Improving Ad-Relevance in Proxy-Based Circumvention Systems

MSCS Thesis

Hira Javaid
2015-03-0004

Advisor: Dr. Ihsan Ayyub Qazi
Co-advisor: Dr. Zartash Afzal Uzmi

Department of Computer Science
Syed Babar Ali School of Science and Engineering
Lahore University of Management Sciences

Dedicated to ...

Acknowledgements

I would like to thank my advisor Dr.Ihsan Ayyub Qazi and co-advisor Dr. Zartash Afzal Uzmi for their continuous advice, motivation and support throughout. It has been a great experience to work and research alongside them. I would also like to thank my colleague Hafiz Kamran Khalil who has co-worked on this project and for his helpful comments on this document.

Abstract

In proxy-based circumvention systems like Tor and Lantern, the content of the ads depends on the location-based characteristics of the proxy that connects to the web server and not the actual user. This results in highly irrelevant ads that are annoying to the user, and are additionally harmful to the online advertising industry, which by allowing web publishers to offer their content free is a crucial part of the Web ecosystem today.

As part of a solution to the problem, Advention is a circumvention system that modulates the functionality of existing proxy-based circumvention tools, specifically Tor, to provide targeted ads. It does this by directing the requests of the censored content via the circumvention tool's proxy, and the requests to the ad ecosystem via the direct internet route. This enables greater transparency into the user's location information, thus allowing an increase in relevant geo-targeted ads. Furthermore, to increase contextually relevant ads, that is ads dependent on the content of the publisher, Advention chooses a proxy in a location linguistically similar to the end-user.

Directing ad requests towards the direct path however, has implications for the privacy of the user as an ad request on the direct path may leak Personally Identifiable Information and the URL that the user is trying to access. The censor may also fingerprint these requests to infer the censored webpage being accessed. The objective of this thesis is to design and integrate mechanisms inside Advention that will ensure that user identity is not compromised. To this end, we incorporate an analysis of the attack surface that Advention exposes to the censor, in terms of the leakage of accessed URLs, as well as a censor's ability to identify users based on fingerprinting network traffic. Additionally, we propose Page Load Times as a measure to demonstrate the usefulness of Advention to the end-user in addition to its primary function of providing relevant ads.

Contents

List of Figures

List of Tables

1. Introduction

1.1 Internet Censorship and Measurement

Internet censorship is a phenomenon under which entities, such as repressive governments, attempt to control the free nature of the Internet, usually for maintaining political and social control. This control is most commonly achieved by actively incorporating systems and mechanisms into the normal functioning of the Internet that bar users from accessing freely available content.

As more and more users turn towards the Internet, especially social media, for sharing and disseminating content, as well as using it as a tool to actively engage in various forms of online activism, there is a corresponding spike in censorship by governments seeking to curb free expression. A recent study, Freedom on the Net 2016 by Freedom House [1] reported that about 67% of internet users live in countries where censorship is regularly practiced. This is a huge swathe of the internet population, and therefore, not surprisingly, censorship has become an area of active research focus. Countries whose censorship regimes have been studied extensively include China [3,4,5,6], Iran [15], Pakistan [9, 10], Syria [14] and Thailand [7]

Since censorship relies on blocking access to free-flow of internet resources from content distributors to content users, the mechanisms used to effectively employ it on a country-level (typically) scale, necessarily use techniques that disrupt standard networking protocols and architectures. These techniques usually attack one or more of the stages of communication that occur, from the time when the user first enters the name of the website in the web browser to the time they receive back the HTML webpage and its resources. Disruption may occur by either modifying, deleting and inserting content or by pro-actively preventing contact between the user and the server. Communication along several of the OSI layers may be attacked, especially the application, transport, and the network layers (See *Section 2.1*).

In response to censorship's increasing disruption of internet's protocols, a large body of work deals with characterizing censorship, how it takes place, when and where it takes place, and the techniques deployed to censor content [16]. These measurements are an initial first-step towards understanding the underlying progression of how censorship occurs, both for internet activists as well as computer science researchers interested in developing circumvention tools that may help censorship evasion. Some of the challenges in this space include obtaining diverse vantage points in a possibly heavily surveilled censorship region. Tools that currently exist for such measurements include OONI[1], Encore and CSaw [17, 18, 10].

1.2 Circumvention

In response to these censorship mechanisms, we have what are known as circumvention tools that allow a user to bypass censorship and access otherwise blocked content. Most common circumvention systems are proxy-based, that is they rely on an external proxy located inside an uncensored network to tunnel traffic on user's behalf. However, the fact that the proxy has a distinct IP address [19] and that any traffic routed towards the proxy passes through a censored network, the censor always has a distinct advantage. It may block all attempts to connect with these circumvention proxies causing the circumvention tool to adopt other methods to evade blockage (such as in Tor which uses special previously unknown relays known as bridges) In addition to these proxy-based systems, we have such methods as using an Open DNS server, domain fronting and decoy routing, that come into the category of non-proxy based circumvention tools.

[1] https://ooni.torproject.org/

1.4 Impact of Internet Censorship

Censorship is typically deployed over at least a country-wide region with millions of internet users, and hence its impact can be seen on a diverse variety of stakeholders in the ecosystem, not excluding the internet's architecture itself. The consequences may be faced by the ISPs, as they incur the financial cost of the deployment of censorship equipment. An increase in encrypted traffic as a result of the usage of tools such as VPN and Tor may also up the cost of an ISP, as it can no longer cache content (as a result of encryption) and needs to contact upstream servers to fetch this encrypted content. Similarly, content providers may also see a decrease in their revenue as users switch over to competing content-providers who provide the same service. This was seen in Pakistan in the context of the Youtube ban as others video-providers jumped in to take the share of the advertising revenue that was previously directed towards Youtube. [9]

Censorship may also cause a noticeable change in user behavior, causing them to self-censor or otherwise alter their internet browsing patterns. This has been seen in the context of porn and video-content consumption in Pakistan as well as self-censorship in the context of politically-motivated censorship in Thailand. [7]

Finally, we may also see collateral damage on Internet's traffic as a result of mechanisms deployed to disrupt with the internet flow. An example of this is the injection of DNS responses where a censoring entity continuously monitors DNS queries and sends fake responses that compete with legitimate ones. However, it may happen that queries to TLD servers from outside the censored network get assigned a path that passes intransit via internet routes in heavily censored areas. If such a query is spotted by the censor's DNS query monitors, then a fake DNS response may be sent to the non-censored originating client. Occurrences of this type of collateral damage has been seen in the transit traffic that has passed through the Great Wall of China's censorship regime. [20]

1.3 Censorship Impact on the Online Advertising System

Online Advertising Industry is the key economic driver of the free model of the internet under which internet content on websites is made freely available in return for users agreeing to view the ads being shown on these websites. Its especially important for small publishers who depend, for the most part, solely on advertising revenue to maintain and keep up their websites.

Ads on the web today are served by a complex architecture of interconnected entities that collect information about users using the mechanisms of online tracking to show closely targeted ads to the end-users. Despite the implications of privacy, this industry continues to flourish, with the IAB[2] reporting a revenue of **72.5 billion** in 2016. [21]

As mentioned in the previous section, censorship impacts a wide range of stakeholders including the ISPs, users and the content-providers. While all of these impacts have been studied in previous works [7,9], no other work has studied its impact on the online advertising system which is the financial cornerstone of today's web. One of the impacts comes in the form of irrelevant ads, especially ads that are targeted based on a user's location and the contextual information provided by the website's content.

When users deploy proxy-based circumvention tools, these tools act as intermediate traffic bypassers that help carry users' requests for censored content away from the prying eyes of a censor. While this allows effective circumvention to occur, the new information that travels to advertising networks does so on behalf of the proxy and therefore is no longer tied to the user. This results in loss of key geographical and contextual insights that enables advertising systems to provide relevant ads. A significant revenue loss for publishers as well as advertisers may occur and this is the impact we hope to study and address in this work.

1.4 Problem Statement

As discussed, proxy-based circumvention systems may cause the user to see irrelevant ads and additionally revenue loss for publishers as well as all the entities involved in the online advertising ecosystem, thus hitting the very structure that keeps the world-wide web alive and functioning. To the best of our knowledge, no previous work, has studied this very crucial consequence of internet censorship.

As part of a solution to the problem, Advention is a circumvention system that varies the functionality of existing proxy-based circumvention tools to provide targeted ads. It does this by directing the requests of the censored content via the proxy, and the requests to the ad ecosystem via the direct internet route. This enables greater transparency into the user's location information, thus allowing an increase in relevant geo-targeted ads. The technique works because requests to the advertising server are almost always intended for advertising servers that serve a large body of internet content including the content served on non-censored websites.

[2] Interactive Advertising Bureau

Thus, censorship regimes, for the most part, do not take the radical step of blocking these servers so as to avoid collateral damage affect uncensored sites.

Directing ad requests towards the direct path however, has implications for the privacy of the user as an ad request on the direct path may leak Personally Identifiable Information and the URL that the user is trying to access. The censor may also fingerprint these requests to infer the censored webpage being accessed. The aim of this work is to build a system that provides relevant ads yet at the same time does not compromise the identity of the user to the censor. To this end, the following thesis contains a measurement study into the privacy implications of directing ad requests via the direct path as well as for the relevance of ads.

1.5 Thesis Flow

The structure of the document is as follows. Section 2.1, 2.2 and 2.3 deal with the broad censorship and circumvention space. The later subsections of Section 2, 2.4 - 2.7 get into the background of the Online Advertising Industry and previous work that has been done in the space of studying the industry as well as building systems that provide privacy-aware targeted advertising. Sections 3 and 4 go into Advention, the problem it solves and its Evaluation and finally Section 5 discusses Advention's challenges and future work.

2 Background and Literature Review

2.1 Internet Censorship Types and Measurement

Internet Censorship in the modern world is continuously on the rise. When censors block communication between a client and the content-serving server, they do so on the basis of unique fingerprintings or distinguishers found on multiple layers of the network stack by which a particular type of traffic can be distinguished.

Some of the forms of Internet Censorship are briefly discussed below:

DNS Layer Blocking

DNS layer blocking occurs at the very first stage of user-server communication when the hostname to the website is translated to an IP address by a user's DNS resolver. If this resolver is located at a censoring ISP, the ISP has full control over the manipulation of subsequent DNS responses. These responses may belong to any of the following types:

1. an NXDomain response indicating falsely the non-existence of a censored domain
2. an IP address corresponding to a Block Page that is a page that indicates to the user that the IP has been blocked
3. an IP address corresponding to an Error Page.

In all cases, the user fails to receive the IP address of the domain that they intended to access.

All of the above types of DNS tampering fall under the heading of DNS hijacking. However, DNS hijacking is not the only form of censorship that may occur on this layer. DNS injection is another type in which a censoring device in the network actively surveils for an sign of DNS queries for hostnames directed to port 53 on the UDP protocol. Once detected, a forged DNS response is sent to the user, which if it get backs to the user fast enough, may usurp the validity of the original legitimate DNS response. [20, 16, 2, 6]

TCP/IP layer Blocking

If not censored at the DNS layer, TCP/IP layer is next in line, where either the initial TCP handshake or the subsequent flow of packets along that connection may be targeted. Just as in the case of DNS injection, a censoring device or a middlebox in the network, looks for signs of traffic which matches the ports or the IPs of a blocked domain. If found, forged TCP reset packets are sent. These reset packets are special packets in which the RST bit in the TCP header has been set to 1, and which indicate to the end-host receiving the packet that the ongoing connection is being terminated. If falsely sent, these packets cause a premature termination of a TCP connection, thus achieving the censor's goal of blocked access to web resources flowing along that connection.

HTTP Layer Blocking

If the connection is not encrypted, censorship may additionally occur on the application layer, when an HTTP GET request is sent out to the server to request a particular resource. Over here, the hostname or the resource path in the HTTP header may be matched with a blacklist of keywords and urls, and as in the case of TCP/IP blocking, an RST packet is sent to terminate the particular connection [16]

TLS Blocking

In addition, if an encrypted connection is being negotiated, connection set-up might also involve the TLS handshake, where the client and the server come to consensus on TLS protocol versions, accepted ciphersuites as well as certificates. As a result of encryption, all types of content and url snooping on the HTTP layer cannot occur at this stage. However, there is a special field known as the Server Name Indication field sent during the TLS handshake process which, in normal circumstances, enables the client to communicate to the server the particular host to which it wants to connect to. This is necessary when multiple domains are situated behind a single IP. But under a censorship regime, the SNI field, which goes out in plaintext, may expose an attack surface to an otherwise secure protocol.

