

# Engineering Privacy with Protest: a Case Study of AdNauseam

Daniel C. Howe  
School of Creative Media  
City University, Hong Kong  
Email: daniel@rednoise.org

Helen Nissenbaum  
Cornell Tech  
New York University  
Email: helen.nissenbaum@nyu.edu

*Abstract*—The strategy of obfuscation has been broadly applied—in search, location tracking, private communication, anonymity—and, as such, has been recognized as an important element of the privacy engineer’s toolbox. However there remains a need for clearly articulated case studies describing not only the engineering of obfuscation mechanisms but, further, providing a critical appraisal of obfuscation’s fit for specific socio-technical applications. This is the aim of our paper, which presents our experiences designing, implementing, and distributing AdNauseam, an open-source browser extension that leverages obfuscation to counter tracking by online advertisers.

At its core, AdNauseam works much like a list-based ad-blocker, hiding ads and blocking trackers. However, it provides two additional features which users may choose to enable. First, it collects each ad that it finds in its ‘Vault’, allowing users to interactively explore the ads they have been served, and providing insight into the algorithmic profiles created by advertising networks. Second, AdNauseam simulates clicks on each ad in order to confuse trackers and diminish the value of aggregated tracking data.

A critic might ask: why click? Why not simply hide ads from users and hide users from trackers? The twofold answer reveals what makes AdNauseam distinctive. To begin, it conceptualises privacy as a societal value. Whereas many privacy tools offer solutions only for individual users, AdNauseam is built on the assumption that, often, effective privacy protection must be infused throughout a system. This assumption presents different and interesting engineering challenges. Second, AdNauseam seeks to concurrently achieve the goal of resistance through protest. And since protest frequently involves being vocal, AdNauseam’s core design may seem to conflict with privacy understood as secrecy and concealment. While such tensions and tradeoffs are not uncommon in privacy engineering (for example, in private communications tools, between security properties and usability), the process of designing and building AdNauseam demanded their systematic consideration and resolution.

In this paper we describe the goals of the project, with a focus on the operational definition of privacy that serves as its guide, and the implemented features to which these goals map. We present the engineering approach employed, including the set of tensions we encountered during implementation; how

they were resolved and our methods of evaluation on both technical and social/ethical dimensions. We discuss challenges of adoption and distribution, including the ban of AdNauseam from Google’s Chrome store. These experiences in design, engineering, and distribution inspire concluding thoughts on the broader challenges of embedding privacy tools like AdNauseam within complex socio-technical contexts, sometimes dominated by actors openly resistant to them.

*Index Terms*—engineering, privacy, tracking, advertising, obfuscation, adblocking, surveillance, values-in-design.

## I. INTRODUCTION

The ad blocking wars [43] reflect wide ranging resistance to aspects of the online advertising landscape. AdNauseam is an open-source, cross-platform browser extension, designed to give technical realization to this resistance, not only by hiding ads and blocking malware, but by leveraging obfuscation to confound those seeking to profile users based on their clicks.

### A. Engineering Philosophy

Our approach to the development of AdNauseam builds on prior work that has explicitly taken social values into consideration during tool design [14], [13], [29]. Throughout the planning, development, and testing phases, we have integrated values-oriented concerns as first-order “constraints” in conjunction with more typical engineering concerns such as efficiency, speed, and robustness. Specific instances of values-oriented constraints include *transparency* in interface, function, code, and strategy; *personal autonomy*, where users need not rely on third parties; *social protection of privacy* with distributed/community-oriented action; *minimal resource consumption* (cognitive, bandwidth, client and server processing, etc.); and *usability* (size, configurability, ease-of-use, etc.). Enumerating values-oriented constraints early in the design process enables us to iteratively revisit and refine them in the context of specific technical decisions. Where relevant in the following sections, we discuss ways in which AdNauseam benefited from this values-oriented approach, as well as tensions between design goals that emerged.

Additionally we followed recommendations from the literature on privacy-by-design [24], [27], [25], specifically by including *Functional Requirements Analysis*, *Data Minimization Strategies*, *Multilateral Requirements Analysis*, *Proportionality/Legitimacy Analysis* and *Socially-informed Risk Analysis* in our process.

### B. Iterative Legitimacy Analysis

Before any privacy-by-design activities are embarked upon, a discussion needs to take place with respect to the “legitimacy” of the desired system given its burden on privacy. Legitimacy is described as “the establishment that the application goals would be useful for the intended use population”. This question ought to also be re-iterated once the design of the system is completed, and possibly even after deployment.

[32].

### C. Design Goals and Constraints

The AdNauseam extension is designed to realize three tangible goals for users. The first is to facilitate increased *understanding* of the complex advertising ecosystem—and the profiling on which it operates—by providing users with the ability to explore interactive visualizations of the ads they have been served, as well as in-interface links to learning resources. The second goal is to provide a means of proactive engagement, allowing users an avenue for *expression* of their dissatisfaction with current advertising mechanisms to those running the systems. AdNauseam’s third, and perhaps most obvious goal, is *protection*; protection against malware and “malvertising” (malicious software that leverages advertising mechanisms to gain access to users’ systems)[40], as well as protection against data aggregation and data profiling via clicks on advertisements.

### D. Feature Mapping

Understanding -> Vault, FAQ, Links  
Expression -> Clicking, DNT  
Protection -> Clicking, Blocking Trackers and Malware (< uBlock)

### E. Risk Analysis

Given the three goals we hoped to achieve and the set of features to which these mapped, we set out to identify risks to which users could be exposed to. For each such risk, we considered the degree to which the user might already be exposed when browsing the web using an unmodified browser, the degree of exposure while using AdNauseam. Finally we considered their exposure using existing alternatives, ad-blockers like AdBlock Plus[2] or wide-spectrum blockers like uBlock[20]. The following risks were identified:

- Increased Tracking by Advertisers and other data-gathers
- Personal Data Leakage (via clicks, via hiding/not-blocking, via export)

- Malware/Malvertising

To establish a conservative lower-bound on exposure, we set a constraint on design and implementation decisions that user exposure with AdNauseam must be strictly lower on all dimensions than with our baseline case of browsing with an unmodified browser. Conversely, we hypothesized that the current performance of uBlock would provide an upper bound on risk exposure for the individual user. As AdNauseam must interact, at least minimally, with advertising servers in order to fulfill its functional requirements, it would necessarily expose users to more risk than current state-of-the-art blockers (e.g., uBlock), which do not have such a constraint. Notice that we refer specifically here to “risk for *the individual*”, a distinction we return to below.

