AdReveal: Improving Transparency and Control in Online Targeted Advertising

Bin Liu*, Anmol Sheth†, Udi Weinsberg†, Jaideep Chandrashekar‡, Ramesh Govindan*  
*University of Southern California, †Technicolor  
binliu@usc.edu, {anmol.sheth, udi.weinsberg, jaideep.chandrashekar}@technicolor.com  
ramesh@usc.edu

ABSTRACT
The multi-billion dollar online advertising ecosystem is driven by the ubiquitous tracking of end users' online activities. Targeted ads are matched to individual user interests mined by online tracking services. Remarkably, an end user today – the presumed beneficiary – has little transparency into this process, cannot reason about how their online behavior is being used, and lacks influence in determining the types of ads delivered to them. In this paper, we address this pressing need for transparency into online ads by developing mechanisms and simple metrics that allow users to understand the extent to which they are targeted, and the level to which different ad categories are focused on selective parts of their interest profiles. We implement these mechanisms as a client-side browser tool, AdReveal, and evaluate these metrics with web browsing data derived from the public search logs of 20 individuals. Our results show that AdReveal can effectively distinguish between different targeting mechanisms employed by advertisers and also provide fine-grained transparency into the ad targeting mechanisms. Finally, using the building blocks in AdReveal, we propose a practical and novel browser based control mechanism that lets users opt-out of specific ad categories and prevent these ads from being displayed to the user.

1. INTRODUCTION
In recent years, there has been a concerted push in online advertising to improve the relevance of ads shown to users by profiling users’ online interests and delivering ads relevant to those interests. A large amount of companies — over 800 such trackers [3] — build profiles of users as they browse the web using different tracking methods, e.g. web & flash cookies, browser fingerprinting, and beacons. This widespread tracking of users, and the subsequent personalization of ads has recently been actively debated and received a great deal of negative press. The lack of sufficient transparency into the advertising ecosystem today is reflected in prevailing social attitudes about the practice of personalizing ads: people associate adjectives such as creepy and scary with the practice [24], primarily because they lack insight into how their data is being collected and used, and being unable to exercise any sort of oversight or control into these processes.

We examine two aspects of the targeted advertising ecosystem that has largely been overlooked so far: transparency (“Why am I receiving ads of this type?”) and control (“I do not want to receive ads of this type”). Consider a user that repeatedly receives ads about cures for a particularly private ailment. The user currently lacks a way to reason about why she is receiving such ads. Is it because the advertisers believe that the user is suffering from the disease? Is it because the sites visited by the user attracts a large number of suffering visitors? Or is it because the user actually tried to buy the particular medication online previously? Upon receiving the ads in question, the user also lacks sufficient control mechanisms to ask not to be tracked along the actions that relate to these ads, or to indicate not wanting to receive such ads.

In this paper we seek to enable a solution that provides end-users simple and intuitive understanding on how their online activity is profiled, and how the ads a user receives are targeted based on these profiles. This understanding should in turn assist users in exercising their choice of ads that they wish to (or not) receive. The proposed solution needs to inter-operate with the existing ad ecosystem and satisfy the following two key requirements. First, our solution should not require the user to simply block all tracking and profiling of users’ online interests. We recognize that blocking (or substantially limiting) tracking and advertising undermine the underlying economy that supports “free” online services that end-users enjoy today, and consequently require refactoring large portions of the ad ecosystem. Second, our solution should not require any explicit coordination with external entities in the ad ecosystem and should only leverage observations made by the end-user. The key challenge involved in meeting the above requirements is that the existing ecosystem is complex, and the decisions of how and which ads get targeted at users are made by several stakeholders in the ecosystem and are completely opaque to end-users.

Existing solutions that seek to address some of the above requirements of transparency and control fall short in several ways. Privacy preserving targeted advertising solutions like Privad [16], Adnostic [23] and RePriv [14] refactor the existing ad ecosystem to allow users to protect their data better, thus are not really deployable. Policy proposals like Do Not Track [12] provide a regulatory framework over the tracking and profiling of user data. However, in the present form, there is no legal mandate for the ad-networks to comply with this directive and this might require government intervention to enforce universally. Finally, industry driven efforts such as AdChoices [7] enables the user some control over certain “categories” across a few participating online trackers and ad networks. However, even with the small number of participating entities, the mechanisms are not evenly implemented and thus hard to use [17]. Most importantly, this effort is driven by the same industry that has a contradicting interest in collecting as much data as possi-
ble. Various browser tools, such as Ghostery [3], AdBlock [1] and NoScript [19], also address some of these issues, however they provide a very coarse-grained control, by either turning off or on all ads and tracking.

To address the limitations of the existing solutions, we present AdReveal, a browser based tool that tracks visited pages and the ads being targeted at the user on these pages to build local profiles of the users’ online interests and received ads. Based on the distribution of the interest profile (semantic categories of the visited webpages) and the ad category profile (semantic categories of the landing pages of the served ads), AdReveal provides novel techniques to quantify the extent to which the ads profile maps onto the user’s online interest profile. This information is presented to the user in the form of metrics that are simple and intuitive for the end-user. The primary contributions we make in this paper are as follows:

- We define practical and simple metrics that rely on observations made at the end-user that summarize the extent to which the user’s profile is used for targeting, how certain ad categories make extensive use of the user’s online interests, and the specific online interests that are used for targeting specific ad categories.
- We implemented these metrics into a functional tool, AdReveal, and use it to measure and characterize targeted display ads (flash and image ads) embedded in webpages. As far as we know, AdReveal is the first practical tool that enables the measurement and analysis of display ads on the web.
- We characterize the metrics we propose using AdReveal across real user web traces as approximated by the publicly available AOL search logs. We report on broad characterizations as well as a detailed study of representative users in our dataset, to validate that the metrics defined do indeed capture the extent of targeting and provide the required transparency.
- Finally, based on the building blocks provided by AdReveal, we propose a practical and novel browser-based control mechanism that lets users opt-out of specific, fine-grained ad categories.