Censorship Measurement

In response to censorship, in recent years we've seen an increase in work that deals with purely studying and measuring the extent of censorship that takes place. The most well-known among these measurement systems is OONI which is an initiative by the Tor Project that attempts to detect and measure internet surveillance and censorship around the world by local passive network probes. To test connectivity, it accesses a website with the local IP address and compare this connectivity at an external network where preferably no censorship is taking place.

Other censorship measurement platforms include CSaw[10], Encore[18] and UBICA [17].

CSaw provides customized circumvention based on the type of censorship that is taking place which in turn enables it to choose a circumvention tool that offers best performance to the end-user. This incentive promises to solve the problem of deployment of censorship-measurement probes.

Encore, on the other hand, exploits cross-origin requests from willing website providers to measure censorship from varied censorship points. When a user visits a participating website, cross-origin requests to censored sites are sent, and are used to measure the current censored state in that region.

2.2 Circumvention Systems

In response to censorship, a variety of circumvention systems have emerged that attempt to bypass a censor’s monitors. These could be either proxy-based systems which incorporate the use of a single or multiple proxies to carry traffic away from a censored region or non-proxy based systems which are dependent on a mechanism other than a proxy. These include such methods as OpenDNS, Domain Fronting and decoy routing [19, 13]. Since proxy-based systems are more relevant to our work we are going to describe them briefly in the following subsections.

2.2.1 Proxy-Based Systems

2.2.1.1 Tor

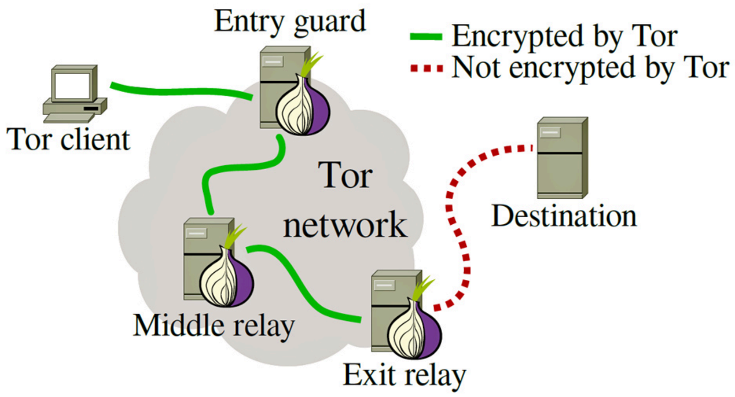


Figure 1: Tor's Architecture[3]

Tor [22] is among one of the more popular tools today that attempts to provide the twin functions of anonymity as well as circumvention of censored sites. As can be seen in figure 1, Tor's anonymity is built around a circuit of multiple relays/nodes (usually three) along which a client's traffic is moved towards its destination instead of the usual direct route. The messages are encapsulated in multiple layers of encryption (via onion routing principles and techniques) and the wrapping and unwrapping of messages happens in such a way that no two nodes can uncover both the source and the destination address of the traffic in question. This is what gives Tor its anonymity.

The main consequence of Tor's basic architecture of three nodes (entry, middle and exit) on the advertising system is that the end-server (the webpage) and hence the advertising system only sees the IP, location and contextual information of the exit node making the connection rather than the user themselves. The ads that the user sees are therefore targeted to the node rather than to the originating user.

[3] https://arstechnica.com/security/2014/01/scientists-detect-spoiled-onions-trying-to-sabotage-tor-privacy-network/

2.2.1.2 Lantern

Lantern[4] is another circumvention tool that allows circumvention of content in censored countries. It does so by maintaining a network of proxies to which the users may connect. These proxies may either be Lantern-owned or owned by other users present in uncensored countries. A user may choose either of the two types of proxies dependent on their personal privacy preferences, and also has the option of choosing a proxy belonging to another user they trust. [13]

As opposed to Tor, Lantern's primary focus is on circumvention and performance and not on anonymity. Similar to Tor and other proxy-based circumvention tools however, it does involve an obscuration of the original source. While this is the reason for successful circumvention, it prevents successful ad targeting from taking place.

2.2.1.3 Single-Proxy Systems

These include all services that provide circumvention by means of a single server that acts as an intermediate relay between the client and the server. Like Lantern, none of these proxies promise to provide anonymity but rather focus on providing a user a safe passage away from the censored region to the end-server.

2.2.1.4 VPN

A VPN or a Virtual Private Network works by creating an encrypted tunnel between the user and the VPN servers that carry the traffic over to the servers of the webpage being accessed. As a result of this intermediation, the censor sees the IP of the VPN server rather than the endpage, and hence the traffic passes forward freely without being dropped by the censor's monitors. As before, the end-server sees the source as the VPN server leading to a significant loss of relevant information about the user.

2.3 Online Advertising Industry

2.3.1 Online Advertising EcoSystem

Advertising on the internet is a rapidly growing industry with revenues totalling $72.5 billion in 2016 in the United States alone [21], an increase of 21 % from 2015. These revenues add to and

[4] https://getlantern.org/

are responsible for the internet's rapid growth by being a financial bedrock on which many publishers and platforms depend for their financial survival. Additionally, as long as the users are willing to view ads and do not employ any blocking measures, the online advertising industry allows the publishers to offer their content completely free of charge.

The advertising network that provides the ads themselves is hugely complex, intertwining the publisher with the advertiser and finally the user by means of a diverse range of intermediate entities. The following section includes a brief overview of all the entities involved and their respective functions in the advertising system. In the later sections, we will take a more granular view into the ad networks and ad exchanges themselves.

2.3.2 Entities

2.3.2.1 Publishers

A publisher owns the webpage, and agrees to place ads, in the form of embedded images or otherwise, on behalf of external entities such as the advertisers. This agreement to show ads alongside content occurs only in exchange with payment commensurate with the content of the webpage, placement of the ad and value of the user to the advertiser.

2.3.2.2 Advertisers

These are entities or groups wishing to advertise their service on publisher platforms and agree to pay a set amount to these publishers in exchange.

2.3.2.3 Ad Networks

An ad network acts as an intermediary between the advertisers and the publishers. It aggregates ad spaces across multiple publishers, categorizes them, and then offers them up to the advertisers to buy. A single platform to buy ads is more efficient for the advertiser as it does not need to contract with all online publishers individually. Similarly, it allows the publisher to sell their ad placement spaces at a single marketplace.

2.3.2.4 Ad Exchanges

Ad Exchanges are a recent evolution of the ad networks which remove the intermediaries which previously mediated communication between the publisher and the advertiser. Removing these intermediaries allows the two entities to communicate directly. Ad Impressions on websites are auctioned in real-time to advertisers who bid on each ad space on the basis of the value it provides to them, in terms of the user, the content of the webpage and so on. We discuss this in more detail in the following sections.

2.3.3 Targeting and Types of Targeting

2.3.3.1 Tracking

Tracking may be essentially defined as a mechanism used to identify users as the browse across the web through multiple publishers. In the early years of the web, only first-party websites could attempt to undertake tracking, and that too only while the user was present on their own webpages by means of first-party cookies, HTTP Referer headers or geolocating IP addresses. After the emergence and increasing popularity of a website model where embedded resources were fetched from multiple parties instead of just one, third-party tracking has become the leading driver of user behavioral information gathering process.

A first-party webpage, that is the main domain which the user is trying to access, may embed resources originating from external entities such as advertising servers, CDNs, social networking sites, and analytics providing servers. When such a webpage is fetched by the user, a cookie travels not only to the primary domain but also to the servers of each of these external entities. This type of a cookie is termed as a third-party cookie in contrast with a first-party cookie that is forwarded to the main domain. The external entities to which this cookie travels include popular advertising servers such as DoubleClick owned by Google and social networking sites such as Facebook and Twitter whose widgets are known to be embedded within a vast majority of publisher webpages [23]. Just by the virtue of this widespread presence, these parties can track users as they browse across websites, and thus maintain a continuous browsing profile connected to their identity, which in the absence of browser fingerprinting, is mostly an IP address.

As users are increasingly drawn towards deleting their local cookies due to the privacy leakage these cookies allow, other innovative and resilient mechanisms have come into play. Among these include the relatively indestructible EverCookies which are cookies designed to be recreated and respawned from multiple browser storage states even after a user destroys them once. Additionally, browser fingerprinting is another method whereby a particular user's fingerprint can be fashioned by means of local, user-centric properties of the particular browser and the system specifications on which the browser is running. [24, 25]

2.3.3.2 How Tracking Drives Targeted Advertising

This capability to put an identity marker on users as they travel across the world wide web allows these servers to aggregate information about their browsing history, which pages they have visited, how many times, and for how long. This type of information can be made to figure out quite an interesting amount of revealing information about a user's interests, likes and dislikes, their location, employment status and other more sensitive private information such as political beliefs, sexual orientation and health and financial challenges [26, 27]. Once data has been aggregated it can be divided into behavioral segments by a host of machine learning and data mining algorithms. These segments are then finally used by advertisers to send customized ads to the end-user in a process known as Targeted Advertising, the main purpose of which is to maximize the effectiveness of advertising and hence the resultant revenue.

Targeting is actively carried out not only by the advertisers themselves but by a range of intermediate Data Collecting or OBA (Online Behavioral Advertising) entities that indirectly sell behaviorally segmented users to the advertisers. [28]

Types of Targeting:

Ad-Targeting Platforms such as Google AdSense[5] offer multiple targeting mechanisms by which an advertising server can target the end-user, or by which the ad server makes the final decision of which particular ad to show to the user. These mechanisms can be categorized as:

1. Geographical targeting
2. Contextual Targeting
3. Behavioral Targeting
4. Retargeting

Geographical Targeting

This type of targeting may occur when a user is shown ads based on their particular location. The location is determined by means of geolocating the IP address of the user extracted from the HTTP GET request sent from the user's browser to the Google Advertising Servers. Location to target can be chosen to as fine a granularity level as that of a fixed radius around a particular

[5] https://www.google.com/adsense/

location, which may enable advertisers to target users based on their business locations or particular places that they want to target. [29, 30]

Contextual Targeting

This type of targeting deals specifically with the particular content of a webpage. As an example, a sports equipment advertiser may choose to target users visiting only websites whose content analysis reveals them to be sports websites. To enable this type of advertising, entities known as ad networks parse the content on a webpage, and extract the keywords or other data-mined elements to later form content categories that can be matched to a relevant advertiser. [31, 32]

Behavioral Targeting

As noted previously, there are entities on the web that actively track and store user behavior and interests for the sole purpose of selling this information to the advertisers. Ads that are shown based on this user profile are known as behaviorally targeted ads, and can include such information as a user particular behavior as well as demographic information such as their gender and age. [31, 32, 27]

Retargeting

This is a special type of advertising where a user is shown ads based on a website they visited before, or having shown an interest in a product available for purchase on that website. A user may for example visit Amazon.com to purchase a book, and then move on to some other website without completing the purchase. An ad endeavoring to persuade a user to purchase the book, sometimes with a discount, could then be shown on other websites that the user visits. Retargeted ads are made possible by a process known as cookie syncing which will be discussed in the following sections on the advertising landscape. [31, 33]

2.3.4 Information Flow in Advertising

2.3.5.1 Advertising Landscape

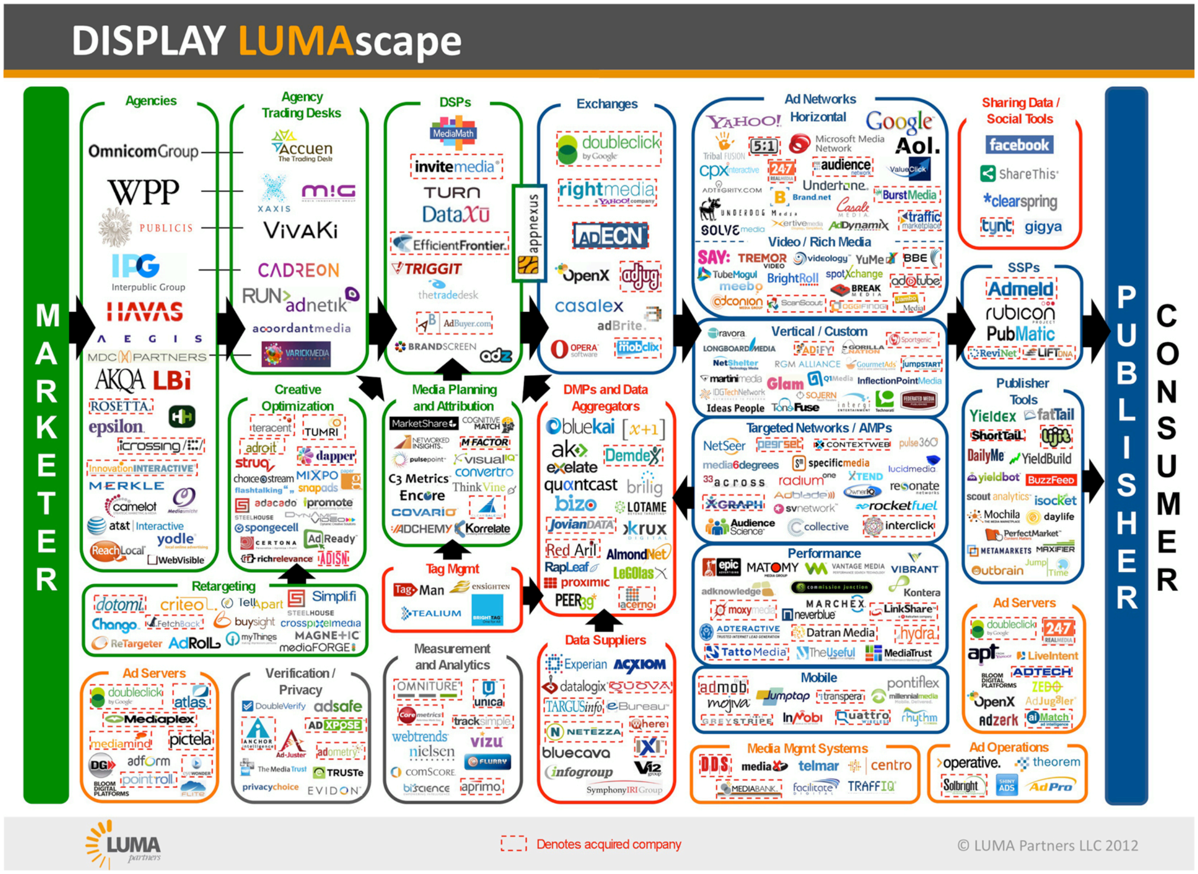


Figure 2: Display Lumascape[6]