### F. Design Tensions

Cryptography researchers and privacy rights organizations tend to favor systems that prevent access to individuals and their information at all cost. The goal is to make access to the individual tamper-proof and to build a technological infrastructure based on non-identifiability of users even vis-a-vis governments. Often, unfortunately, achieving this ambitious goal undermines system usability and drives system cost to a point where marketability and adoption of the solution becomes difficult.

[47]

## II. ARCHITECTURE

### A. Overview

AdNauseam is a free, open-source browser extension (for Chrome, Firefox, and Opera) that blocks online ads while quietly clicking each ad behind the scenes in order to register visits in ad network databases. The goal of the software is to pollute the data gathered by trackers and, by diminishing confidence in this particular indicator, render their efforts to profile less effective. At the same time, the software allows users to engage in a form of expression, by actively disrupting the economic system that drives surreptitious tracking, and by creating mistrust (advertisers generally pay ad networks for clicks) within the advertising system. Additionally, AdNauseam makes the ads it collects available to users to explore at their convenience, via an interactive display designed to facilitate real-time understanding of the advertising system at work. The software is comprised of four modules, each responsible for one of its primary functions: detection, extraction, visualization, and visitation.

### B. Detection

This module is responsible for the analysis and categorization of request made following a user-initiated page view. Such requests are most often made to 3rd-parties which can be first classified according to the type of elements they provide; whether advertisements, analytics, beacons, social-media, or functional widgets. The largest proportion of such requests (40-50%) are made to the first group, on which this module

focuses, which includes ad and ad tracking services [52]. The module is then responsible for differentiating between requests that can be blocked, and those that should be allowed; and in the latter category, between those that yield visual page components and those used only for tracking. In order to efficiently and correctly categorize 3rd-party requests (and the resources they return), we leverage the capabilities of the open-source uBlock-Origin [20] project, described by its authors as a “wide-spectrum blocker”. uBlock is a configurable, list-based “blocker”, that is effective and efficient [52]. Like other blockers, uBlock allows users to specify one or more publicly accessible lists of resources to be blocked and/or allowed. Each list contains a set of syntactic matching rules for the retrieval of resources by the browser. When each request is made, the software first determines whether it should be blocked or allowed. If allowed, and the element is a visual element, a subsequent determination will be made as to whether the element should be visible or hidden. If hidden, the element is downloaded and included in the page’s DOM (the hierarchical, tree-like representation of elements on a webpage), but is made invisible to the user. Both blocking and hiding are specified via rules that may include the serving domain, the type of resource (e.g., images or video), and/or properties of the DOM container (for example, a DIV with a specific id or class). For uBlock, rules are included from widely distributed lists that are updated and maintained by individuals and communities (e.g., “EasyList” [21], or “Peter Lowe’s ad server list [37]”). Additionally, users can augment these public lists with custom rules that they create, either to block or hide new content, or to whitelist a page, site or element. The detection module works incrementally as page elements are loaded (or dynamically generated) and inserted into the DOM. DOM elements marked for hiding are given a CSS class that sets their display to invisible and collapses the surrounding DOM so as not to leave blank space where the item would normally appear. Each element hidden in this way is then passed to the *Extraction* module for further processing.

### C. Extraction

Once a visual element has been detected and hidden, the system must then determine whether it is in fact an advertisement. If so, the extraction module of the system must extract the properties needed for processing by the *Visualization* and *Visitation* modules. These properties include timestamp, size, content-url, target-url, page-detected-on, etc. Depending on configuration, the extraction module may also persist the content of the advertisement itself, rather than relying on the content-url, which may go stale at some time in the future. The module, therefore, must also be capable of resolving and serving locally caching content, whether images, animations, or DOM fragments (e.g., IFRAMEs). Text-only ads, as often found on search engines, present a slightly different challenge, as these are generally served inline along with page content rather than requested from a 3rd-party server. In these non-image cases, several additional fields are aggregated to form the content payload (title, description, tagline) and there is no

content-url linking to external resources. To enable extraction of this data, AdNauseam ships with a custom set of CSS selectors used to parse specific DOM attributes on text-ad sites (Google, Ask, Bing, etc.) Such filters run only on specific domains where text-ads have been previously discovered.

### D. Visualization

In order to facilitate understanding of the data and mechanisms of online advertising systems, AdNauseam provides users with interactive visualizations of their collected ad data. These visualizations provide both high-level displays of aggregate data (see Figure 1), as well as the option to drill-down and inspect individual ads (see Figure 2), including data like the page on which the ad was found, the target URL, the text copy, the viewed-on date, advertising network, and image or video “content”. Additionally, a number of derived functions provide additional metrics (i.e., the total estimated charge to advertising networks for the ads visited on a given page or in a given time-period, as in Figure 3). Ads may be filtered and sorted according to a variety of criteria: by date, topic-category, ad-network, page-category, etc. The current implementation of this module works on JSON data stored in the user’s browser profile, and is implemented in the popular d3 visualization framework which maps data entities to native DOM elements via JavaScript. The visualization module is a distinct contribution of AdNauseam, furthering our goal of increased understanding in two ways: 1) to enhance the user-experience with greater insight into the online advertising landscape; and 2) to enable interested users and researchers to study the ad data, and generate insight into the larger picture beyond momentary interactions. To facilitate these goals, we include mechanisms for importing and exporting ad data sets, which can be loaded and saved as plain-text JSON files directly from the extension. The use of this data, aggregated across users, for further research (with appropriate mechanisms for user consent) is an interesting area for future work. Such capabilities hold the potential to further address the epistemic asymmetries between Web users and advertising networks.