The rest of this paper is structured as follows. Section 2 provides a quick overview of the online ad targeting ecosystem. In Section 3 we define the transparency metrics we propose. In Section 4 we present the design and implementation of AdReveal followed by an evaluation of the proposed transparency metrics in Section 5. In Section 6 we propose novel techniques to provide end-users control over targeted ads, present related work in Section 7 and conclude in Section 8.

2. BACKGROUND

In this section, we briefly sketch the online ad ecosystem and describe the different kinds of ads that are displayed to users, and how these ads are targeted. We provide this background based on case studies of setting up online advertising campaigns for Google, Yahoo, and AOL. We begin by listing the key stakeholders in the ad targeting ecosystem.

Publishers are the owners of websites where ads are actually displayed and seen by end-users (e.g., www.cnn.com). Advertisers wish to place ads about their products and services on the publisher web pages (e.g., the auto company www.honda.com). Rather than contracting with each other directly, they both contract with one or more ad-networks to act as intermediary aggregators (of ad space and of interested bidders). The actual buying and selling of ads is conducted via auctions and enabled by ad-exchanges. As the client loads the publisher’s webpage in her browser, a call is made to the ad-exchange to fetch an ad along with the user’s cookie and URL information. The ad is selected from a real-time auction, whose outcome depends on the interests of the user visiting the webpage, the quality metrics of the ad-space, and various parameters setup by the advertised like the bid cost, cost per mille impressions (CPM) and desired click through rates (CTR).

Given how complex this ecosystem is, and the various parties involved, and the various metrics tracked by different parties, several ad campaign management platforms (also called ad targeting platforms) have emerged, which essentially horizontally integrate multiple pieces of the ecosystem (e.g., Google AdSense, www.google.com/adsense). These platforms enable advertisers to define and set up ad campaigns by simply describing the user demographic they wish to target, along with web page categories in which they would like their ads to appear. These “filters” are set up by selecting one or more categories from a pre-defined taxonomy (platform specific). Users’ interest are inferred and mapped to the same taxonomy based on analyzing the history of web pages visited by a user; this is achieved by the different publishers installing tracking code that contain the ad networks tracking cookies that enables the ad network to track and profile users as they browse the web. Based on this tracked history, users are mapped onto a set of categories which is the user’s online interest profile that consists of a list of interest categories represented by a tree-like hierarchy structure (e.g., Movies → Action and Adventure Films → Superhero films).

Figure 1 shows the number of categories and the distribution of their depth in the tree for the four trackers that publicly disclose their taxonomies. We observe that Google’s profiling catalog is the largest with 20% of the catalog entries having a depth of up to seven levels. This very narrow (and detailed) dissection of a users online behavior is what allows advertisers to very precisely target end-users and occasionally with great success.

Based on the high level description given by advertisers, existing ad targeting platforms use a number of mechanisms to actually place ads onto web pages that are visited by users. Ads served to the user are either contextual, retargeted or behavioral, and these vary in the level of user information used in the selection of the ad. We now briefly describe all three targeting techniques.

Contextual Targeting Ads are selected to match the subject or theme of the page in which they are embedded (it ignores the profile of the visitor). The targeting is implicit, based on prior knowledge of the typical user to the website: a company selling auto insurance would insert ads on well known auto related sites because the typical visitor to that site is likely to be interested in such products (even without consulting the profiles built for the user). Other factors that could also influence placing contextual ads are location, time of day. With contextual targeting, the expectation is that users with different profiles visiting a site would receive similar kinds of ads, and these tend to match the topic of the website (or something quite related).

Retargeting is used by advertisers to focus on users who
have shown explicit interest in a product (perhaps by visiting the product website) in an effort to make the user actually finish the transaction (of buying the product). For example, consider a user who is shopping for auto insurance and visits an auto insurance website to get a quote and leaves the website without completing the transaction. The auto insurance company uses retargeting to display insurance ads (with potential discounts) in other websites that the user goes to afterward, so as to entice the user to come back and complete the transaction. Here, user information is used, but in a very narrow sense. The advertiser only cares about the user’s interest in a very specific action (or intent) and the ads focus on that. Moreover, retargeting is limited to a single site domain and typically based on more recent web history of the user.

Behavioral Targeting involves displaying an ad to a website visitor that matches their constructed online interest profile, based on a longer history of sites they have visited. This goes beyond the “single domain” aspect of retargeting and is meant to target some set of user interests (vs. particular sites visited). With behavioral targeting, a user might get ads for auto insurance, on websites unrelated to cars or auto insurance, because their profile has an interest category of “auto insurance” generated by having visited a number of (different) sites about auto insurance. This particular form of targeting is perhaps the most controversial, given that it relies on detailed analysis of the user’s online interests, and the targeting occurs on webpages that are potentially unrelated to the product.

3. ENABLING TRANSPARENCY IN AD TARGETING

Transparency, ideally, implies being able to precisely state why a specific ad is being displayed to an end-user. This is quite straightforward for re-targeted ads but not at all for the other two categories. The ad-networks and the ad selection algorithms are enabled by ad auctions that can be impacted by many factors, and not all of these are “visible” from the end-user’s perspective. For these reasons, it is impossible in the current ecosystem, close to the user, to reason about individual ads being behavioral or contextual. Thus from the perspective of the client, we can only reliably differentiate between re-targeted ads and interest based ads, which cover both contextually and behaviorally targeted ads.