[6] http://www.lumapartners.com/wordpress/wp-content/uploads/2012/04/Display-LUMAscape_2012-04-05.jpg

As can be seen in the famous Display Lumascape image in Figure 2, the current advertising landscape is hugely complex. A vast network of entities, each with their own function, connect the Publishers with the Advertisers. In the following section, we will start with an initial background into the history and then briefly explain the entities and their functions.[34]

Historical Overview

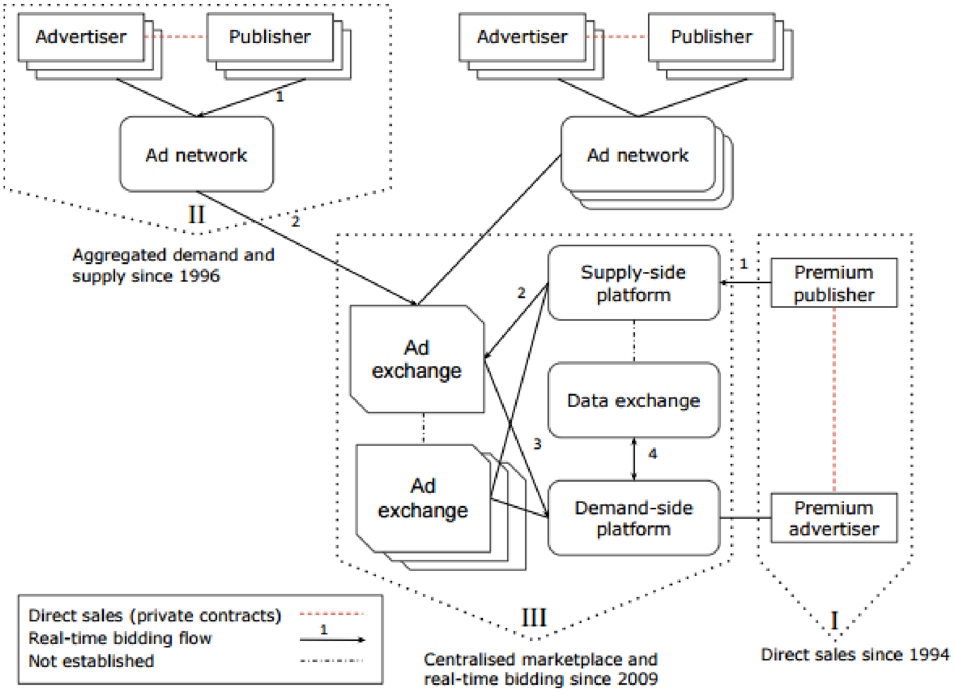


Figure 3: Historical Overview. Box I represents the intial premium contract based advertising, Box II illustrates the AdNetwork Model and finally Box III shows the current evolution of the industry in the form of Ad Exchanges [35]

Figure 3 illustrates a brief history of the online advertising industry. In its beginning stages, before the proliferation of ad networks and ad exchanges, placement of ads on webpages occurred by means of direct contracts between the publishers and the advertisers. Premium contracts were negotiated by the publishers with advertisers, with the publishers ensuring a fixed number of impressions to the advertisers. Advertisers did not have any insights on what kind of audience was being targeted, their behavior or identification.

Ad Networks

As an improvement on direct contracts between publishers and advertisers, ad networks came into being to provide more transparency and a finer degree of targeting for the advertisers. These networks are essentially intermediate online marketplaces that seek to connect the publishers with the advertisers. Both of these entities, on their end, enter into contracts with the ad network, whose job it is to connect the right publishers and users with the particular demands of the advertisers. The essential function of an ad network was to aggregate inventories over multiple websites and offer them at one place to advertisers.

Additionally, It is over here, inside ad networks, that the process of targeting, as discussed previously, comes into play. Ad Networks segment the users according to the tracking data they have and simultaneously segment publishers on the basis of the content within them. These categories are then matched with the particular targeting criterion of the advertisers to place the most relevant ad on the most relevant website for the most behaviorally or geographically relevant user. Among the companies that own ad networks include Google, Yahoo and Microsoft [34, 64]

Ad Exchanges

The proliferation of ad networks however led to the emergence of platforms known as ad exchanges which allow the buying and selling of ads in real-time auctions by a process known as Real-Time Bidding (discussed later). Multiple ad networks reside inside a single ad exchange which enables a more efficient distribution of ads between the publishers as in the case of ad networks [64]. Example ad networks include Google's AdX, Yahoo's Right Media Exchange, AppNexus, OpenX, Rubicon Project and Microsoft Ad Exchange. [36]

Supply-Side Platforms

These are platforms that act on the behalf of a publisher during the process of Real-Time Bidding. They enable publishers to manage their inventories by for example fixing desired prices for certain ad placements and setting preferences for certain advertisers or bidders.

Demand-Side Platforms

Demand-Side Platforms deal with the advertiser side of things, and enable them to place bids and manage their budget across multiple ad networks and publishers. [35]

2.3.5.2 How Ads are Fetched

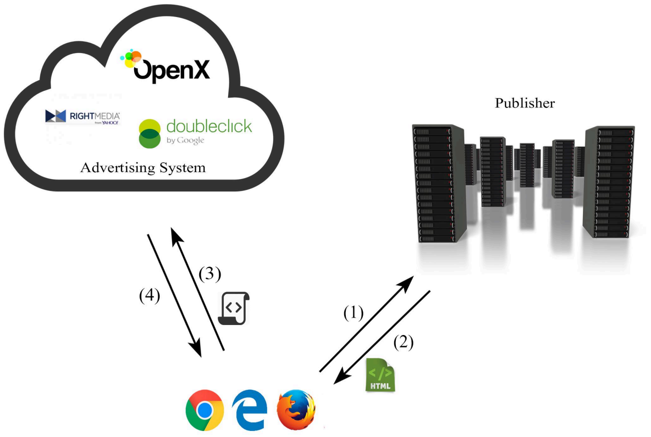
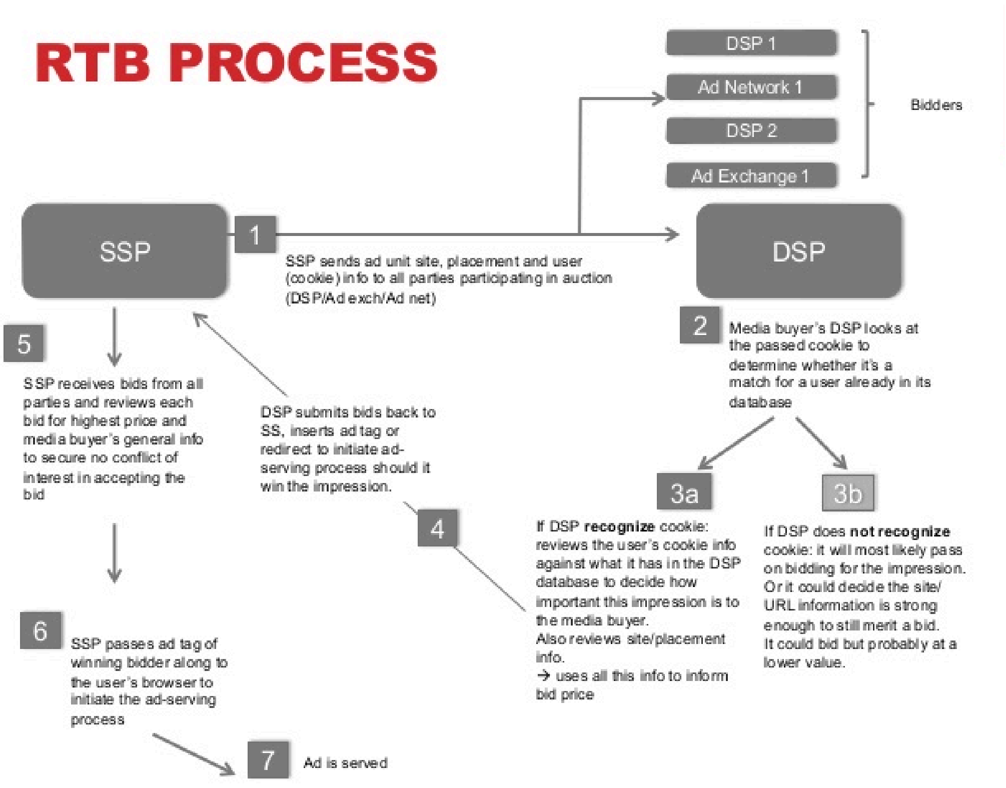


Figure 4: How Ads are retrieved

Simple Ad-Fetching

Figure 4 shows the flow of information that takes place when an ad is retrieved for a user on a webpage. When a user types the url of a webpage in a browser, an HTTP GET request is sent over to the publisher (1), who sends back the HTML of the webpage (2). Embedded within this HTML is something known as an ad tag (3), which in simple terms, is just a piece of HTTP request (contained within a tag) used to indicate to the ad server that an ad is required at that particular placement on a particular website and by a particular user. The HTTP request code contains within its query string parameters keywords that enable the advertiser to know the particular website and the keywords that define it. Furthermore, this request can be geographically located by means of an IP address to enable the advertiser to provide geo-relevant ads. [OpenX Ad Networks vs Ad Exchanges] Based on all the information inferred from the ad tag, the advertising system makes its decision about which ad to show to the particular user, and sends it back in the form of an image back to the user (step 4)

Real Time Bidding



1 SSP sends ad unit site, placement and user (cookie) info to all parties participating in auction (DSP/Ad exch/Ad net)

2 Media buyer's DSP looks at the passed cookie to determine whether it's a match for a user already in its database

3a If DSP **recognize** cookie: reviews the user's cookie info against what it has in the DSP database to decide how important this impression is to the media buyer. Also reviews site/placement info. → uses all this info to inform bid price

3b If DSP does **not recognize** cookie: it will most likely pass on bidding for the impression. Or it could decide the site/ URL information is strong enough to still merit a bid. It could bid but probably at a lower value.

4 DSP submits bids back to SS, inserts ad tag or redirect to initiate ad-serving process should it win the impression.

5 SSP receives bids from all parties and reviews each bid for highest price and media buyer's general info to secure no conflict of interest in accepting the bid

6 SSP passes ad tag of winning bidder along to the user's browser to initiate the ad-serving process

7 Ad is served

Figure 5: How Real Time Bidding Takes Place

RTB bidding differs from standard exchange between the publisher and the ad network by introducing an interesting concept of real-time bidding. In real-time bidding, the initial request to the advertising system proceeds forwards as before. This time however, this request is directed towards an ad exchange by means of an SSP representing the publisher. Once inside an ad exchange, the ad-exchange opens up this request to multiple advertising parties or DSPs representing these entities along with the information the ad exchange has about the publisher, ad placement, and the behavioral characteristics of the user whose browser the ad request originated from. The behavioral characteristics of the user are more specifically derived by the DSPs using a process known as cookie syncing or cookie matching. When an SSP sends its user cookie to the DSP it has no way of identifying the user except by the cookie SSP holds. To enable a DSP identify the user, an SSP sends an HTTP redirect from the user to the DSP. Piggybacked on this request is the cookie SSP itself holds on the user. This enables the DSP to maintain a matching of SSP's cookie with it own cookie in its databases. In subsequent ad auctions when an ad request from the user reaches the DSP, it compares this cookie with the cookie in its local databases, and all the behavior of the user associated with it.