### E. Visitation

This module allows users to simulate a visit to each ad that AdNauseam has collected, with the intention of appearing to the serving website (and the ad-network) as if the user had manually clicked the ad. The current version of the software implements these clicks via AJAX requests, which simulate requests (matching headers, referer, etc.) that the browser would normally send. This provides users with protection against potential malware in ad payloads, as responses are not executed in the browser, and thus JavaScript, Flash, and other client-side scripting mechanisms are not executed. Similarly, AdNauseam does not allow cookies to be set via responses from visits. In making these design choices, we favored user-protection (from potentially dangerous ad payloads) over the appearance of authenticity in AdNauseam clicks, as discussed in the *Evaluation* section below. What are the expected results of visiting some (or all) of users’ collected ads? There are

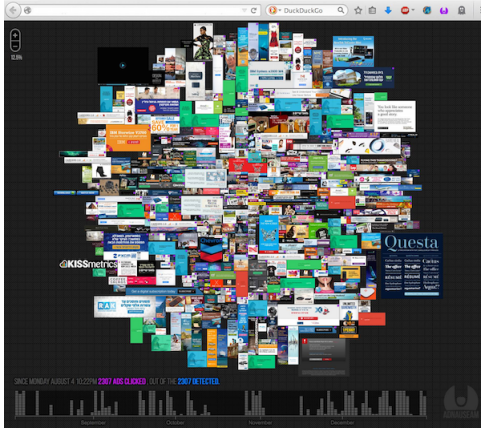


Fig. 1. AdNauseam's AdVault visualization.

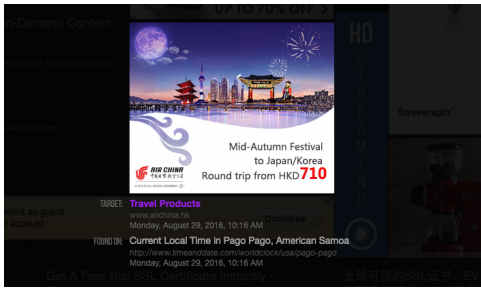


Fig. 2. Inspecting a single ad in the AdVault.

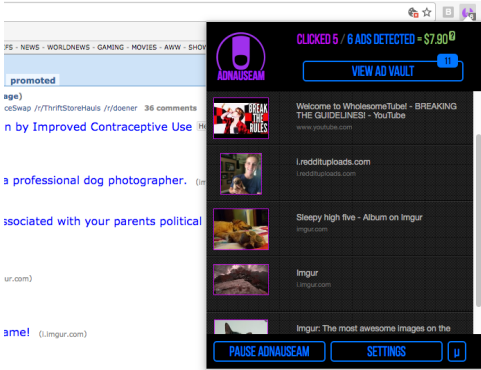


Fig. 3. Estimated cost to advertising networks.

a number of potential outcomes of this behavior, though it is difficult to be certain of any, given the opaque nature of the adversary as discussed below. First off, the data profiles of users stored by advertising networks and data brokers will be polluted, as users' actual interests are hidden. This both protects the user, and to a lesser degree, the larger user community, as aggregate statistics become less accurate. Second, as advertisers must now potentially pay publishers for decoy clicks, a degree of mistrust is introduced into the economic relationship driving the system. This is perhaps

the most compelling argument for this strategy, as it could, given adequate adoption, force advertisers to change their behavior, either by developing new algorithms to filter such clicks, and/or by adopting more privacy-friendly policies. In the former case, where some or even all of such automated clicks are discarded by filtering techniques, then the software has, in a minimal sense, already successfully protected those who use it against tracking. However this strategy has also attracted critics. Below we argue that this approach, although contentious, is both ethically justified and warranted (at least while awaiting more long-term solutions), in order to protect users and safeguard privacy expectations. A more in-depth discussion of the ethical arguments can be found in the *Evaluation* section below.

### III. EVALUATION

Evaluation of AdNauseam was performed iteratively throughout development, often guided by solicited and unsolicited feedback from various constituencies, including users, developers, extension reviewers at Mozilla and the Opera store, and a range of privacy and security advocates. When considering how to evaluate the software, the question of whether AdNauseam in fact “worked” seemed at first to be the most obvious and simple to address. We soon realized, however, that the meaning of this question shifted as users' behaviors, goals, expectations, and perceived risks varied. Evaluating AdNauseam on the basis of feedback from the various constituencies was often a two-part process: first determining users' orientations, and then examining their feedback in light of their respective goals, concerns, and priorities. Additionally, beyond the technical issues with which we grappled, some of the critiques consistently expressed ethical concerns. Thus, we have split the evaluation discussion into two parts. The first focusing on technology, the second on ethics.

#### A. Technical

In evaluation of the obfuscation-based strategies for counter-surveillance, one generally must consider the degree to which the generated noise exhibits a relatively high degree of *indistinguishability* with regards to data the system intends to capture; that is, it must be difficult for an adversary to distinguish injected noise, in order to expunge it, from the data it is attempting to collect. [15], [4]. For example, to evaluate an Private Web Search tool, e.g., TrackMeNot[30], one might extract logs of queries from users, which contain both user queries and noise queries and run best-practice machine-learning (or other) algorithms to attempt to separate the two sets. Although one can never know the actual capabilities of an adversary (especially those, like Google, with vast resources at their disposal), however one can make educated guesses as to the type of attacks that might be performed, whether, in the search case, based on timing attacks, query content, side channel, or other means. For the AdNauseam case, evaluation is not as straightforward. To begin we have a number of distinct cases based on whether the user had installed an

adblocker prior to using AdNauseam, and whether the enabled the ad hiding function of AdNauseam.

must When evaluating AdNauseam’s generated clicks, the first

In the case of clicks, typical evaluation metrics (such as those proposed in X,Y,Z) do not apply, as there is no real data we are trying to disguise with noise data. We are instead creating systemic noise (driving down the value of clicks, degrading the aggregate data obtained from clicks, injecting doubt into the financial transactions that drive the system ). For the majority of ADN users, an adversary goes from seeing  $j$  clicks per time interval where  $j$  ranges from 0-k (depending on whether the user already uses an adblocker), to 1 clicks where 1 dwarfs k. Thus is trivial for an adversary to determine that a user has begun using AdNauseam. We do not try to hide this data. So we can then ask the question, does AdNauseam adequately hide the small number of clicks

1) *Comparative Analysis*: To evaluate the performance of AdNauseam we compare it, on several dimensions (number of 3rd-parties blocked, page-load-times, and memory-use), with other browser extensions designed to protect users from online advertisers and trackers. Each test was first run without any extension, then with AdNauseam, then with Adblock Plus [2], currently the most widely installed adblocking extension, then with uBlock-Origin [20], the open-source content-blocker on which AdNauseam is based, and finally with Privacy Badger [12], discussed below in ‘Related Work’. Tests were performed using each extension’s default settings after resetting the Chrome browser to its install state. After visiting each of the websites in the test set (between 15 and 85 popular URLs, depending on the test), via the Selenium browser automation tool, with each of the extensions, we evaluated their safety (Figure 4) in terms of the number of 3rd parties interacted with, their memory efficiency (Figure 5), and their page-load speed (Figure 6). As can be seen in the graphs below, AdNauseam performed better on all dimensions than using either no blocker, or the highly popular AdBlock Plus. As expected, AdNauseam did not perform as well as uBlock, due to the need to allow visual ad resources to download, rather than blocking them outright. Privacy Badger varied according to the specific test in question, as well as on whether it had been pre-trained before the test.