We believe that with interest based ads, even if individual ads cannot be attributed accurately, it is still possible to observe patterns at an aggregate level. We define a metric, targeting score, that captures the extent to which users are being targeted based on their interests. In other words, given a set of ads being delivered to a user, we can compute a score that can tell us if the ads are largely contextual, based on the web pages currently being visited, or if they are very behavioral, based on the websites visited in the past (and less related to the current web pages). In the first case, the score should be low and it is unlikely that a user would see ads that relate to previous behavior. In the second, with a higher targeting score, there is an increased likelihood of an ad being displayed that relates to sites that the user visited in the past. Importantly, this score is computed locally, at the user, and does not require any cooperation from external entities in the ad ecosystem.

In the rest of this section, we describe how to identify ads as being retargeted or interest based and then describe a novel way of computing the targeting score metric. In the next section, we describe how this metric was implemented in the browser.

3.1 Identifying Re-targeted Ads

A re-targeting ad campaign requires the advertiser to tag different pages in her website with specific Javascript code generated by the ad-exchange. The different tags enable the advertiser to target users that performed specific actions on the website, and create different advertising strategies based on these sequential actions, e.g., homepage visit compared to adding items to the cart and not checking out. Hence, re-targeted ads ignore the user profile and “follow” the user on the web, re-targeting the product to convince the user to come back to the advertiser’s webpage.

Re-targeted ads and campaigns can be detected in a straightforward manner by simply monitoring and logging all domains visited by the user, that host webpages containing re-targeting tags in the page source. Subsequently, when an ad is displayed to a user, we can match the domain that the ad points to (the site that would have been visited if the ad was clicked) against the set of identified re-targeted domains. Thus, if we track all the pages visited by the user, we are certain to detect the original re-targeting tags, which enables us to match the corresponding ads domain. When AdReveal identifies a re-targeted ad, it shows the user the exact actions in her clickstream, enabling users to reason about how their interaction with the website impacts the ads they receive from them.

3.2 Interest based Ads

For a contextual ad campaign, we expect that individual users’ profiles are largely ignored and the ads will bear some relation to the theme and content of the web pages. On the other hand, for behavioral ad-campaigns, we expect that the ad-networks will focus more on the specific online interests of users. At a high level, this results in a key distinction in the distribution of webpages and ad categories that will be observed: behavioral ads will span a wide distribution of page categories (since the ads follow the user interests, and not the pages); and contextual ads will be limited to a few page categories that are the same or related to the pages being visited.

With this intuition, we then define a framework that will help a user reason about the following specific questions:

1. To what extent are ads being targeted to the user based on their particular interest profile? We define an aggregate targeting score that allows users to understand how much of their personal information is being used to select the interest based ads that are being displayed to them. The score is high when this is the case, and low when a large fraction of the ads are contextual.

2. Do some ad categories target the user’s interest profile...
more than others? This allows users to understand if particular ad categories (and the particular products being advertised) are exploiting very specific information about the interest profile.

3. What specific interests from the user’s profile are being used to select ads? This informs the user if any (potentially) sensitive, private parts of their web browsing behavior are being used to select ads for them.

In the rest of the section, we describe exactly how to compute the targeting score and other metrics that will empower users by giving them a way to answer the questions posed above.

Starting from scratch, with each page visited by the end-user, and the set of ads that are displayed in the pages, we maintain and update the following distributions and counts. We first define some notation that will be used through this section; the notation represents the view of a single user.

Let $C = \{c_1, c_2, \ldots, c_n\}$ be a set of page and ad categories and let $S = s_1, s_2, \ldots, s_m$ be the sequence of webpages visited by the user (in order). Each $s_i$ is associated with a category $c_j$. In addition, each page $s_i$ has a number of embedded ads, each of which is also associated with a category from $C$. We now define a number of distributions as follows:

- **User Interests Profile** $PU = (pu_1, pu_2, \ldots, pu_n)$: A probability distribution across the categories of pages visited by the user. This is extracted from the user clickstream and updated with each page that is visited. Thus, $pu_i$ is simply the fraction of the user’s pages that are from category $c_i$.

- **Ads Profile** $PA = (pa_1, pa_2, \ldots, pa_n)$: A probability distribution, across the various categories, of all ads delivered to the user so far. Thus, $pa_i$ is the fraction of ads displayed to the user that are from category $c_i$.

- **Pure Random Ads Profile** ($PR$): A synthetic probability distribution where ads are sampled across the categories that exist in the user profile. To construct this, for each page visited by the user, let $k$ denote the number of ads contained in the page, we pick $k$ categories uniformly from all the categories $c_i$ where $pu_i > 0$. This captures the behavior of the ad-network when it is using no information about the page itself to display the ad and using only information about the categories that the user has shown interest in.

- **Pure Contextual Ads Profile** ($PC$): A synthetic frequency distribution where all ads on a page are extracted from the category of the page itself. To generate this, for each page visited by the user, we assign all $k$ ads contained in the page to the category $c_i$ (which corresponds to the category for the visited page). Then $PC$ is the resulting aggregate distribution across the set of categories. This distribution captures the ad-networks behavior if it were behaving in a completely contextual manner – ignoring the interest profiles of the user and simply delivering ads targeting the content of the page.

- **Category relation Matrix** ($M = [m_{i,j}]$): a matrix where the rows correspond to visited page categories, and the columns to ad categories. Each entry $m_{i,j}$ counts the number of ads of category $j$ that were displayed on pages of category $i$.

For each of the distributions defined above, we also define a windowed versions $PU[k,l], PA[k,l], PR[k,l], PC[k,l], M[k,l]$, which are constructed only on the subsequence $s_k, \ldots, s_l$, i.e., by only considering the pages visited between $s_k$ and $s_l$ (inclusive).