In the process of a bid, multiple such DSPs place their bids on the ad according to the value they place on the user. The highest bidder wins the auction and earns the right to place their ad for that user. All of this entire request-chain takes place within a few hundred milliseconds, the time it takes for the request to go the webpage publisher and come back with a response. [37, 35, 33, 38]

2.3.5.3 Revenue

The way an advertiser chooses to pay a publisher in the Online Advertising Industry is represented by means of several pricing models. These include CPM or Cost Per Mille (Cost per thousand impressions) where an advertiser pays the publisher for a thousand views, CPC (Cost Per Click), or Cost Per Acquisition where a cost is paid by the advertiser only after a certain criterion has been met for example a click, a sale or the submission of a form. Premium Contracts in the beginning followed a CPM model while ad networks have been known to employ both CPC as well as CPA models. [35] Real-Time Bidding, on the other hand, follows the CPM model for the most part. [38]

2.4 Advertising Measurement Systems

This category of research basically deals with systems that seek to measure how information collected by online tracking mechanisms is used to target users and serve them relevant ads.

2.4.1 Challenges in Measuring Online Advertising Systems

This paper is one of the initial works in this field that sought a more transparent view into the online advertising landscape. It introduces measurement methodologies to measure ad networks, and how data about the users, which these networks regularly collect, is being used to provide targeted ads. Much of this had historically not been made public at the time this paper was written, and still is obfuscated for most ad networks for reasons of keeping it as a trade secret. This paper sought to find out how search, contextual and ads on social networking sites differ as you vary the user behavioral information available to the ad network. A few of the challenges this paper addressed were the difficulties of comparing two ads in the face of adservers obfuscating the unique IDs of particular ads, as well as the challenge of collecting ads in the presence of ad churn whereby multiple loadings of a webpage loads different ads. [39]

2.4.2 AdReveal: Improving Transparency into Online Targeted Advertising

This is a work that seeks to provide transparency to the end-user about the specific kind of targeting mechanisms used to serve a particular ad. This, they argue, would lead to a more fine-grained control by the user into the kind of ads that the users wish to see, and which kind of targeting they want to be a part of. For this purpose, a measurement tool is developed as a browser extension that determines contextual, behavioral and retargeting on the basis of machine learning classifiers and a dataset of 139K ads and 103K webpages. The paper also presents an analysis of the particular ad categories that employ different types of targeting. For example they found that ad categories related to Insurance, Tourism and Travel and Real-Estate were heavily behaviorally targeted. In addition, the authors also found a general overall prevalence of behaviorally targeted ads, more so than contextually targeted ads. [31]

2.4.3 Adscape: Harvesting and Analyzing Online Display Ads

This is another measurement study that tries to understand the dynamics within the online advertising system. A crawling measurement infrastructure is developed that collects ads shown to users based on varying user profiles. 180 English-language websites were crawled using 340 different user profiles to collect an ad dataset of 175K different ads. In addition to some general characteristics of the adscape, the authors main focus is discovering the impact of user profiles on the proportion of targeting ads. A significantly high prevalence of targeted ads as compared to untargeted ones was found roughly 80%. In addition, they also find about 3.7K unique advertising entities inside their dataset. [32]

2.4.4 Tracing Information Flows Between Ad Exchanges Using Retargeted Ads

As mentioned before, Online Tracking is the key mechanism that is being used to drive targeted advertising. Tracking may occur through third-party cookies or if such cookies are destroyed via more persistent mechanisms such as browser fingerprinting, Flash and Ever cookies.

In all of the above mentioned user identification methods, the flow of identifying information travels from users' browsers to tracking entities or advertisers like DoubleClick (owned by Google) and social media entities like Facebook. In contrast to this type of single-directional flow, there is an additional form of both-way data sharing that takes place between the ad exchanges themselves. This incorporates the novel use of a method known as cookie-matching to allow the aggregation of partial data that each ad exchange has to form a fuller picture of a user's behavioral patterns. The authors of this paper develop a methodology that isolates the Ad Exchanges among which this type of flow is taking place. They do this by making use of the properties inherent inside retargeted ads. [33]

2.4.5 I Always Feel Like Somebody is Watching Me

This paper's main focus in on Online Behavioral Advertising. Using user-profiles or personas with specific behavioral traits such as movies or cooking, they build an automated measurement system that as previous works mentioned before tries to bring a more subtler understanding of the ad system. Their main insights include the high extent of OBA, the targeting of sensitive topics such as religion or health by the advertisers, as well as the fact that DNT or the Do-Not-Track flag is not yet respected by advertising entities. [27]

2.5 Advertising and the Online Tracking/Privacy Debate

2.5.1 Online Tracking and its Privacy Implications

Recent years have seen widespread furore over the privacy implications of the information gathered by means of currently prevalent online tracking mechanisms. While the information made available through these systems helps drive the entire advertising industry, not excluding the publishers themselves, it is a fine tread in the middle as many users are increasingly discomforted by the pervasive nature of this tracking and its effects on their privacy. The increasing prevalence can be illustrated by this research [empirical study of web cookies] which showed that DoubleClick alone can observe visitors on about 40% of websites present on Top 100K Alexa websites. Similarly, another work discusses the privacy implications of Cookie Matching and Real Time Bidding revealing that as much as 27% of user browsing history can be leaked to the bidders during the RTB process [38]

Some studies however show that users have mixed feelings over targeted and behavioral advertisings. Some users believe more targeted ads would be acceptable as long as they have more control over the kind of data that is being collected about them and the specifics into which entities are collecting this data [40] More fine-grained control such as choosing ahead of time which particular information to disclose is also appreciated by a large-extent of users.[41] Other users recognize the revenue benefits that collection of their profiles and subsequent targeted ads may offer to publishers and advertisers but are concerned about malicious usage of their data, such as data falling into the wrong hands [42], in addition to generic privacy concerns, some even fear the creation of inaccurate profiles if big data is misconstrued and misinferred by faulty or biased algorithms. [43] Additionally, there is also the danger of increasing self-censorship by some users as they are made more aware of the data collection occurring in the background [44]

2.5.2 Online Tracking and Its Effectiveness to the Web EcoSystem

While it is expected that advertising targeted to the user will generate more revenue, relatively few studies have been done in this space to empirically show the effectiveness of targeted ads to the advertising system [45]. Among these, one study shows how targeted advertising may provide improved click-through rate by examining the click-through log of advertisements gathered from a commercial search engine. The improvement can be as much as 670% if users are properly segmented in sponsored search. [46]

Other sources show that interest-based targeted ads can accrue a revenue benefit of as much as 200% to publishers especially small-scale ones that are more likely to depend on ad revenues for their maintenance and survival. [47]

2.5.3 Adblocking, Anti-AdBlocking, the Arms Race and Finding a Middle

Ads have not always received a positive reception from the end-users. Some studies estimate an overall AdBlockPlus[7] using population as hovering around 22% of the total active users in the data from a European ISP [37]. In addition to AdBlockPlus, some users use adblockers like uBlock[8] or Ghostery[9] to block ads they perceive as annoying or irrelevant to their browsing experience. All of these browser extensions offer an ad-free browsing experience along with the promise of better page load times. Perceiving this as a threat to their overall revenue, websites have come up with anti adblocking mechanisms that block out adblocking users from accessing their webpage [48, 49] . Not to be left behind in this fast-paced cat and mouse game, the adblocking community has introduced adblocking blockers[10] that prevent these anti-adblocking scripts from detecting the presence of an adblocker.

Adblockers function by typically using filter lists or pre-known patterns of ad strings that are matched against the requests on a webpage. These can be bypassed by publishers by introducing ads with obfuscated request patterns undetectable by AdBlocker filter lists. However, further complicating this situation for the advertising servers is the Federal Trade Commission's strict regulations that require advertisements to be clearly labeled and distinctly perceivable as an ad by the user. This has induced some recent ad blocking research to utilize perceptual ad blocking that attempts to recognize ads by visually detecting behavioral advertising disclosure icons. A good example of this is the AdChoices icon attached in one corner of some ads these days. [50]

There seems to be no near end to this arms-race between the advertisers/publishers on one end and users on the other. AdBlocking and more privacy-minded users claim that advertisers should not have a free pass to collect their information and show ads without prior consent, while publishers point out that if users are not willing to pay for content, then they shouldn't be permitted to view it, since quality content-generation takes time, effort and money. In addition, supporting the publisher point of view may be the fact that blocking ads may result in

[7] https://adblockplus.org/

[8] https://www.ublock.org/

[9] https://www.ghostery.com/

[10] https://reek.github.io/anti-adblock-killer/

detrimental effects on small-scale publishers who depend entirely on the revenue stream from advertisers. The adblocking wave has already resulted in the closing down of some of these, and some fear that this may lead to a monopoly of big companies like Google and Facebook and the death of small-scale publishers who might be forced to host their content on the platforms belonging to these big players. This might potentially result in undesirable centralization of content that accompanies content being controlled by a few handpicked entities. [51, 52]

Trying to walk the middle in this controversial debate is the AdBlockPlus's Acceptable Ads program[11] and Brave Browser introduced by the creator of JavaScript Brendan Eich[12] It is built on the Chromium web browser, and offers better page load times and privacy by removing web trackers and ads. Instead anonymous ads are served by the browser's network itself and additionally users get paid to view those ads.

Other systems that try to walk a balanced line between privacy-enabling adblocking on one hand and targeted adserving on the other are discussed in the following section.

2.6 Privacy-Aware Relevant Advertising Systems

Research that comes in this category attempts to propose systems that preserve user-privacy and at the same time give access to targeted ads. For most of these papers, such anonymity is made possible by an intermediary, either local or external, that takes over some functions of the Ad Network or an Ad Exchange so as to prevent it from seeing granular details into the behavior of the user.

2.6.1 Privad

This paper [60] argues that a balance between targeted advertising and privacy can be provided by an intelligent design that provides both. The Privad system that they suggest contains the publishers, advertisers and an intermediate Ad Network/Ad Exchange (or a broker as the paper terms it) as before. Three new components have been added. Firstly, aggregation of user interest is done on the user end by means of a client software. This local client software does all the function previously done by an ad network, and categorizes user browser history into coarse-grained, non-privacy leaking interests. To provide anonymity to the end-user an intermediate entity known as the dealer anonymizes all communication between the user and the broker. In addition, there is a reference monitor located between the client and the dealer which allows privacy advocates to audit client software and ensure that it is following the Privad protocol and not violating any privacy precepts.

[11] https://acceptableads.com/
[12] https://brave.com/

When a user wishes to see an ad, it transmits coarse-grained categories to the broker via the anonymizing dealer. These categories are the superset of a user’s actual interests and the resultant ads are subsequently also a superset of the ads that are actually shown to the user. Once ads are transmitted by the user, they are locally cached by the client and finally loaded inside the webpage. If a user views or clicks such an ad, then this information, along with publisher ID, is conveyed to the broker by the anonymizing proxy in between. This kind of an ad flow ensures that a reasonable amount of revenue may be obtained by the online advertising industry without loss of privacy.

2.6.2 WIT

WIT is a privacy enabling service running as a proxy that simultaneously provides targeted ads to be shown. It relies on the underlying insight behind Targeted Advertising which is that while targeted requires some sort of identification information, the identity of the actual user may not be usually needed. Following this observation, WIT, functioning on a principle similar to NAT, replaces the public cookies of the user with private cookies and furthermore attempts to make sure that user profiles are not uniquely identifiable yet still at the same time convey useful information to the advertising system. It also monitors all leakage of Personally Identifiable Information as well as browsing history. The moment a user's browsing history becomes uniquely identifiable enough for the advertising system to identify the user, a user's cookie is dropped and replaced by a new one. [61]

2.6.3 AdNostic

ADNostic is a private behavioral advertising system that exists as a browser-extension and maintains a local repository of user interest categories based on urls visited. These categories are later used to build a user profile. AdNostic works in conjunction and with support from ad networks. If they notice the installation of AdNostic, instead of making the ad decision themselves, they send back a list of n ads which they think are most appropriate. AdNostic then selects the final ads based on its local user profile history.