2) *Indistinguishability vs. Data Leakage*: For obfuscation to function effectively as a means of counter-surveillance, the noise generated by a system must exhibit a relatively high degree of *indistinguishability* with regards to data the system intends to capture; that is, it must be difficult for an adversary to distinguish injected noise, in order to expunge it, from the data it is attempting to collect. [15], [4] Thus, generally speaking, we strive to make AdNauseam visit requests indistinguishable from requests that might be sent by the browser following a manual request from the user. However, there are a number of cases where this goal comes into tension with other aims of the software, specifically that of user protection (both from malware and from data leakage). For example, when crafting a visit request, we must

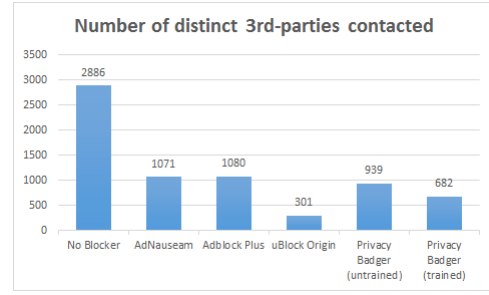


Fig. 4. Number of distinct 3rd-parties contacted.

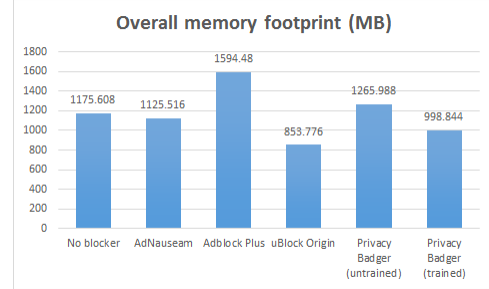


Fig. 5. Overall memory footprint (MB).

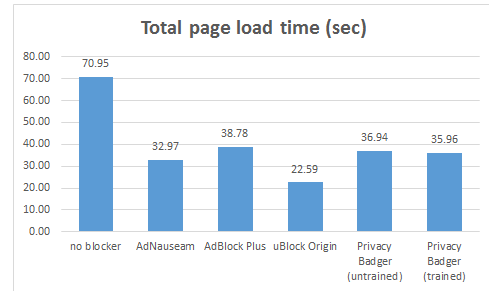


Fig. 6. Total page load time (sec).

decide how accurately to mimic the data that the browser normally sends, specifically regarding user-agent and referer headers, and whether to include the cookies normally sent with the request. If we do so, then our request is indeed more indistinguishable from user requests (assuming the browser is not modified to hide such details), and thus more difficult for an adversary to filter. However, it may also leak information to advertising networks that a user considers private: the URL of the page the ad was found on, and the type of browser, operating system, etc. that they are running. Similarly, we must decide whether to block incoming response cookies from AdNauseam visit requests, whether the DOM of the incoming request should be parsed and executed, and whether client-side scripts should be allowed to run. While we can (and do) provide user configurable settings for all these parameters, we must still, for each case, consider the appropriate default setting by weighing risks to the user against potential gains in

obfuscatory power. For AdNauseam, we have decided on user-configurable settings initialized with whatever default setting maximizes user protection. Thus, by default we block the user-agent header (to deter browser fingerprinting) and the referer (so as not to leak page-view data). Similarly, incoming cookies from visits are blocked – though this should not have any direct effect on indistinguishability – further minimizing the tracking to which users are exposed. Because we use AJAX requests for our visits, a DOM is not constructed from the response and client-side scripts are not executed. One vector of attack to which we are thus open is from an adversary who, upon receiving a click request, sends a preliminary response containing JavaScript code that executes from within the DOM. In this case, if the client-side script never runs, then the click is never executed. We have experimented with solutions that address this issue and thus better support indistinguishability (including executing clicks in sandboxed invisible tabs), but have yet to find a solution that adequately protects users and is cross-platform. For the moment we leave this as future work.

3) *Expression vs. Protection*: We have talked of the expressive and protective capabilities of data obfuscation generally, and of AdNauseam specifically. Abstractly conceived, these two capabilities seem to lie at opposite ends of a spectrum – on the one end, providing protection against surveillance and profiling, on the other end, enabling users to be heard in their expressions of critique, dissent, or protest. On the protective end, the noise generated by a system, as discussed above, should exhibit a high degree of indistinguishability. A tool that is perfectly protective, for which it is never possible to filter noise from data, will often be functionally invisible to an adversary. But if an adversary is literally unaware of injected noise, then the expressive capability of that action is nil (at least when considered from the perspective of the adversary). Conversely, if a system is highly expressive, it will likely be easier for an adversary to filter the noise it generates, thus diminishing the protective capabilities of the obfuscating tool. In the case of ScareMail (see Related Work below), for example, it would not be difficult for an engaged adversary to both detect users of the tool and to filter out the trigger-word-laden signatures generated by it. In practice, however, the relationship between expression and protection is more complex. Filtering might, in some cases, even serve to create temporary spaces free of surveillance. For example, in the case of ScareMail, an adversary filtering (and ignoring) data from ScareMail signatures, might create a zone for messaging not subject to trigger-word monitoring, at least temporarily. A variation on this dynamic may affect AdNauseam users. Were an ad-network capable and willing to react by filtering AdNauseam clicks, users would be in the interesting position of being ignored by the system they are trying to evade. Being snubbed by the advertising system in this way means they will also have achieved the protection they sought from AdNauseam. The case of TrackMeNot [30], a tool that obfuscates users’ interests by automatically sending fake search queries to Web search engines, also embodies subtle interactions between protection and expression. Af-

ter installation of the tool, it would be relatively easy for search engines to detect usage of the extension by referring to the user’s past search history and noticing the sudden spike in the search frequency. Users have thus successfully communicated their discontent, possibly even forcing search engines to address the resulting increased in resource demand. However, even if search engines know that users are employing TrackMeNot, they may not be able to perfectly distinguish between “real” and “fake” queries; that is, there may be a significant percentage of TrackMeNot-generated queries that are indistinguishable from user-generated queries (see [15] for an analysis of this question). As such, TrackMeNot provides expressiveness as well as a degree of protection. An adversary may be aware that a tool is injecting noise into its system, yet be technically, culturally, or otherwise unable or unwilling to filter it. From a tactical perspective, as tool designers leveraging obfuscation, this combination of both protection and expression, is a sweet spot toward which we can aim. To do so however will require more precise definitions of these criteria – how can we more formally evaluate, for example, the expressivity of a system that embeds complex interactions between human and non-human actors? We return to this question in our conclusions below.