Based on these computed distributions, we can extract a number of different properties of the underlying process that is selecting the ads being displayed to the user and in the following, we define some specific metrics that help us answer the questions posed previously.

3.2.1 Computing the Targeting Score

The targeting score captures at some aggregate level whether the ads being displayed to the user, over some period of time, are contextual or behavioral. If the ad-network was using a purely contextual strategy, then we expect the distribution of $PA$ to roughly have the same shape as $PC$. On the other hand, if the ad-network is targeting the user specifically and delivering ads based on their interest profiles, then $PA$ would resemble $PR$. Entropy naturally captures the notion of the spread of a distribution, and we derive a targeting score by comparing the entropies of the various distributions being tracked. The entropy of a probability distribution, $E[P]$ is defined as $E[P] = \sum_i -p_i \log p_i$. Based on the intuition described earlier, we expect $E[PR]$ to be an upper bound for the entropy of served ads (even larger than with a strategy that was completely behavioral). As the entropy of the served ads $E[PA]$ moves farther away from $E[PC]$ (and closer to $E[PR]$), it is more likely that the ads are targeting the user’s interest profile i.e., the ad network is targeting behaviorally. Thus, we define the targeting score as the normalized distance between $E[PA]$ and $E[PC]$:

$$\text{score} = \begin{cases} \frac{E[PA] - E[PC]}{E[PC] - E[PA]} & \text{if } E[PA] \geq E[PC] \\ \frac{E[PC] - E[PA]}{E[PC]} & \text{otherwise} \end{cases}$$

A low score indicates that the ads received are mainly contextual and a high score indicates that the ads received are not related to the category of the webpage and are likely to be more behavioral.

Note that we can compute $E[PR]$ and $E[PA]$ on overlapping windows of different sizes (which would incorporate some history into the profile before we start considering the ads being delivered).

3.2.2 Ranking Ad Categories

In order to examine particular ad categories and order them based on the level of interest targeting, we can compute the entropy across the columns of $M_{i,j}$. Recall that columns represent ad categories and rows represent page categories. Thus, each column captures the spread in ads of that particular category across all the page categories. A high entropy here, for an ad category, implies that the targeting is broad and spans several page categories evenly and are likely to be targeting the user’s interest profile. If this were not the case, ads would tend to associate with a few specific page categories (e.g., ads about shoes showing up on pages about fashion, clothing, or shopping), and this would result in the entropy being much smaller.

Thus, to enable users to understand what ad-categories are specifically targeting their interests, and to what extent, we generate the entropy across the columns in $M_{i,j}$ and rank the corresponding $C = \{c_1\}$ in decreasing order.

3.2.3 Identifying Unevenly Targeted Interests

We would also like to help the user identify which of their particular interest categories are being targeted by the ad-networks. In other words, for a particular ad-category, how are the ads embedded across pages of different categories.
This can uncover cases where the ad-networks, based on some analytic correlations carried out offline, target users on related categories. For instance, ads for beer are likely to be shown on pages about sports and baseball. Understanding this gives users a way to control the selection of ads delivered to them. To use a concrete example, consider a user that starts to see ads for baby-strollers when browsing pages on seemingly unrelated categories, and that the shopping ads-category has relatively high entropy (see previous discussion). The user can then understand what page categories are being linked to their interest in shopping – perhaps healthcare, shopping (expected), and life-planning.

This particular information is directly quantified in the matrix $M_{i,j}$, the rows that have a high count for the particular ad-category are the ones likely to be linked together (assuming that the entropy is low for that ad-category). This particular facet is hard to quantify precisely, but can be qualitatively argued and we discuss several anecdotal examples in the following section.

In the next section, we describe exactly how to build mechanisms inside the browser that can expose these metrics and characterizations to the user and allow them to understand and control the flow of ads being delivered to them.

4. AD DETECTION & CLASSIFICATION

In this section, we describe the design and implementation of AdReveal, a browser extension that monitors and collects information about the ads being served to end-users and computes the targeting score as described previously. We chose to implement AdReveal as a browser extension, and not as a http proxy implementation, since a lot of the page elements that are loaded on the webpage are downloaded by dynamic Javascript that executes inside the browser. We note that the main difference between AdReveal and existing ad monitoring and blocking browser extensions, such as AdBlock [1] and Ghostery [3] is the ability of AdReveal to extract detailed information about the ads and user profile and monitor the evolution of these profiles over time.

For every webpage that is browsed by the user, AdReveal extracts and stores the following information in a local database: (i) the different ad network trackers that are present on the webpage, (ii) the url of the page along with a category for the page, (iii) for each ad embedded in the page, the destination landing page of the ad and the category of the destination landing page. The category descriptors of the webpage and ad URLs are provided from the same taxonomy of categories.

Figure 2 provides an overview of the main modules of AdReveal. We describe each of the modules and highlight the key challenge we address in the implementation – enable measurements for image and flash ads through a browser extension that works within the security sandbox model of the browser and across complex DOM structures of webpages.

4.1 DOM Parser and Preprocessor

This module is responsible for several key functions: (i) pre-processes the webpage to create a list of potential HTML elements that contain ads, (ii) logs any ad network trackers it finds, (iii) logs the webpage URL along with its category and (iv) overlays visual elements on the webpage to provide users with the processing results and targeting score.

The list of ad elements in the page is created by iterating through every HTML element of the DOM tree and comparing it against a list of predefined ad patterns. We use the open source URL pattern database distributed by Ghostery [3] to detect both interest-based and re-targeted ad URL patterns. For image based ads contained within the <img> element, the module inspects <href attribute for the URL patterns of the ad network. For flash ads that are contained either within the <object> or the <embed> element, the module inspects the <flashvars> attribute for the URL patterns.