Finally, in AdNostic, problem of conveying to the ad-network which particular ad was viewed is solved by using homomorphic encryption.[28]

3. Design of Advention

3.1 Impact of Proxy-Based Circumvention Tools on Advertising

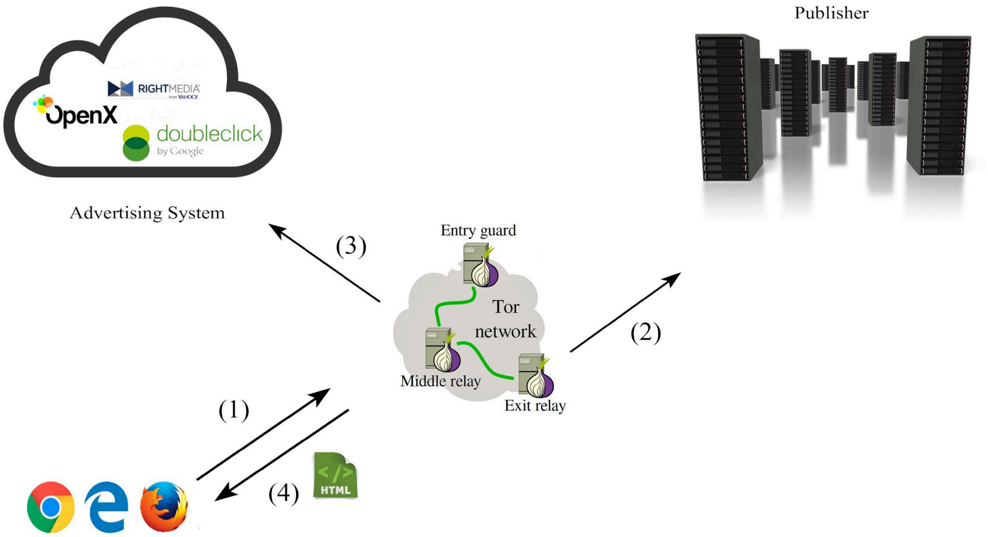


Figure 6a: Ad Retrieval Path While Using Tor

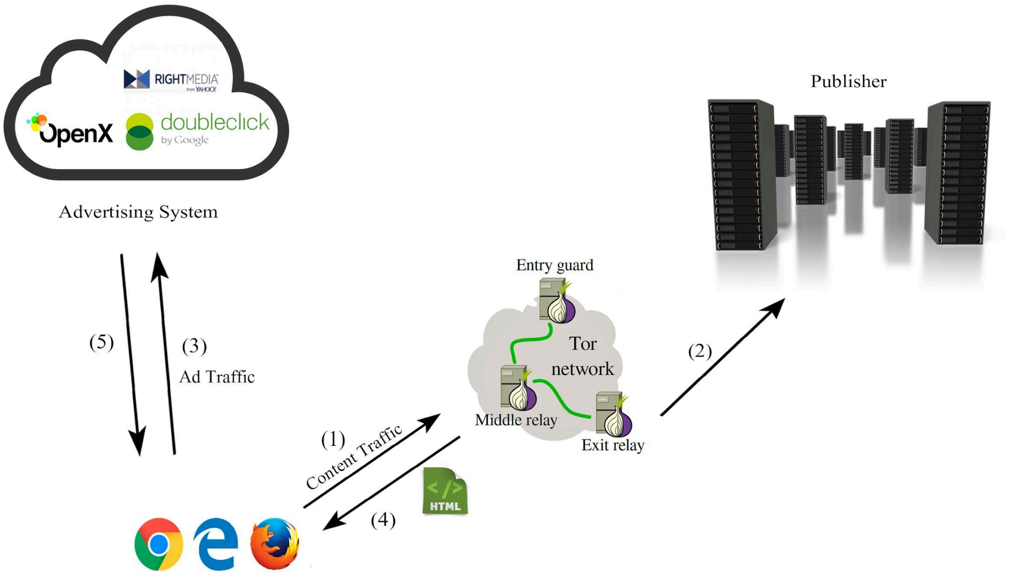


Figure 6b: Ad Retrieval Path While Using Advention

As discussed in the previous section 2.4.4, ad fetching occurs as an Ad Tag, found within the publisher's HTML, containing contextual and geographical information, is sent from the user's end to the Advertising System. Based on the information supplied by this Ad Tag, the Advertising System makes its decision of showing a relevant ad. In the case of proxy-based circumvention tools however, this information originates from the proxy instead of the end-user causing a decrease in overall relevance.

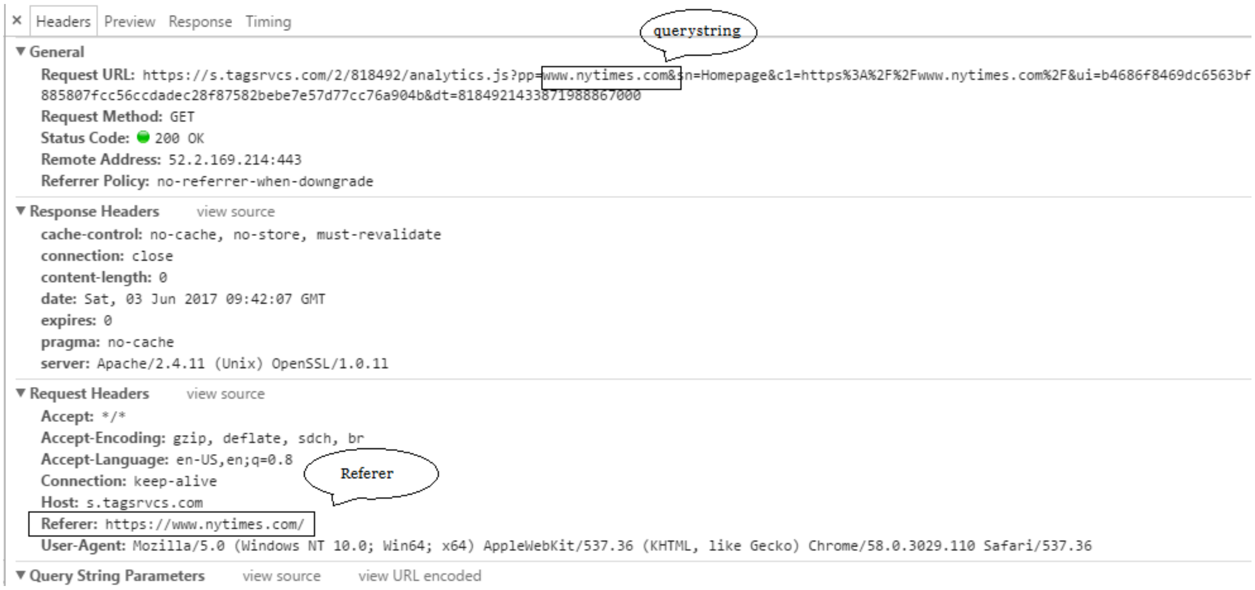
In this thesis, we will consider specifically the impact of using Tor as a circumvention tool. The effect of Tor on relevant ads is illustrated in Fig 6 (a). In step 1, user sends an HTTP request to the publisher as before. This HTTP request however, may now belong to a censored page (if Tor is being used as a circumvention tool), and travels via Tor's multiple-relay anonymity network onwards to the publisher. This affects relevance of ads in two ways:

1. As shown in Step 2 of figure 1, content and ad traffic now uses Tor as an intermediary before arriving at the final publisher destination. As the ad tag travels to the advertising system, it now does so from Tor's Exit Node instead of the actual user. This causes an incorrect inference of the user's original location and hence *geographical ads* shown to the user are targeted to the exit node's location.
2. Since IP address and location inferred by the publisher also now belongs to the Exit Node, the content delivered to the user is specific to exit node's location. Hence, incorrect contextual information in the form of keywords is sent to the advertising system which causes the ad system to show irrelevant *contextual ads.*

3.2 Advention

Advention’s Design

The essential design of Advention as a solution to the problem described above is shown in Figure 6(b). The key insight behind Advention is to split a webpage’s traffic into two. Content Traffic, that is all traffic belonging to servers that supply a publisher’s core content travels via Tor as before. This enables effective circumvention of censored content. Ad Traffic, on the other hand, is now diverted from the Tor path and sent via Direct Path instead. The Advertising System can now infer correct geographical information of the actual user and hence serve relevant geographical ads. Additionally, if exit node’s location is chosen to be in the same location as the user then relatively relevant contextual ads can also be served.



```
▼ General
   Request URL: https://s.tagsrvcs.com/2/818492/analytics.js?pp=www.nytimes.com&sn=Homepage&c1=https%3A%2F%2Fwww.nytimes.com%2F&ui=b4686f8469dc6563bf
   885807fcc56ccdadec28f87582bebe7e57d77cc76a904b&dt=8184921433871988867000
   Request Method: GET
   Status Code: ● 200 OK
   Remote Address: 52.2.169.214:443
   Referrer Policy: no-referrer-when-downgrade
▼ Response Headers     view source
   cache-control: no-cache, no-store, must-revalidate
   connection: close
   content-length: 0
   date: Sat, 03 Jun 2017 09:42:07 GMT
   expires: 0
   pragma: no-cache
   server: Apache/2.4.11 (Unix) OpenSSL/1.0.1l
▼ Request Headers     view source
   Accept: */*
   Accept-Encoding: gzip, deflate, sdch, br
   Accept-Language: en-US,en;q=0.8
   Connection: keep-alive
   Host: s.tagsrvcs.com
   Referer: https://www.nytimes.com/
   User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36
▼ Query String Parameters     view source     view URL encoded
```

Figure 7: URL and Referer Header Leakage

Sending requests via the direct path however has implications on the privacy of the user from the censor. If a request belonging to an ad request goes in plaintext in HTTP, then the domain a user is trying to access may leak out either in the Referer Header or the QueryString parameters of the request (shown in figure 6). A passive censor monitoring network traffic may be able to collect these requests and look for any access to a censored url. If found, then the originating client may be penalized or the censor may take some other legal action against the user. To prevent this, we look at the proportion of leakage that occurs in Advention, and block requests that go out in HTTP. Furthermore, if the traffic is encrypted, the censor may attempt to fingerprint traffic by means of well-known website fingerprinting attacks. To figure out whether this attack is possible, we are also currently looking at any website fingerprinting attacks that may be possible on Advention.

As we've seen before, a key insight behind Advention is to send the ad requests via the direct path instead of the Tor Network. It is well known that trackers and the requests belonging to ad servers slow down a website to a large extent. When these requests go via the Tor network, the latency is expected to increase even further. Since Advention directs these requests via the direct path, page load times are expected to decrease. We use this insight to provide Page Load Times as a user incentive, specifically for those users who do not consider relevant ads as something they place a large importance upon.

A Note on Anonymity:

Advention is not meant to be a system that provides perfect anonymity to the end-user, and therefore while recognizing that we are reducing Tor's anonymity, we present Advention as a system that focuses more on privacy rather than anonymity. While content anonymity from the censor is still maintained, advertising servers now have a transparent view into the source of their ad requests. This may affect anonymity in multiple ways. Not only do the advertising servers are privy to user identity (beyond reasonable degree of plausible deniability afforded by NAT), if pressured upon to do so, these servers may also collude with the censor and violate anonymity. However, this is something we recognize as a limitation of Advention which we do not address at this point.

4. Evaluation

4.1 Methodology Overview

For our experiments, we used Selenium Version 3.0.3 as Browser Automation Framework to automate the functionality of a browser such as Firefox. In addition, we used Firefox Version 52.0.2, and configured it with all relevant Tor's settings, including the extension *HTTPS Everywhere*. *BrowserMob Proxy* was used as a Man In the Middle Proxy to collect HTTP request traces, and the Ad server requests among these were distinguished by a list of pre-known ~2408 Ad Server[13] list. This is a well-known list solely made of adservers as opposed to some other lists that also include entities involved in tracking. Its available as an option in AdBlockPlus and used by users to block ads outside AdBlockPlus as well.

For the Page Load Time experiments, HAR or HTTP Archive format[14] files were collected to obtain time for individual ad resources.

In addition, for our fingerprinting experiment ,we utilized tcpdump to collect packet traces. These traces were parsed in Python to obtain packet timing and Tor cell information.

DataSets collected for our Privacy and AdScape experiments are listed below in Table 1.

DataSet Name	**Number of Websites**	**Type of Data Collected**
DataSet I	7649	Adserver and Publisher Protocols
DataSet II	9341	Referer Headers, Embedded Requests, Adserver and Publisher Protocols

Table 1: Data Sets

[13] http://pgl.yoyo.org/adservers/
[14] https://en.wikipedia.org/wiki/.har

4.2 HTTP/HTTPS AdScape and Privacy in Advention

For these series of experiments, we look into the relative proportion of HTTP and HTTPS Adservers, as well as the proportion of overall requests that are HTTP *and* leak the URL either in their Referer Header or as a querystring parameter embedded inside the request itself. For each embedded subresource on a webpage, if it matched any of the adservers found in our list (of adservers), it was counted as an ad resource, and its protocol is subsequently noted and all the relevant headers collected. Finally we analyze the overall Attack Surface exposed by Advention, and how we can reduce it in Advention.