## B. Ethical

AdNauseam functions in a complex sociotechnical system, which is driven by political and economic motives hidden from ordinary users. Because most of us do not have the ability to influence or shape this system, interventions like AdNauseam (and others similar to it) provide a means of voicing discontent and achieving a cloak of protection. In the case of AdNauseam, the underlying mechanism is obfuscation – the deliberate and strategic injection of noise into technical systems in order to confound advertising trackers. In previous sections, we discussed known technical challenges and AdNauseam’s attempts to meet them, but we also acknowledged that the limited, one-sided perspective of tool builders poses challenges to evaluation itself, that is, measuring the efficacy of selected mitigations. In spite of this, we managed to evaluate AdNauseam in terms of various technical metrics and compare its performance to other privacy-enhancing tools that address advertising. In this section, we focus on an equally important set of ethical challenges. AdNauseam invites two sources of ethical criticism. The first is concerned with its ad blocking function, the second with its data obfuscation function. Because ad blocking is neither distinctive nor (by design) AdNauseam’s primary aim, and because it has already attracted significant public attention (e.g. the “ad block wars”), we set aside the active debates surrounding the use of ad blockers, resistance from service providers (recently Facebook [33]), and instead focus on whether the obfuscating strategy of clicking all ads is defensible in ethical terms. In adopting the philosophy of data obfuscation AdNauseam seeks to shields users from the inexorable, and inappropriate probes of services and third parties, not by hiding them from those parties but by transforming these probes into counter-probes (metaphorically,

this philosophy resembles a judo master's – absorbing an attacker's energy to strengthen her own defensive counter strike). Choosing obfuscation, however, means taking seriously the ethical critiques that it has drawn, including charges that it is inherently dishonest, wastes resources, and pollutes data repositories, among others. Addressing these issues in *Obfuscation: A User's Guide to Privacy and Protest* [8], the authors charge creators of obfuscating systems to answer two questions: first, whether their aims are laudable; and second, whether alternative approaches exist which might achieve these aims at lesser cost. Because AdNauseam resembles other obfuscating systems discussed, its ethical legitimacy can be established for some of the features it shares with them. Given space limitations of this paper, we therefore focus on AdNauseam's distinctive features and the surrounding context relevant to its ethical evaluation. Regarding Brunton and Nissenbaum's first charge, namely, ensuring that AdNauseam's aims are laudable, we take as a point of departure that ubiquitous online surveillance violates the tenets of a liberal democracy. The troubling nature of this surveillance apparatus is exacerbated by its surreptitious operation, its prevarication, and its resistance to the wishes of a majority of users. Others have eloquently established these claims through systems' analysis, demonstrations and public opinion surveys. [50], [17], [39], [48], [49] Data generated from online surveillance contributes to the creation of valuable, but often highly problematic profiles that fuel the information and behavioral advertising industries with uncertain, potentially negative effects on their subjects (for a good discussion, see [44]). Against this backdrop, we judge the aims of AdNauseam, which include the disruption of this process, to be morally defensible. The second charge to designers of obfuscating systems is whether the methods they have selected impose lower collateral costs than alternative approaches for achieving similar ends. Comparing the purported cost or damage caused by AdNauseam against alternative approaches involves more measurements and even more uncertainties than we are able to tackle here. But, by the same token, this dearth of concrete evidence also poses a challenge to critics who accuse ad blockers – and would similarly accuse AdNauseam – of harming the Web's economy. Even if one holds that the “best” resolution would be societal-level regulation, there has been little progress on this front despite sustained privacy activism. Moreover, the promising beginnings of a multi-stakeholder solution, namely the do-not-track initiative was roundly scuttled by the online advertising industry. (For more information on this, see [8].) As important as seeking credible alternatives, however, is weighing the purported harms or costs of using AdNauseam. Among the latter, the harm of “wasting” network bandwidth or server resources is ironic at best, given the vast amount of bandwidth used by advertisers and trackers, the degradation in performance that results from loading this unwanted content into users' browsers, and the financial toll that such content takes on users paying for fixed data plans. From an ethical perspective, as argued in *Obfuscation*, it is questionable whether the term “waste” is appropriate at all. We think not. For those who deliberately choose to install

and use AdNauseam, it offers utility as a protective shield for privacy and an escape from inappropriate profiling. In our view, these are not worthless endeavors. One of the most aggressive charges leveled at AdNauseam is that it perpetuates “click fraud”. Since obfuscation and fraud both involve forms of lying that disrupt entrenched systems, it is important to evaluate whether the two forms are alike. To carry this out, we consult various definitions: This one, “[Click] fraud occurs when a person, automated script or computer program imitates a legitimate user of a Web browser, clicking on such an ad without having actual interest in the target of the ad's link,” [36] comes close to capturing AdNauseam in its notion of clicking without actual interest, but this definition seemed overly broad in that it commits users to click only on ads in which they are interested, and this seems an unjustifiable restriction on liberty of action. We also argue that if the automated script is performing as an agent of an individual, through that individual's legitimate choice, then the script is a proxy for the legitimate user. John Battelle's account [6], which includes motive and intention, gets closer to the standard meaning of “fraud” in “click fraud,”: the “decidedly black hat” practice of publishers illegitimately gaming paid search advertising by employing robots or low-wage workers to repeatedly click on each AdSense ad on their sites, thereby generating money to be paid by the advertiser to the publisher and to Google.” Motivation is similarly important in this statement: “Click fraud is the subject of some controversy and increasing litigation due to the advertising networks being a key beneficiary of the fraud.” [10] While elements of the above definitions overlap with AdNauseam's mechanized clicking on ads without genuine interest in their targets, machine automation is only incidental to click fraud, and may simply involve “low-wage workers.” More significant is what AdNauseam does not share with click fraud, namely action on behalf of stakeholders that serves either their direct financial interests or those of the developers or users of AdNauseam. In cases of click fraud that have been litigated, this condition, namely the intention to inflate earnings for those who employ them, has been critical. Finally, since we do not agree that visitors to websites have an obligation to click only those ads of genuine interest, we see no fraud in not doing so. We readily admit that one of AdNauseam's primary aims, in clicking all ads, is to disrupt the business models supporting surreptitious surveillance. From this, it does not follow however that AdNauseam (or other similar tools) is responsible for the demise of free content on the Web. First, it is not, as we make clear on the project page, advertising itself that is the primary target of the project, but rather the ubiquitous tracking of users without their consent. Contextual advertising that does not involve tracking can certainly support free content just as it has in the past. Second we should note that Web content is not actually “free” as this argument implies. The development of the Internet has been supported largely by government funding (and thus by taxpayers) since its beginning. In fact, vast infrastructure and energy costs are still born in large part by taxpayers, not to mention the potentially species-