The module logs the trackers that are present in the page by intercepts all HTTP requests that contain a user cookie to a predefined list of online trackers. Furthermore, it logs the existence of re-targeting scripts by comparing against a predefined re-targeting pattern file.

Finally, the module can block, highlight, and provide additional context to the ads on the page. This enables AdReveal to provide the user with visual notification on the extent of tracking as discussed in Section 3.

4.2 Ad Landing Page Extractor

This module infers the landing page of an ad, i.e., the page that the browser is directed to if a user clicks on the ad. The trivial solution of extracting the landing page by emulating a user clicking on the ad is not feasible, because doing so would be considered a click-fraud and it could also potentially perturb the user’s interest profile maintained by the ad network. Thus, this module infers the landing page of the ad from the value of the attributes discussed above.

In our experiments, we found that more than 80% of the ads have a landing page that is encoded in these attributes, while the remaining ads require actively following HTTP redirects, thus we cannot extract the landing page.

To complicate things further, image and flash-based ads are often embedded in nested iframe tags that span multiple levels. In these cases, the same origin policy enforced by modern web browsers only permits an outer iframe to inspect its immediate inner iframe and not vice-versa. This means that the module cannot directly parse the landing page of ads nested deep within iframes.

To address this challenge, AdReveal use the ability of browser extensions to inject JavaScript code into iFrames. Once the code is injected into the iFrame that contains the ad, it can then communicate with a special background page, and send the extracted landing page URL to it. This way the module can obtain all ads’ landing pages, regardless of the nesting level then reside in.

4.3 URL Category Extractor

In order to extract semantic information, this module classifies the categories of all the URLs that AdReveal processes, namely the pages browsed by the user, and the landing pages of the ads. A previous approach used by Privad [10], is to build a local text classification engine that parses the content.
tents and meta data of the page, and carries out a textual analysis of the page to classify it. While this approach is feasible for pages that the user browses, in order to apply it for landing pages of the ads, AdReveal needs to actually download the landing page, thus encountering the same issues as discussed above.

Instead, we make use of the Yahoo content analysis APIs [25] to provide the semantic categories associated with a webpage. The API receives a URL as the request parameter and returns a list of potential categories along with a confidence score. Out of this categories, AdReveal picks the category with the highest confidence, and stores it in the local database. We note that there are other similar tools [2,5,6], however, we found Yahoo’s API to be the most detailed and accurate.

### 4.4 Implementation Details

We implemented AdReveal as a Chrome browser extension. The design of AdReveal is generic enough that it can be easily ported to other browsers. One important detail is that AdReveal needs to detect display ads, the corresponding landing pages and re-targeting scripts. While some ad-blocking tools, like Adblock [1], publish open databases of regular expressions that match HTTP requests to ad-networks and exchanges, none of these allows for the landing page of the ad to be detected. In addition, they do not contain re-targeting patterns, and thus we have to manually identify these. In the current implementation, we only cover Google’s DoubleClick ad network, which has the largest market share (15.4%) of display ads [4]. The re-targeting JavaScript for the DoubleClick ad-exchange has a unique, easily identifiable pattern, which is easily searchable across the elements of the page. We find this URL pattern by setting up a re-targeting ad campaign through Google AdSense. As future work, we plan on extending AdReveal to other ad networks and ad exchanges by identifying the requisite patterns and incorporating them into AdReveal.

### 5. EVALUATION

In this section we evaluate the ability of AdReveal to provide the transparency mechanisms we propose in Section 3. We begin by describing the dataset we use to evaluate the transparency mechanisms for interest-based ads and re-targeted ads. Along with providing a detailed analysis for specific users in our dataset, we also provide a broader aggregate analysis for the two targeting mechanisms across all the users in our dataset.

#### 5.1 Dataset

We use browsing traces derived from real users’ search queries: the public AOL dataset [20] consists of user searches of about 650k users. From this, we select 20 users at random and generate a URL trace as follows. We install AdReveal into a chrome browser instance (independently for each user) and use Selenium [22] (a browser automation framework). We then visit the top 5 returned results in order one at a time with a delay of 2 minutes in between. This behavior loosely captures the behavior of a user trying to locate information about the search topics. Concurrently, AdReveal characterizes all the pages visited and the ads that are received (we are currently limited to those sent by DoubleClick).

Table 1 provides a summary of the dataset generated by AdReveal for the 20 users. On average, a user’s trace took 1.5 days, contained roughly 1133 web pages and AdReveal identified 861 DoubleClick ads within these pages. A page has an average of 0.76 DoubleClick ads, and about 40% of the pages contain at least one DoubleClick ad.

<table>
<thead>
<tr>
<th></th>
<th>Min</th>
<th>Max</th>
<th>Med.</th>
<th>Avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hours to complete the crawl</td>
<td>25.60</td>
<td>66.53</td>
<td>31.33</td>
<td>37.75</td>
</tr>
<tr>
<td>Number of pages</td>
<td>768</td>
<td>1996</td>
<td>940</td>
<td>1334.50</td>
</tr>
<tr>
<td>Number of ads</td>
<td>383</td>
<td>1619</td>
<td>789</td>
<td>861.55</td>
</tr>
<tr>
<td>Number of ads per page</td>
<td>0</td>
<td>9</td>
<td>0</td>
<td>0.7601</td>
</tr>
<tr>
<td>Number of page categories per user</td>
<td>61</td>
<td>87</td>
<td>77.50</td>
<td>76</td>
</tr>
<tr>
<td>Number of ad categories per user</td>
<td>35</td>
<td>63</td>
<td>44</td>
<td>45.35</td>
</tr>
</tbody>
</table>

Table 1: Summary of the AOL dataset used in evaluation

**Figure 3:** Distribution of number of consecutive webpages that the user is not tracked by DoubleClick cookies and re-targeting scripts.