4.2.1 Threat Model

We consider a passive, local observer, typically the censor, as our adversary. The censor can observe and tap network traffic either at any of the intermediate routers or Internet Exchange Points between the client and Tor's first entry node, or may capture the entry node itself to monitor all incoming network traffic.

4.2.2 Privacy Leakage

Before discussing the results of Privacy Leakage in our experiments, we briefly discuss Mixed-Content Blocking as well as the working of HTTPSEverywhere, both of which are crucial to our experiments.

4.2.2.1 Mixed-Content Blocking

Mixed content on webpages is said to happen if the main domain is loaded over HTTPS but all or some of the embedded resources such as ads, external resources from other website servers or CDNs, etc. are loaded over HTTP. This downgrades the security of a webpage and may cause it to become more vulnerable to man-in-the-middle attacks [53, 54] Mixed content is itself divided into types. One is Passive Mixed content which is request for subresources that are images, audio or video. All of these resources represent passive content that doesn't interact via Javascript or otherwise with the page contents. An MITM attack on these resources can therefore only take the form of active modification. Active Mixed Content, on the other hand, refers to resources that are scripts, flash or iframes that actively interact with the webpage via JavaScript. If such a resource goes out in HTTP, then it could lead to serious security loopholes in the website such as an ability to modify the webpage as well as steal private information such as credit-card numbers.

All modern browsers including Firefox and Chrome, have an implemented policy of blocking all active mixed content loaded inside their browsers.

This is an advantage in the case of Advention, reducing the overall HTTP attack surface as some of the active HTTP requests are blocked. The experiment that follow have their mixed-content blocking turned off. This is in line with the default configuration of Tor [55]

However, given that we have this option, we can turn it on in the final implementation of Advention to considerably reduce our attack surface.

4.2.2.2 HTTPS Everywhere

HTTPS Everywhere is a browser extension supported by Chrome, Firefox and Opera, and developed by a joint effort of the Tor Project and the Electronic Frontier Foundation. It converts all domains, including those belonging to embedded resources, to HTTPS if their servers support the protocol. This is useful if for example a user enters http:// in the browser or if the HTML of a webpage contains the HTTP version of a resource even when the server serving that resource supports HTTP.

In the context of our experiment, HTTPS Everywhere is useful for the following reasons:

1. It converts all embedded ad resources whose servers support HTTPS to HTTP
2. Provides us an interesting way to reduce our attack surface, that is URLs visible to the censor. If HTTPS Everywhere converts an *http* ad server domain to *https,* then that particular domain need not be blocked. This will ensure correct targeting information travels to the advertising system without the censor being able to eavesdrop.

4.2.2.3 Results

The following graphs show the main insights that we gleaned from our DataSets obtained in Table 1

1. **Total Number of HTTP/HTTPS AdServers**

The first graph illustrates the diminishing rate of increase in the number of ad servers present on Top ~8K websites. As can be seen from the graph a very small percentage of the total 2408 adservers are present on the Top Alexa Websites. Based on this, we can tentatively conclude that the number of adservers that in reality serve Top websites lie within a very narrow range. If such a boundary is known, then we need only be concerned about HTTP/HTTPS supporting properties of the adservers that lie within this range, rather than be concerned about the total number of adservers in existence.

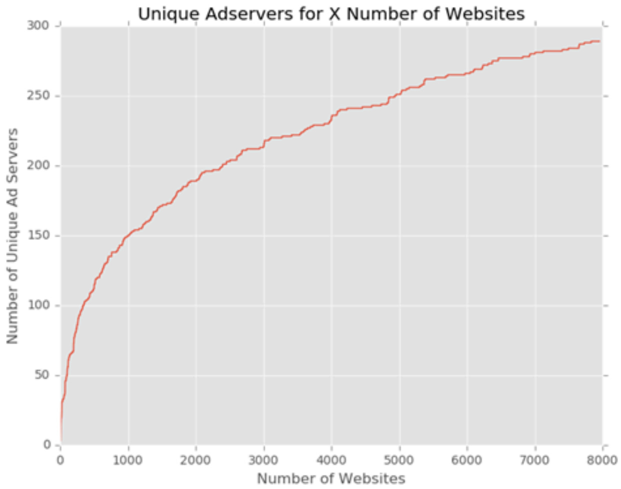


Figure 8: Number of Adservers serving Top ~8K websites. Among the 289 present 191 are HTTPS and remaining are HTTP

2. Proportion of HTTP/HTTPS AdServers

The graph in Figures 9 and 10 show the proportion Top Ranked Adservers present that are HTTP as compared to the ones that are HTTPS. From our results, we can see that about 95% are HTTPS and 5 % are HTTP.

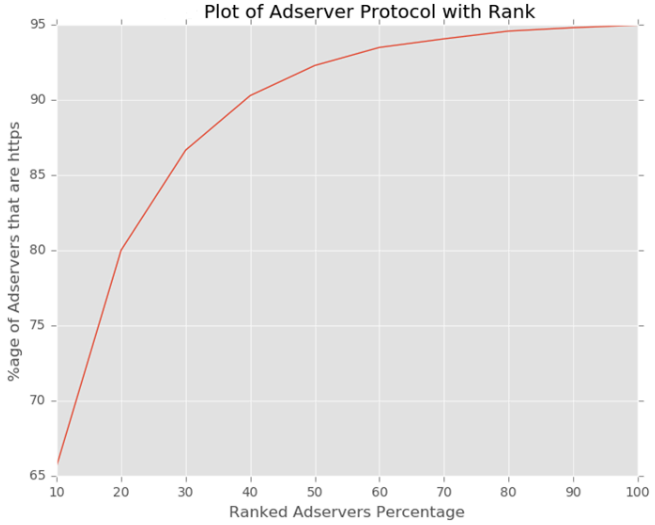


Figure 9: HTTPS Adservers

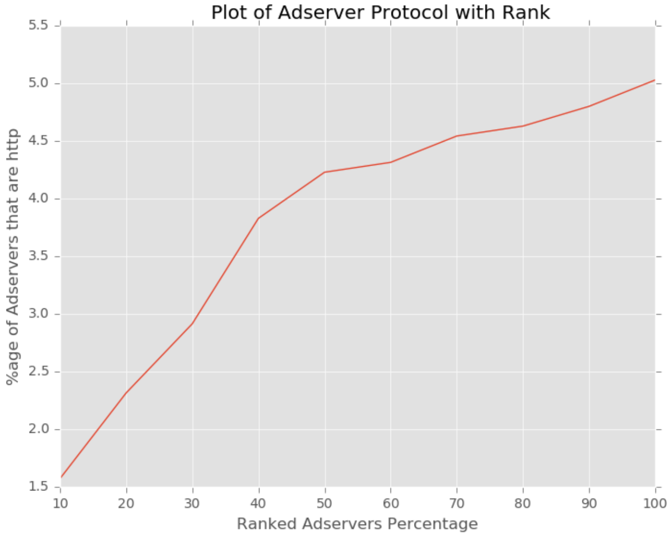


Figure 10: HTTP Adservers

3. Publisher-centric proportion of HTTP/HTTPS Ad Server Requests

The following graph shows the proportion of HTTP and HTTPS requests present in HTTP and HTTPS publishers. Overall, we have 4% HTTP requests, and the remaining are

HTTPS. The insight that we can gain from this, in the context of Advention, is that a very small percentage of requests that are HTTP need to be examined for any sign of leakage.

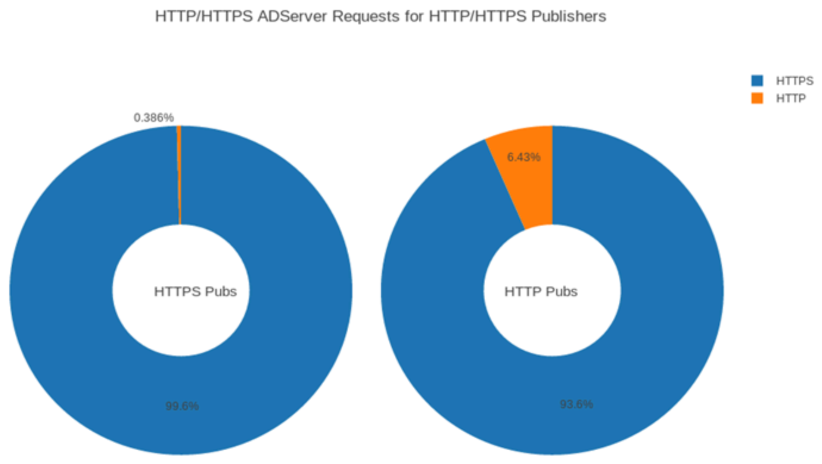


Figure 11: HTTP/HTTPS AdServer Requests for HTTP/HTTPS Publishers

4. URL and Referer Leakage

The graph in figure 4 shows the results from DataSet 2. For HTTPS Publishers about 1032 requests and 1689 Referer Headers leak URL of the main domain. For HTTP publishers however, this number significantly increases to about 2058 Requests and 12722 Referer Headers. This leakage is quite extensive, and needs to be addressed in the final design of Advention.

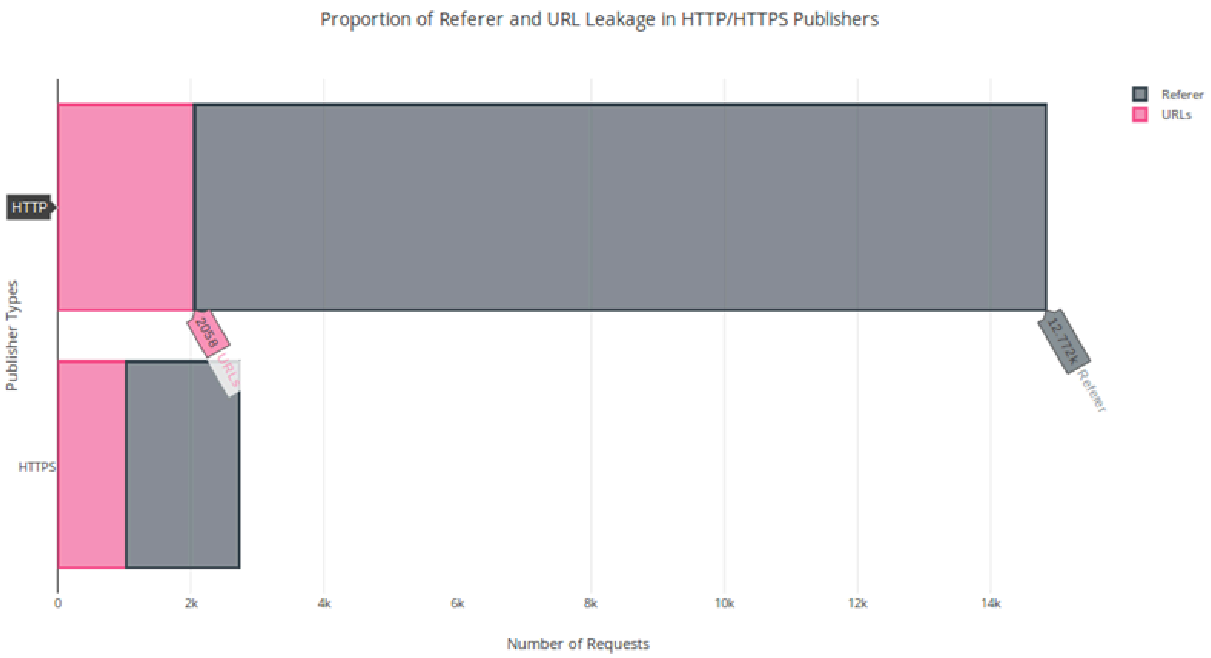


Figure 12: URL and Referer Leakage Proportion

4.2.2.4 Attack Surface

An Analysis of the Attack surface for URL and Referer Leakage is shown in table 2.

Webpage Type	Number of Webpages	URL Leakage	Referer Leakage	Average URL Leakage Per Page	Average Referer Leakage Per Page
HTTP	6297	2058	12772	0.32	2.02
HTTPS	3044	1032	1689	0.33	0.55

Table 2: URL and Referer Leakage

As can be seen from the above table, a maximum of 2 requests per webpage need to be blocked to enable Advention to not leak anything about user-accessed URLs to the censor. The effect of this on the design of Advention is discussed below.