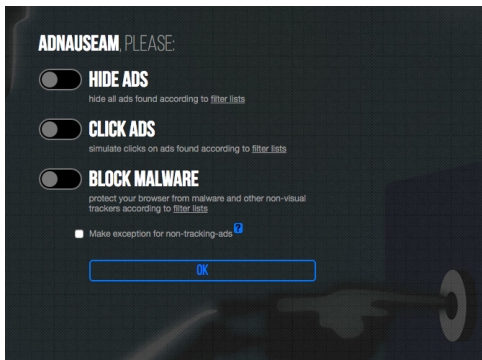


Fig. 7. Opt-in sliders on first install page.

threatening cost to the environment posed by increasing data traffic [26]. Critics may say about users of AdNauseam, as they say about those who use ad blocking tools generally, that they free ride upon those who allow themselves to be tracked. However, in our view this presumes an entitlement on the part of trackers that is indefensible. Those who choose AdNauseam for its anti-profiling functionality may turn the tables on critics here, charging trackers and profilers with destructive exploitation of users [8]. Lastly, in regard to free-riding, we wish to point out that the hiding of ads is an optional element of current versions of AdNauseam, one that users must explicitly opt-in to when they install the software (see Figure 7); AdNauseam’s visitation and visualization modules work equally well whether the user elects to view ads or hide them.

#### IV. RELATED WORK

The strategy of obfuscation has been broadly applied—in search, location tracking, private communication, anonymity—and, as such, has been recognized as an important element of the privacy engineer’s toolbox.

In recent years, researchers have studied advertising networks in a range of ways. Barford et al. [5] presents a large-scale characterization of the advertisement landscape, considering aspects of the advertising system that include new ad arrival rates, advertiser popularity, and number of ads and advertisers per website. Roesner et al. [45] were the first to present a taxonomy of the different trackers (i.e., in-site, cross site, cookie sharing, and social media trackers) inhabiting this landscape. Other studies have explored the newer and subtler tracking mechanisms now in use [1], [18], [51]. Guha et al. [23] first presented the challenges of measuring targeted advertising, including noise due to ad-churn, network effects like load-balancing, and timing effects. Others have focused on the economics of display advertising [16], correlations between ads served and both input data (e.g., users actions) and user profiles [35], [9]. Research has also documented the role of privacy concerns in relation to advertising. Goldfarb and Tucker [17] showed that privacy-focused consumers react negatively to advertisements that are both targeted and obtrusive. A number of laboratory studies and surveys, such as Malheiros et al. [39], Tsai et al. [48], and Turow et al. [50],

have documented and confirmed consumer discomfort with targeted advertising [49].

Several user-level tools have been developed to address elements of advertising surveillance. Two earlier initiatives have attempted to provide ad blocking integrated with some broadly-defined social good. AddArt [3] for Firefox, replaces blocked ads with user-configurable art, while AdLiPo [28], for Google Chrome, replaces ads with constraint-based poetry. These relatively simple tools offer playful alternatives to all-or-nothing ad blockers, while still providing relative awareness of ad content on pages. Lightbeam [42] launched by Mozilla in 2013, provides displays of users’ 3rd party connections when browsing the Web, including advertising networks (though not advertisements themselves). Floodwatch [19], described as “a collective ad-monitoring tool for social good”, is the one user tool of which we are aware that attempts to provide visualizations similar to our own, though it requires communication with a trusted 3rd-party server to do so; something at odds with our design goals. Privacy Badger [12], described as an extension that “blocks spying ads and invisible trackers” warrants mention in that it is the only other tool we have discovered that proposes a minimal avenue of resistance for users. The tool works to block 3rd party-requests, much like traditional adblockers, but rather than operating via pre-compiled block lists, Privacy Badger makes real-time decisions based on content, blocking only those resources (ads included) which are engaged in tracking. Websites honoring Privacy Badger’s “Do Not Track” (DNT) header (this is not the same as the W3C’s do-not-track initiative) are whitelisted and no longer blocked, thus providing an incentive for content-providers to engage in privacy-respecting behavior. The current version of AdNauseam also includes this behavior (both the sending of the DNT header, and the whitelisting of sites who post their conformance to an accepted DNT policy) as a user-configurable option.

Additional projects have been described in [8], including FaceCloak [38], which obfuscates data profiles on the Facebook server, while the “true” profile is visible only to friends also using FaceCloak, BitTorrent Hydra [46], which encourages the proliferation of torrent sites to serve as decoys for anti-BitTorrent efforts, and CacheCloak [41], which sends GPS queries to mobile apps from diverse locations to mask a user’s actual location. There have also been a number of subsequent obfuscation schemes for the search case, five of which are detailed in Balsa et al [4]. Other relevant work, described in [31], has come from the art/tech community. “I Like What I See”, by Steve Klise [34], is a Web browser extension that automatically clicks all “Like” links on Facebook. As with other works employing obfuscation as a strategy, the project has an easily understood narrative. On the project’s Github page Klise writes: “When you visit Facebook, click the thumbs up in the extension bar and start scrolling and liking. Liking and scrolling. Every instance of the word ‘Like’ will be clicked. Don’t worry, Facebook is a fun place full of all of the stuff you like.”