**Figure 4:** Percentage of browsed pages and served ads contained in the top-k categories

<table>
<thead>
<tr>
<th></th>
<th>Top-k categories</th>
<th>% of coverage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Subsequently, each search term for the user is submitted to Bing.com (this is the only search engine that does not rate limit queries). We then visit the top 5 returned results in order one at a time with a delay of 2 minutes in between. This behavior loosely captures the behavior of a user trying to locate information about the search topics. Concurrently, AdReveal characterizes all the pages visited and the ads that are received (we are currently limited to those sent by DoubleClick).

**Figure 3** plots the cumulative distribution of the run-length of these consecutive browsing traces. The figure shows that tracking by DoubleClick is almost ubiquitous where for 80% of consecutive browsing traces, users cannot browse more than 2 consecutive pages without being tracked by DoubleClick. Re-targeting scripts are less common, but still quite prevalent – less than 20% of the consecutive sequences have a length of more than 20; the median for re-targeting is approximately 9 consecutive pages.

**Diversity of Ad and Browsing Profiles.** We now quantify the diversity in the ad and browsing profiles of the users in our dataset. Figure 4a shows the percentage of the user’s total number of browsed pages that are contained within the top-k categories. Figure 4b shows the same metric for
the total number of ads delivered to the users. Each box span the 25-75 percentile, the line shows the median and the whiskers extend to 1.5 times the box height.

Figure 4a shows that the top-10 categories include roughly half of the browsed pages. However, the tail of the distribution is long, and only 83% of the pages are included in the top-30 categories. Unlike the browsing profile, Figure 4b shows that the ad category profile across all the users spans much fewer categories. The top-10 ad categories contain almost 80% of the ads served to the users. This difference is also evident from Table 1, showing that the average number of categories per user is 76 while the average number of ad categories served to users is 45.

To summarize, we observe that users have a rich and diverse browsing profile, with some categories being more dominant than others. The ads served to users span much fewer categories. This indicates that ads are not directly related to the categories of the pages that user’s browse and indeed target a smaller portion of the user’s online interests.

5.2 Interest Based Ads

In this section we evaluate the effectiveness of the metrics proposed to provide users greater visibility into interest based ads. We provide a characterization of two example users from our dataset followed by a summary of observations across all users.

Distribution of the targeting score. Across all users we observed the lowest score to be 0.04 and the highest score to be 0.72 with a median of 0.3. This relatively low median indicates that the ads received by users were more contextual than behavioral. We attribute this to the relatively short time duration of our experiments. We expect the metric to provide higher scores over a longer time interval as the user profile evolves and is used for targeting. We now pick two example users from our dataset and provide a detailed analysis of their transparency metrics.

5.2.1 Quantifying User Interest Profile Usage

As defined in Section 3, the targeting score of a user quantifies the extent to which the individual user’s online interest profile is being used to target interest based ads. We expect to observe a low targeting score for users who primarily receive contextually targeted ads and a high targeting score for user who primarily receive behaviorally targeted ads.

Figure 5 shows, for two example users, the entropy for accumulated number of browsed pages, of the served-ads categories \( E[PA] \), the user profile categories \( E[PU] \) and the upper bound \( E[PR] \) and lower bound \( E[PC] \). Figure 5a provides an example of a user whose profile is being excessively used in to serve targeted ads, which resulted in the highest targeting score (0.72) at the end of the crawl in our dataset. On the other hand, Figure 5b shows an example for a user whose served ads are very close to the lower bound, indicating that most of the ads received by the user were contextually targeted, with a final targeting score of 0.23. We note that the initial increase observed in both plots is due to the time it takes the distributions to gain sufficient number of categories. As expected we observe that the \( E[PA] \) for both users is bound by \( E[PC] \) and \( E[PR] \). This trend was validated at almost all the users in our dataset.

5.2.2 Extent of Targeting Across Ad Categories

Computing the entropy of the interest based ads for each

category enables the end-user gain visibility into whether certain ad categories target the user’s profile more than the others. This ranking of the ad categories also highlights the ad categories that potentially could be using sensitive parts of the user’s online profile.

Figure 5 shows the ranking of the per-category entropy for the two users. We observe that even though the media ad category has the highest entropy for both users, the rest of the categories are ranked differently. Additionally, the targeting of media related ads for both users is very different. For the user with the high targeting score, the media ads were targeted across webpage categories that spanned the user’s online categories that were related to television and music, but also spanned completely unrelated categories like jewelry and watches, ethnic groups, and furniture. On the other hand, the media related ads for the user with the low targeting score was mainly limited to the television category of the user’s online interests.

5.2.3 Trends Across Ad Categories

The discussion in the previous section shows that users may end up being targeted differently even for ads from the same category. In this section we seek to understand whether advertisers of certain ad categories consistently make use of either contextual or behavioral targeting across all the users in our dataset.

To this end, for each user and each ad category we count the number of ads that appear in each profile category, and compute the entropy of the resulting vector (column vector in the matrix \( M \)). An overall low entropy distribution would imply a dominantly contextual targeted ad category and a high entropy distribution would imply a behaviorally targeted ad category.

Figure 6 shows the CDF of the entropy of a few selected ad categories across all users in the dataset. We observe that across the six categories, media has the highest entropy distribution and finance is the lowest. All the other four categories span a wide spectrum of the entropy scores indicating that ads from these categories contain a mix of contextually and behaviorally targeted users.