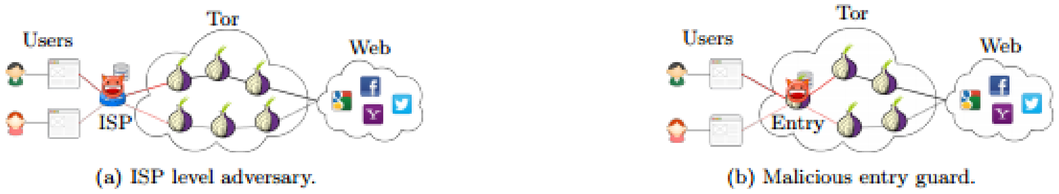
4.2.2.5 Effect on the Design of Advention

To deal with the leakage of URLs inside HTTP requests sent to the adserver, we introduce two modes to Advention:

1. Default Strict Mode: This is the mode where all such HTTP requests are blocked to enable privacy from the censor.
2. User-Dependent Mode: The user can choose to turn the Strict Mode Off and On depending on the laws in the censored country.

The first mode of Advention allows complete privacy from the censor. However, since Referer Header Information about the visited url is also utilized by the ad servers, the impact of such a blocking on the advertising system is currently unknown.

4.2.2.6 Website Fingerprinting Attack



(a) ISP level adversary.

(b) Malicious entry guard.

Figure 2: WF Non-targeted attacks in Tor.

Figure 13: Website Fingerprinting [56]

Website Fingerprinting is an attack where a network adversary may try to identify encrypted traffic by means of supervised classification on network traces using such features as packet timing, size or direction. Previous work [56, 57, 58, 59] has dealt at length with such a type of attack on Tor's traffic whereby an adversary is interested in detecting specific kinds of patterns corresponding to a url within Tor.

Typically, in literature, two types of models exist for such an attack. Open World model is when an adversary tries to identify a fixed set of monitored pages among a set of background unknown traffic. A Closed World model stand in contrast to the Open World model in the sense that the adversary only encounters patterns in user traffic on which it has previously trained its classifiers on.

In the context of Advention, we believe that we need to make sure that the design of Advention does not make this fingerprinting easier. One way this could happen is due to Advention's separation of encrypted content traffic from Ad Traffic. Ad Traffic for the most part represents the dynamic portion of the webpage, so if this is removed from the traffic going via Tor, then there is a possibility that the probability of the censor able to detect a particular URL may increase.

To explore this, we are using an already previously implemented attack by Tao Wang and Ian Goldberg at Waterloo that uses a kNN classifier[15] [58, 59] to classify Tor's encrypted traffic in an Open World Model. A set of 100 monitored pages are used with a background traffic of 9000 Top Alexa pages.

We are currently using *tcpdump* with Python to collect packet timing and direction information for Tor cells belonging to each of the websites above. This experiment is still in its data collection stages so we do not have results for it at the moment.

4.3 Ad Relevance

4.3.1 Results

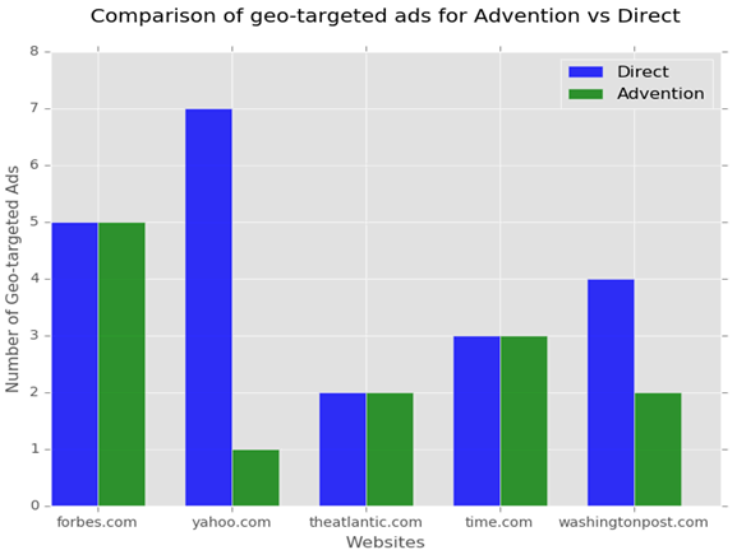


Figure 14: Ad Relevance for Geo-Targeted Ads

[15] https://cs.uwaterloo.ca/~t55wang/wf.html

Figure 14 shows the relevance of geo-targeted ads for Advention. For this result, manual experiments were done for Alexa Top 50 News Sites. The above results are shown for websites with the presence of a reasonable number of ads so as to be able to better quantify relevance. As can be seen in the graph above Advention matches the relevance for Direct Path significantly, matching exactly for three of the total websites.

4.3.2 An Analysis of the Revenue Gained By Advention

Consider Figure 14. For the direct path, total number of geo-targeted ads shown to the user equal 21. Similarly, total number of such ads shown for a user with Advention equal 14. For Tor however, correctly targeted geographical ads are effectively zero.

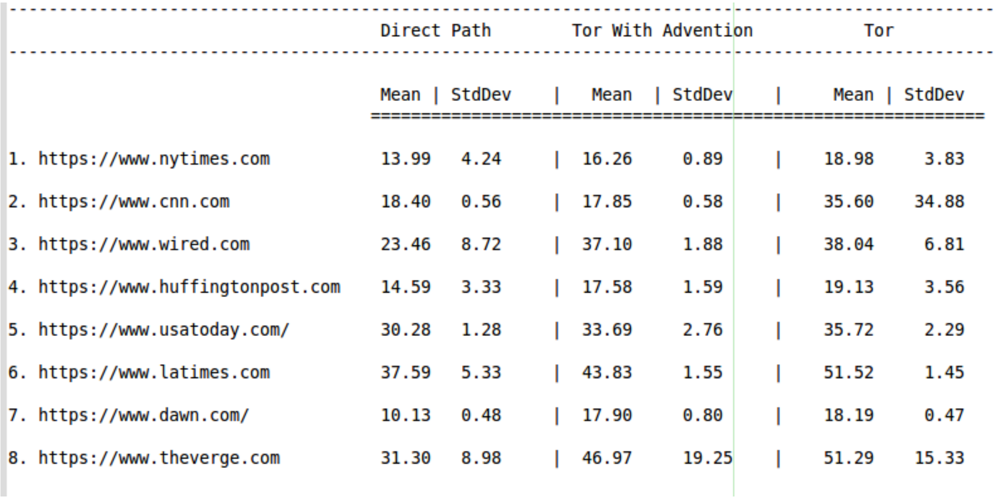
Assuming $X are spent by the advertiser per ad, then the $14X spent for Advention can be expected to contribute to a higher Return On Investment for the Advertiser. This is because the users are now seeing ads that correspond to companies and advertisers that are actually located in their country and hence more relevant.

On the other hand, assuming a fixed Y number of incorrectly targeted geographical ads are shown on Tor. Then the total amount spent by the advertiser $XY will, with a few exceptions, potentially result in a zero ROI, since the ads do not belong to the country the user is in, and hence the user is much less likely to click on them.

4.4 Page Load Times

As shown in the previous sections, a portion of the internet-using population does indeed prefers relevant and targeted ads more than irrelevant ones. However, for the rest of the population, seeing relevant ads may not in itself be a sufficiently tempting incentive towards installing Advention. In the following section, we look at some results for the Page Load Times offered by Advention, to put the metric forth as a user incentive in our system.

As we saw earlier, Advention sends all the ad requests on a webpage via the direct path. Since ad resources are typically expected to consume a sufficient proportion of the total PLT of a webpage, it can be assumed that if these resources are sent via the direct path rather than the multiple-node Tor path, we can improve the total PLT in Advention considerably as compared to that of PLT experienced in Tor. The following results show whether this can happen.



```
-------------------------------------------------------------------------------------------------
                                    Direct Path        Tor With Advention          Tor
-------------------------------------------------------------------------------------------------

                                    Mean | StdDev    |   Mean   | StdDev    |     Mean | StdDev
                                  ============================================================

1. https://www.nytimes.com          13.99   4.24     |  16.26     0.89      |    18.98     3.83

2. https://www.cnn.com              18.40   0.56     |  17.85     0.58      |    35.60    34.88

3. https://www.wired.com            23.46   8.72     |  37.10     1.88      |    38.04     6.81

4. https://www.huffingtonpost.com   14.59   3.33     |  17.58     1.59      |    19.13     3.56

5. https://www.usatoday.com/        30.28   1.28     |  33.69     2.76      |    35.72     2.29

6. https://www.latimes.com          37.59   5.33     |  43.83     1.55      |    51.52     1.45

7. https://www.dawn.com/            10.13   0.48     |  17.90     0.80      |    18.19     0.47

8. https://www.theverge.com         31.30   8.98     |  46.97    19.25      |    51.29    15.33
```

Figure 15: OnLoad PLT Times for 8 websites

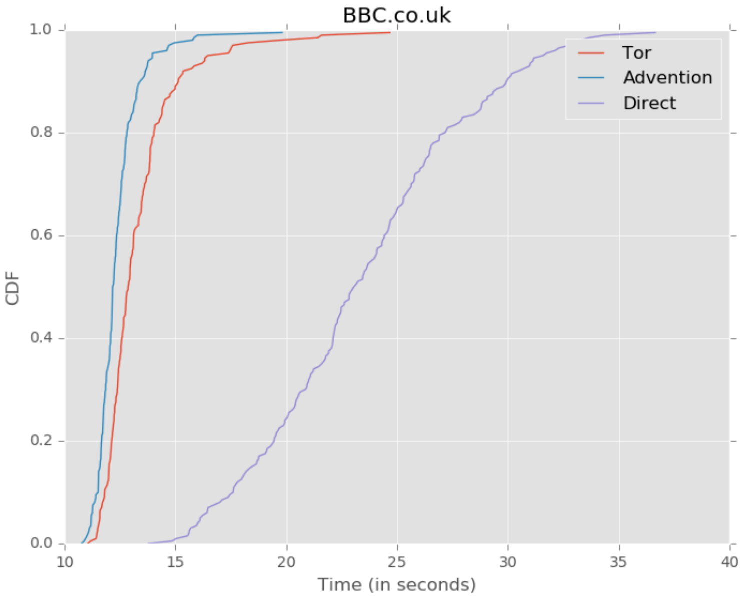


Figure 16a: Comparison of Tor with Advention for bbc.co.uk

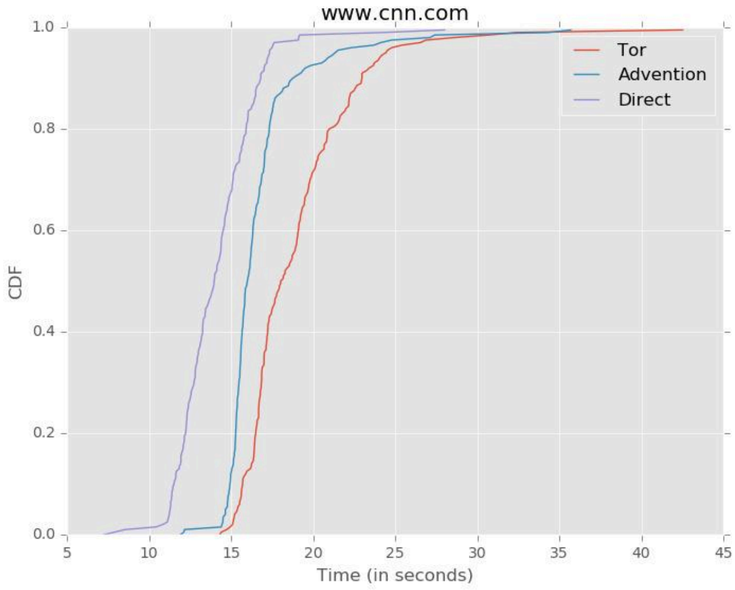


Figure 16b: Comparison of Tor With Advention for cnn.com

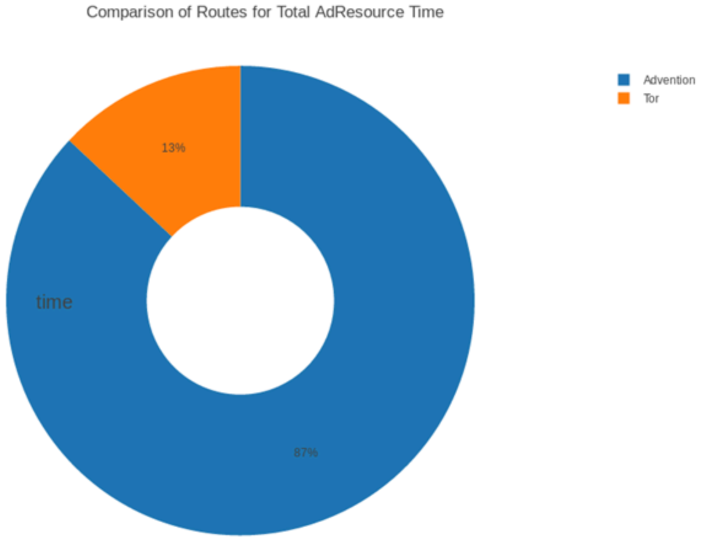


Figure 17: Proportion of Websites giving better Total Accumulated Ad Resource Time

Figure 15 shows improvements seen for Advention over a period of 5 iterations for 8 webpages. The timing for each page were computed from the onload event provided by Firefox's Navigation Timing API[16], which effectively measures the final time seen after all of the

[16] https://developer.mozilla.org/en/docs/Web/API/Navigation_timing_API

resources on a webpage have been loaded. The results show an improvement in mean values for all webpages.