“ScareMail” by Ben Grosser [22] is another Web browser



extension that employs obfuscation in the context of email surveillance. Extending Google’s Gmail, ScareMail adds to every new email’s signature an algorithmically-generated narrative containing NSA search terms. This narrative acts as “a trap for NSA programs like PRISM and XKeyscore, forcing them to look at nonsense”. Grosser describes the project as follows: “ScareMail proposes to disrupt the NSA’s surveillance efforts by making NSA search results useless. Searching is about finding the needles in haystacks. By filling all email with ‘scary’ words, ScareMail thwarts NSA search algorithms by overwhelming them with too many results. If every email contains the word ‘plot’, or ‘facility’, for example, then searching for those words becomes a fruitless exercise. A search that returns everything is a search that returns nothing of use.” Following justifications for the earlier TrackMeNot [30], ScareMail proposes “a model of privacy built on visibility and noise as opposed to one built on encryption and silence” (Grosser). “Invisible”, by Heather Dewey Hagborg [11], extends obfuscation beyond the browser and into the terrestrial world, applying the strategy to the context of genetic privacy, erasing and obfuscating traces of your DNA to frustrate identification. The “Invisiblekit”, available in a limited edition from the New Museum store is a suite of two complementary products: The Erase spray deletes 99.5% of the DNA you leave in public, while the Replace spray cloaks the remaining .5% with DNA noise.

## V. FUTURE WORK

AdNauseam provides individuals with a means expressing a commitment to online privacy without the need to depend on the good will or intervention of 3rd-parties. Although fully functional, AdNauseam is perhaps best considered as a proof of concept for a particular approach to privacy, that is, privacy through obfuscation. As discussed, AdNauseam’s potential lies in its capacity to protect individuals against data profiling, as well as providing, at the same time, a proactive means of expressing one’s views to monolithic and largely uninterested corporations. One key challenge for AdNauseam and similar approaches is a means of providing rigorous, scientific assessments of performance against opaque adversaries; this is to say that we do not (and will not) know precisely the mechanisms that are in place for registering ad clicks, nor precisely the diverse interests of stakeholders in the online advertising ecology. Going forward, a scientific approach to evaluating AdNauseam’s performance, or the performance of any system adopting obfuscation, needs a means of measuring success, namely, evidence that decoy clicks have been registered and have an impact on the resulting profile. Such needs are likely to turn not only on the statistical analysis of signal-to-noise ratios, but also on a practical understanding of how ad-click data is actually mined and used, and the extent to which it influences aspects of user profiles. This would allow future iterations of obfuscation-based tools to be both effective and efficient in the noise they produce. More concrete future work on AdNauseam could take any of several directions. In the near term, we hope to apply obfuscation to the problem of

browser fingerprinting; with AdNauseam issuing, with each request, randomized plausible combinations of the data used for fingerprinting (canvas metrics, system fonts, browser plug-ins, user-agent, etc.). A second area, on which we have already begun preliminary work, concerns the question of how to perform indistinguishable clicks without leaking user data, as discussed above. Though complex, P2P approaches for the sharing of obfuscation data between users is a potentially ripe area of future work for obfuscation in general, and might also help address this issue, with users potentially visiting the ads detected by peers as a means of shielding their data while maximizing the indistinguishability of visits. A central challenge here would be meeting functional criteria while not compromising on the design constraints discussed early in this paper, e.g., transparency and independence from potentially untrustworthy 3rd-parties.

## VI. CONCLUSIONS

We conclude with a philosophical point. AdNauseam operates in an environment that is not only technologically, but also socially complex. Advertising mechanisms operate in a complex, volatile, and competitive marketplace in which user data is a highly valuable resource. For individuals, however, whether or not they view discrete online actions as sensitive, patterns recorded over time potentially open a window into their lives, interests, and ambitions. Thus the vast surveillance infrastructure that online advertising currently represents is not only a source of individual vulnerability, but could also interfere with the rights to free and autonomous inquiry, association, and expression that are essential to a healthy democratic society. Consequently, there remains a tension between individual users, important social and political values, and the economic interests of publishers, advertisers, and advertising networks. In a better world, this tension would be resolved in a transparent, trust-based mutual accommodation of respective interests. Instead, users who are concerned with online privacy find little transparency and few credible assurances in the policies of advertising companies that privacy will ever trump pursuit of direct profit. In light of this, trust-based mutual accommodation of necessity gives way to an adversarial relationship. AdNauseam, a tool for this world and this relationship, gives users a say in shaping the terms of engagement with advertising companies. While we believe AdNauseam represents an important short-term strategy to a particularly problematic set of dynamics, we would prefer a world in which AdNauseam is not needed. Finally, in some of the most revealing exchanges we have had with critics from the advertising industry, we note a palpable sense of indignation, one that appears to stem from the belief that users have an *obligation* to remain legible to their systems, a duty to remain trackable. We see things differently; advertisers and service providers are not by default entitled to the externalities of our online activity. Rather, the average user should be in control of the opacity of their actions, while powerful corporate entities should instead be held to high standards of transparency. Unfortunately this is the opposite of the status

quo. The trackers want us to remain machine-readable, so that they can exploit our most human endeavors (sharing, learning, searching, socializing) to extract value and pursue profit. AdNauseam attempts to represent an alternative position.