5.3 Re-targeted Ads

In this section we evaluate the transparency AdReveal provides for re-targeted ads. We focus the evaluation across the aggregate set of all users since the detection of re-targeted ads is straightforward and ads that a user receives are directly dependent on the websites she visited that contain
The categories of Travel dataset, we crawled the top 100 websites from Alexa across USA. The proximity of our experiments to the presidential elections in the top-15 categories, which is most likely related to the presence of re-targeting ads, the first focuses mostly on online businesses. We also observe that re-targeting spans multiple categories, containing pages for renting apartments not selling, thus the potential revenue is not as high. We found re-targeting is quite prevalent and was detected in 31% of the Travel websites, 28% of the Shopping related websites and 13% on websites related to Health.

Distribution across user profile categories. We quantify the extent of which re-targeting campaigns span the user’s interest profile. Figure 8a shows that 60% of the ads of re-targeted websites appear in more than 2 page categories, and 20% appear in more than 6. However, for 10% of the websites users receive ads across a large number (greater than 12) users interest categories. Need a statement to state the implications of this result.

Targeting users immediately. Finally, we quantify how quickly do users get re-targeted ads from a website after having visited it. Figure 8b shows the distribution of the number of pages users browse between the first time they encounter a website that supports re-targeting and the first number of websites that contained a re-targeting script. We found that re-target is quite prevalent and was detected in 31% of the Travel websites, 28% of the Shopping related websites and 13% on websites related to Health.
re-targeted ad the user receives from the same domain. The figure shows that re-targeting campaigns are quite aggressive in targeting the user. For half of the re-targeting ad campaigns, users receive re-targeted ads within 25 webpages and 80% of the campaigns target the user after less than 300 pages.

We also observe a long tail in the above distribution where 10% of the re-targeting ads are displayed after more than 700 pages. This is most likely the result of the frequency with which we crawl webpages. Specifically, when creating a re-targeting campaign, the advertiser can specify the time duration to re-target the user after the user has visited the page. Since our dataset visits a page every two minutes, a single day includes roughly 720 pages. Thus, if the advertiser specified to re-target the user only after a day, then we can expect to have more than 720 pages.

6. ENABLING USER CONTROL OVER AD TARGETING

In this section, we briefly review existing mechanisms available to end-users to control or counter the display of targeted ads, and then describe a novel browser based mechanism, enabled by the capabilities described in AdReveal, to allow users a degree of control over the categories of ads that are being displayed to them.

Existing tools to control targeted ads either block all ads from being rendered on the webpage or techniques that completely suppress the tracking by ad networks. Ad blockers [1] and script blockers [19] prevent the ad from being displayed and block the execution of Javascript code downloaded from the ad network domains. Alternately, mechanisms to control the extent of tracking via third party cookies, like Ghostery [3] and Do Not Track [12], block the flow of tracker cookies to third party trackers or notify the ad network about the users preference to be not tracked and profiled. These techniques have two key limitations. First, they provide only binary control and do not accommodate users that wish to (or not) receive ads of certain categories. Second, they significantly undermine the economics of the online ad ecosystem that in turn supports the “free” services that users use.

None of the existing tools allows the users to be selective about the types of ads, or more generally, the ad categories that she is being targeted with. In this section, we build upon the ideas described previously and discuss (i) a novel mechanism, category delisting by selective replay, which allows users to indicate what they want to receive ads on a specific category, and (ii) enforce control by preventing ads of the selected categories from being displayed in the browser.

Category delisting by selective replay: End-users today have very little control over the profiles that are created about them by the ad networks (only 3 out of the 800 or so allow users to modify their profiles.). These profiles are stored remotely (in the ad-network) and the cookie, which is an index into the profile database, is stored locally in the local browser. Thus, simply deleting the cookie is overly drastic; this will completely purge the user profile from the ad-network and all information about the user is lost. Instead our proposed mechanism deletes the cookie, creates a new cookie (this maps to a redacted profile in the ad-network), and re-associates the cookie with the browser.

The category delisting by selective replay leverages two key capabilities of AdReveal: First, it assists the user to reason about certain ad categories that either make extensive use of their online interests or use certain categories that are perhaps sensitive to the user. This helps users make an informed decision about the specific category of ads they would like to block or receive. Second, AdReveal provides the association between the ads to be blocked and the corresponding categories (for interest based ads) or webpages (for re-targeted ads) to be delisted from the user profile.

In addition, these mechanisms are entirely browser based, and do not require cooperation from the ad-networks, or any other changes to the current ecosystem.

Interest based ads: Redacting ad categories from the profile for interest based ads uses the idea of selective replay. Users select a set of ad categories they would like to “opt-out” from, and AdReveal creates a list of webpages that need to be eliminated from the new profile being created. Subsequently, starting from a blank profile, the tool visits every webpage in sequential order, but skips those that need to be blocked. At the end of this process, a set of new cookies is obtained, one for each ad-network and which are used to overwrite the existing cookies in the browser. Thus, after this process is complete, ads for the opted-out categories are less likely to be (behaviorally) targeted at the user; from the point of view of the ad-network, the user does not care for these categories.

Retargeted ads: Blocking a re-targeted ad is much simpler and does not require selective delisting of the user profile categories. The blocking is achieved by simply replaying the user’s clickstream and avoiding the specific website that contained the re-targeting tags and Javascript code. Note that AdReveal also keeps track of every webpage that has re-targeting tags embedded. This ensures that the user does not receive any further re-targeted ads from the website for the new cookie.

Selective Blocking: The category delisting by selective replay mechanism is a best effort approach and does not guarantee that ads from the block categories will never show up on webpages visited by users. This is because there are alternate control paths by which an ad can appear on a page, and these mechanisms only cover the two prominent control paths. Alternately, a user could continue visiting websites that are related to the blocked ad category. To address these scenarios, the selective blocking mechanism carries out two functions. First, to suppress ads from the blocked category, the mechanism uses a similar approach to the landing page extractor module to extract the category of the ad and block the ad elements from being rendered on the webpage. Second, to ensure that the user does not get profiled over categories that need to be blocked (because of certain blocked ad categories), the mechanism blocks all requests to trackers until the URL of the webpage is classified. Only if the category is not blocked do the requests get forwarded to the different online trackers.