Similarly, figures 16a and 16b, show results for individual websites *bbc.com* and *cnn.com* (chosen for their ad-heavy content). Both of these show an improvement for Advention.

To get a more granular view into the time experienced by the ad resources themselves, we did a separate experiment for 25 webpages. HAR file for each webpage was collected, and the accumulated time for all ad resources computed. The results are shown in Figure 17. For 87% of the webpages, Advention showed better Mean Page Load Times than Tor.

5. Future Work

For future work in Advention, we are considering including proxy-based circumvention tools other than Tor such as Lantern. This will enable Advention to be a more holistic ad-relevant circumvention system. In addition, Advention needs to be built as either an extension or a Cross-Platform Framework, rather than as a plugin. With this, we will be able to give users more granular control over the kinds of ads they wish to see, as well as detailed insights into the kind of privacy leakage that is occurring during their browsing. In the measurement aspect of Advention, we need to analyze the data we've collected for the Fingerprinting attack, as well as bring a more detailed picture of the proportion of the Contextual and Geo-targeted Ads that Advention provides. Finally, it would be interesting to have a more empirical look into the amount of Revenue Gain that Advention provides to the Advertising System and have an Anonymity Model that measures the extent of anonymity.

6. References

[1] Freedom in the World 2016: 2017. *https://freedomhouse.org/sites/default/files/FH_FITW_Report_2016.pdf*. Accessed: 2017- 06- 03.

[2] Aceto, G. and Pescapé, A. 2015. Internet Censorship detection: A survey. *Computer Networks*. 83, (2015), 381-421.

[3] Anonymous. Towards a comprehensive picture of the Great Firewall's DNS censorship. In FOCI. USENIX, 2014.

[4] Roya Ensafi, Philipp Winter, Abdullah Mueen, and Jedidiah R. Crandall. Analyzing the Great Firewall of China over space and time. In PETS. De Gruyter Open, 2015.

[5]Ensafi, R. et al. 2015. Examining How the Great Firewall Discovers Hidden Circumvention Servers. *Proceedings of the 2015 ACM Conference on Internet Measurement Conference - IMC '15*. (2015).

[6] Farnan, O. et al. 2016. Poisoning the Well. *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society - WPES'16*. (2016).

[7] Gebhart, G. and Tadayoshi, K. 2017. Internet Censorship in Thailand: User Practices and Potential Threats. *IEEE European Symposium on Security and Privacy 2017*. (2017).

[8] Khattak, S. et al. 2016. SoK: Making Sense of Censorship Resistance Systems. *Proceedings on Privacy Enhancing Technologies*. 2016, 4 (2016)

[9] Khattak, S. et al. 2014. A Look at the Consequences of Internet Censorship Through an ISP Lens. *Proceedings of the 2014 Conference on Internet Measurement Conference - IMC '14*. (2014).

[10] Nisar, A. et al. 2015. A Case for Marrying Censorship Measurements with Circumvention. *Proceedings of the 14th ACM Workshop on Hot Topics in Networks - HotNets-XIV*. (2015).

[11] Tschantz, M. et al. 2016. SoK: Towards Grounding Censorship Circumvention in Empiricism. *2016 IEEE Symposium on Security and Privacy (SP)*. (2016).

[12] Marczak, B., Weaver, N., Dalek, J., Ensafi, R., Fifield, D., McKune, S., Rey, A., Scott-Railton, J., Deibert, R., and Paxson, V. An analysis of China's "Great Cannon". In 5th USENIX Workshop on Free and Open Communications on the Internet (FOCI 2015) (2015)

[13] David Fifield, Chang Lan, Rod Hynes, Percy Wegmann, and Vern Paxson. Blocking-resistant communication through domain fronting. In PETS. De Gruyter Open, 2015

[14] Chaabane, A. et al. 2014. Censorship in the Wild. *Proceedings of the 2014 Conference on Internet Measurement Conference - IMC '14*. (2014).

[15] S. Aryan, H. Aryan, and J. A. Halderman. Internet Censorship in Iran: A First Look. In FOCI, 2013

[16] Gill, P. et al. 2015. Characterizing Web Censorship Worldwide. *ACM Transactions on the Web*. 9, 1 (2015), 1-29.

[17] Aceto, G. et al. 2015. Monitoring Internet Censorship with UBICA. *Traffic Monitoring and Analysis*. (2015), 143-157.

[18] Burnett, S. and Feamster, N. 2015. Encore. *ACM SIGCOMM Computer Communication Review*. 45, 5 (2015), 653-667.

[19] Karlin, J., Ellard, D., Jackson, A., Jones, C. E., Lauer, G., Makins, D. P., and Strayer, W. T. Decoy Routing: Toward Unblockable Internet Communication. In USENIX Workshop on Free and Open Communications on the Internet (2011).

[20] Anonymous 2012. The collateral damage of internet censorship by DNS injection. *ACM SIGCOMM Computer Communication Review*. 42, 3 (2012), 21.

[21] Internet Advertising Revenue Report: 2016. *https://www.iab.com/insights/iab-internet-advertising-revenue-report-conducted-by-pricewaterhousecoopers-pwc-2/*. Accessed: 2017- 06- 03.

[22] R. Dingledine, N. Mathewson, and P. Syverson. TOR: The second generation onion router. In *Proceedings of the Usenix Security Symposium*, 2004

[23] Detal, G. et al. 2013. Revealing middlebox interference with tracebox. *Proceedings of the 2013 conference on Internet measurement conference - IMC '13*. (2013).

[24] Acar, G. et al. 2014. The Web Never Forgets. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS '14*. (2014).

[25] Englehardt, S. and Narayanan, A. 2016. Online Tracking. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*. (2016).

[26] Mayer, J. and Mitchell, J. 2012. Third-Party Web Tracking: Policy and Technology. *2012 IEEE Symposium on Security and Privacy*. (2012).

[27] Carrascosa, J. et al. 2015. I always feel like somebody's watching me. *Proceedings of the 11th ACM Conference on Emerging Networking Experiments and Technologies - CoNEXT '15*. (2015).

[28] V. Toubiana, H. Nissenbaum, A. Narayanan, S. Barocas, and D. Boneh. Adnostic: Privacy Preserving Targeted Advertising. In Proceedings of the 17th Annual Network and Distributed System Security Symposium, NDSS ’10, February 2010

[29] "Geotargeting - Adsense Help". *Support.google.com*. N.p., 2017. Web. 1 June 2017.

[30] "Target Ads To Geographic Locations - Adwords Help". *Support.google.com*. N.p., 2017. Web. 1 June 2017.

[31] Liu, B. et al. 2013. AdReveal. *Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks - HotNets-XII*. (2013).

[32] Barford, P. et al. 2014. Adscape. *Proceedings of the 23rd international conference on World wide web - WWW '14*. (2014).

[33] Muhammad Ahmad Bashir, Sajjad Arshad, William Robertson, and Christo Wilson. Tracing information flows between ad exchanges using retargeted ads. In 25th USENIX Security Symposium (USENIX Security 16), pages 481–496, Austin, TX, 2016. USENIX Association

[34] The Display LUMAscape Explained: 2017. *http://www.adopsinsider.com/ad-ops-basics/the-display-lumascape-explained/*. Accessed: 2017- 06- 03.

[35] Yuan, S. et al. 2013. Real-time bidding for online advertising. *Proceedings of the Seventh International Workshop on Data Mining for Online Advertising - ADKDD '13*. (2013).

[36] Ad exchange: 2017. *https://en.wikipedia.org/wiki/Ad_exchange*. Accessed: 2017- 06- 03.

[37] Pujol, E. et al. 2015. Annoyed Users. *Proceedings of the 2015 ACM Conference on Internet Measurement Conference - IMC '15*. (2015).

[38] Olejnik, L. et al. 2014. Selling off Privacy at Auction. *Proceedings 2014 Network and Distributed System Security Symposium*. (2014).

[39] Guha, S. et al. 2010. Challenges in measuring online advertising systems. *Proceedings of the 10th annual conference on Internet measurement - IMC '10*. (2010)

[40] Farah Chanchary and Sonia Chiasson. 2015. User Perceptions of Sharing, Advertising, and Tracking. Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)

[41] Leon, P. et al. 2013. What matters to users?. *Proceedings of the Ninth Symposium on Usable Privacy and Security - SOUPS '13*. (2013).

[42] GCreep: Google Engineer Stalked Teens, Spied on Chats (Updated): 2017. *http://gawker.com/5637234/gcreep-google-engineer-stalked-teens-spied-on-chats*. Accessed: 2017- 06- 03.

[43]Ur, B. et al. 2012. Smart, useful, scary, creepy. *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12*. (2012).

[44] McDonald, A. and Cranor, L. 2010. Americans' attitudes about internet behavioral advertising practices. *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society - WPES '10*. (2010)

[45] Farahat, A. and Bailey, M. 2012. How effective is targeted advertising?. *Proceedings of the 21st international conference on World Wide Web - WWW '12*. (2012).

[46] Yan, J. et al. 2009. How much can behavioral targeting help online advertising?. *Proceedings of the 18th international conference on World wide web - WWW '09*. (2009).

[47] Beales, Howard and Eisenach, Jeffrey A., An Empirical Analysis of the Value of Information Sharing in the Market for Online Content (January 2014). Available at SSRN: https://ssrn.com/abstract=2421405 or http://dx.doi.org/10.2139/ssrn.2421405

[48] How WIRED Is Going to Handle Ad Blocking: 2017. *https://www.wired.com/how-wired-is-going-to-handle-ad-blocking/*. Accessed: 2017- 06- 03.

[49] IAB Tech Lab Publisher Ad Blocking Primer: 2017. *https://www.iab.com/iab-tech-lab-publisher-ad-blocking-primer/*. Accessed: 2017- 06- 03.

[50] Storey, G., Reisman, D., Mayer, J., & Narayanan, A. (2017). The Future of Ad Blocking: An Analytical Framework and New Techniques. Retrieved from http://randomwalker.info/publications/ad-blocking-framework-techniques.pdf

[51] Welcome to the Block Party – The Awl: 2017. *https://theawl.com/welcome-to-the-block-party-3acf5e6cdf6d*. Accessed: 2017- 06- 03.

[52] Adblock as a Tragedy of the Commons – David Carroll – Medium: 2017. *https://medium.com/@profcarroll/adblock-as-a-tragedy-of-the-commons-6364d43fbfee*. Accessed: 2017- 06- 03.

[53] What Is Mixed Content? | Web | Google Developers: 2017. *https://developers.google.com/web/fundamentals/security/prevent-mixed-content/what-is-mixed-content*. Accessed: 2017- 06- 03.

[54] Mixed content blocking in Firefox | Firefox Help: 2017. *https://support.mozilla.org/en-US/kb/mixed-content-blocking-firefox*. Accessed: 2017- 06- 03.

[55] SSL, Mixed Content: 2017. *https://tor.stackexchange.com/questions/12585/ssl-mixed-content*. Accessed: 2017- 06- 03.

[56] Juarez, M. et al. 2014. A Critical Evaluation of Website Fingerprinting Attacks. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS '14*. (2014).

[57] Panchenko, A. et al. 2016. Website Fingerprinting at Internet Scale. Ndss. February (2016), 21–24.

[58] Wang, T. and Goldberg, I. 2013. Improved website fingerprinting on Tor. Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society - WPES ’13. (2013), 201–212.

[59] Wang, T. et al. 2014. Effective Attacks and Provable Defenses for Website Fingerprinting. 23rd USENIX Security Symposium (USENIX Security 14). (2014), 143–157.

[60] Guha, S. et al. 2011. Privad: practical privacy in online advertising. NSDI ’11: Proceedings of the 8th USENIX Symposium on Networked Systems Design and Implementation. (2011).

[61] Advertising, B. et al. 2015. Web Identity Translator. Proceedings of the 14th ACM Workshop on Hot Topics in Networks Article No. 3. *HotNets-XIV* (2015).

[62] Fredrikson, M. and Livshits, B. 2011. REPRIV: Re-Imagining Content Personalization and In-Browser Privacy. IEEE Symposium on Security and Privacy. (2011).

[63] Backes, M. et al. 2012. ObliviAd : Provably Secure and Practical Online Behavioral Advertising. IEEE Symposium on Security and Privacy. (2012).

[64] Openx, A. 2010. Ad Networks vs . Ad Exchanges : How They Stack Up. July (2010).