users to more reputable and trusted sources.

REFERENCES

To be completed in the updated version of this paper should this submission be accepted.