7. RELATED WORK

Most of the work related to this paper falls into three distinct categories: (i) studies that examine the effectiveness of behavioral targeting, (ii) efforts in characterizing the current ecosystem, and increasing user perception about how

2If the user chooses to block ad categories that she has not yet received, then we assume that these ads will be contextually targeted and associate the corresponding use profile category to the ad.
data is collected and potentially used by the ad ecosystem, and (iii) new architectures and frameworks for privacy-aware advertising where users receive targeted advertising without revealing all their information to the ad networks. In the following, we briefly describe some of these ideas and draw a contrast to our own work.

A considerable amount of work has been carried out by advertisers in understanding whether behavioral targeting is beneficial and effective. [26] tries to relate behavioral targeting to measured click through rates (CTRs). In [10], the authors explore whether inferred user profiles can be correlated with ad clicks (for particular categories). These ideas are further extended in [13] which proposes a rigorous theoretical framework for distilling targeting effectiveness, and constructs empirical models to explain ad clicking variations due to targeting. The general take-away from the work in this area is that behaviorally targeting users has a positive impact on advertising revenue. In [15], the authors measure behavioral targeting from the perspective of the end-user and take a first step in understanding how user behavior (web browsing) can influence the ads being displayed. Our work goes beyond this study and tries to reason about why particular ads are displayed and helps users control their experience. Further, only textual ads were considered in [15] while our tool is capable of processing image and flash ads, which form an increasingly large fraction of the ads seen today.

The second broad category of research in the area is around understanding and improving user perception of the processes that underlie the ad-ecosystem, specifically the practice of behavioral targeting. A detailed survey of the various methods used to track users can be found in [21] which also catalogs the prominent tracking agencies by crawling a very large number of popular websites. Other user studies tried to evaluate social acceptance of behavioral targeting [11, 18, 24]. As reported in these studies, users associate behavioral tracking with adjectives such as creepy or scary, and this mistrust stems from a severe lack of knowledge about exactly how, why and where data is collected and used. All these efforts have contributed significantly to raise awareness in the general population and bring privacy concerns to the forefront, and this has spurred several competing solutions by consumer advocates as a way of allowing users more control over their online actions. It operates by setting a flag in the HTTP header, indicating to the ad-networks that the particular user does not wish to be tracked. However, in the present form, there is no legal mandate for the ad-networks to comply with this directive and this might require government intervention to enforce universally.

The advertising industry, in an effort to stave off possible intervention, has introduced a few initiatives at self-policing and information disclosure. The most prominent being Ad-Choices [7], which instantiates a small, recognizable icon next to ads, which when clicked, provides some information about why the ad is being displayed and allowing the user to opt-out of such ads. A recent study states that this effort seems poorly implemented and not uniformly implemented across the various ad networks [17]. These efforts [7, 12], at a high level, match the goals we set out in this paper, i.e., to provide transparency and (or) control. However, our approach does not rely on the ad-networks compliance or cooperation and does not affect their underlying business models.

Finally, the last body of work is motivated by addressing the privacy concerns inherent in the ecosystem. Here, we see new architectures that support the delivery of relevant ads to users without requiring that users disclose their web browsing histories to third parties and ad-networks. Privad [16] provides privacy guarantees by storing all the information for ad-targeting locally. Web traffic is routed through an anonymizing proxy that strips out all identifying information and ads are delivered by a broker entity that is untrusted. Privad introduces new agents – ad-brokers that collect and distribute ads, and dealers which proxy for users- and is incompatible with the current ad ecosystem. Adnostic [23] also suggest storing the user’s profile locally; rather than individual ads being pushed to the browser, it requests a large bundle of ads from the ad-network and selects the displayed ad from this set based on the local profile. ObliviAd [8] makes use of the secure co-processor (SC), and proposed a Private Information Retrieval (PIR) protocol for distributing advertisements without revealing user information to the ad networks. A drawback of ObliviAd is that it requires specialized hardware and is not compatible with systems that exist today. RePriv [14] describes a novel architecture where the user profile is constructed near the user and then only sent to the ad-network with explicit user approval. CoP [9] uses a special cookie to store behavioral information, which is sent to the ad network only when an ad needs to be displayed. The ad network updates the cookie content through a machine learning method and then sends back an ad along with the updated cookie to the user.

Although the above methods provide strong privacy guarantees, their common problem is that they all require significant changes in the advertising ecosystem, either by completely changing the way they operate, introducing new hardware components or relying on adherence to (yet) non-existing regulations. Our main motivation is to introduce transparency and inform users to the extent that they are being behaviorally targeted. We build a practical system that achieves this, and in addition, discuss methods for extending it so that privacy-aware users can prevent ads of particular categories to be displayed to them.

8. CONCLUSION

We present the design and implementation of AdReveal, a novel browser based tool that provides end-users a way to reason about how their online interests relate to the ads that they receive. We describe a mechanism to compute a targeting score, a single metric that informs users about the extent of fine grained ad targeting that they are currently experiencing. We then describe some ideas on how users can exercise control over the categories of ads being received, if they are uncomfortable with the level of targeting (on any particular category or interest profile). AdReveal enables this transparency and control completely inside the browser and does not require any cooperation or redesign of the existing ad ecosystem. We also present a detailed characterization of this targeting metric and related measures over web browsing sessions derived from the search logs of 20 real users. In our future work, we plan to publicly release this tool after implementing the ad-control mechanisms described in this paper and gain a deeper understanding of user attitudes and issues with targeted online ads.
9. REFERENCES