## REFERENCES

- [1] Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., & Diaz, C. (2014). The web never forgets: Persistent tracking mechanisms in the wild. In *Proc. of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 674-689). ACM.
- [2] AdBlock Plus. "AdBlock Plus." n.d. <<https://adblockplus.org/>>.
- [3] AddArt. "AddArt." n.d. <<http://add-art.org/>>.
- [4] Balsa, Ero, Troncoso, Carmela, and Diaz, Claudia, 2012. "OB-PWS: Obfuscation-Based Private Web Search". *Proceedings of the 2012 IEEE Symposium on Security and Privacy (SP '12)*. IEEE Computer Society, Washington, DC, USA. 491-505. Print
- [5] Barford, P., Canadi, I., Krushevskaja, D., Ma, Q., & Muthukrishnan, S. (2014). Adscape: Harvesting and analyzing online display ads. In *Proceedings of the 23rd international conference on World wide web* (pp. 597-608). ACM.
- [6] Battelle, J. (2011). The search: How Google and its rivals rewrote the rules of business and transformed our culture. Nicholas Brealey Publishing, Chicago
- [7] Blas, Zach, "Facial Weaponization Suite", n.p. 2011. Web <<http://www.zachblas.info/projects/facial-weaponization-suite>>.
- [8] Brunton, Finn, and Helen Nissenbaum. *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge: MIT Press, 2015.
- [9] Castelluccia, C., Kaafar, M. A., and Tran, M. D. (2012). Betrayed by your ads! In *Privacy Enhancing Technologies* (pp. 1-17). Springer Berlin Heidelberg.
- [10] Click Fraud. (n.d.). In Wikipedia. Retrieved August 1, 2016. <[https://en.wikipedia.org/wiki/Click\\_fraud](https://en.wikipedia.org/wiki/Click_fraud)>
- [11] Dewey-Hagborg, H. "Invisible." 2014. <<http://www.newmuseumstore.org/browse.cfm/invisible/4,6471.html>>.
- [12] Electronic Frontier Foundation. "Privacy Badger." n.d. <<https://www EFF.org/privacybadger>>.
- [13] Flanagan, Mary, Howe, Daniel C. and Nissenbaum, Helen. "Embodying Values in Technology: Theory and Practice." *Information Technology and Moral Philosophy*. Eds. Jeroen van den Hoven and John Weckert. Cambridge: Cambridge University Press, 2008. 322-353.
- [14] Friedman, B., D.C. Howe, and E.W. Felten. (2002) "Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design". In *Proceedings of 35th Annual Hawaii International Conference on System Sciences*, January 2002.
- [15] Gervais, Arthur, Shokri, Reza, Singla, Adish, Capkun, Srdjan and Lenders, Vincent. "Quantifying Web-Search Privacy." *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14)*. New York, NY: ACM, 2014. 966-977. Print.
- [16] Gill, P., Erramilli, V., Chaintreau, A., Krishnamurthy, B., Papagiannaki, K., and Rodriguez, P. (2013). Best paper-Follow the money: understanding economics of online aggregation and advertising. In *Proceedings of the 2013 conference on Internet measurement conference* (pp. 141-148). ACM.
- [17] Goldfarb, A., and Tucker, C. (2011). Shifts in privacy concerns. Available at SSRN 1976321.
- [18] Gomer, R., Mendes Rodrigues, E., Milic-Frayling, N., & Schraefel, M. C. (2013). Network analysis of third party tracking: User exposure to tracking cookies through search. In *Web Intelligence (WI) and Intelligent Agent Technologies (IAT)*, 2013 IEEE/WIC/ACM International Joint Conferences, 1, (pp. 549-556). IEEE.
- [19] Floodwatch. "FloodWatch." n.d. <<https://floodwatch.o-c-r.org/>>.
- [20] Gorhill. "uBlock Origin - An efficient blocker for Chromium and Firefox." 2016. <<https://github.com/gorhill/uBlock>>
- [21] "EasyList." 2016. <<https://easylist.to/>>
- [22] Grosser, Ben. "ScareMail." 2013. Web <<http://bengrosser.com/projects/scaremail>>.
- [23] Guha, S., Cheng, B., and Francis, P. (2010). Challenges in measuring online advertising systems. In *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement* (pp. 81-87). ACM.
- [24] GÄijrses, Seda, Carmela Troncoso, and Claudia Diaz. "Engineering privacy by design." *Computers, Privacy & Data Protection* 14.3 (2011).
- [25] GÄijrses, Seda, Carmela Troncoso, and Claudia Diaz. "Engineering privacy by design reloaded." *Amsterdam Privacy Conference*. 2015.
- [26] Hazas, M., Morley, J., Bates, O., & Friday, A. (2016, June). Are there limits to growth in data traffic?: on time use, data generation and speed. In *Proceedings of the Second Workshop on Computing within Limits* (p. 14). ACM.
- [27] Hoepman, Jaap-Henk. "Privacy design strategies." *IFIP International Information Security Conference*. Springer Berlin Heidelberg, 2014.
- [28] Howe, Daniel C. "AdLiPo" 2014. <<http://rednoise.org/adlipo/>>.
- [29] Howe, Daniel C. and Nissenbaum, Helen. "TrackMeNot: Resisting Surveillance in Web Search." *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*. Eds. Ian Kerr, Carole Lucock and Valerie Steeves. Oxford: Oxford University Press, 2009. pp417-436.
- [30] Howe, Daniel C. and Nissenbaum, Helen. "TrackMeNot" New York University Computer Science Aug. 2006. Software/browser extension <<http://cs.nyu.edu/trackmenot/>>
- [31] Howe, Daniel C. "Surveillance Countermeasures: Expressive Privacy via Obfuscation". In *A Peer-Reviewed Journal About (APRJA)*. Christian Ulrik Andersen and Geoff Cox (eds.) Aarhus: Digital Aesthetics Research Center, Aarhus University, Berlin, 2015. Vol 4, Issue 1.
- [32] Iachello, G, and G. D. Abowd. "Privacy and proportionality: adapting legal evaluation techniques to inform design in ubiquitous computing." *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 2005.
- [33] Johnston, C. "Why Facebook Is Really Blocking the Ad Blockers", In *The New Yorker*. Fri, 12 Aug. 2016
- [34] Klise, Steve. "I Like What I See." 2012-14. Software/browser extension <<https://github.com/sklise/i-like-what-i-see>>.
- [35] Lecuyer, M., Ducoffe, G., Lan, F., Papancea, A., Petsios, T., Spahn, R., ... and Geambasu, R. (2014). "Xray: Enhancing the web's transparency with differential correlation". In *23rd USENIX Security Symposium (USENIX Security 14)*, San Diego, CA.
- [36] Liu, D., Chen, J., and Whinston, A.B. "Current Issues in Keyword Auctions". In *Business Computing*. Eds. Gediminas Adomavicius and Alok Gupta. Bingley: Emerald Group Publishing Limited, 2009. 69-98. Print.
- [37] Lowe, P. "Peter Lowe's Adserver List." 26 August 2016. <<http://pgl.yoyo.org/adserver/>>.
- [38] Luo, W., Xie, Q., and Hengartner, U., "FaceCloak: An Architecture for User Privacy on Social Networking Sites". *Proc. of 2009 IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT-09)*, Vancouver, BC, August 2009, pp. 26-33.
- [39] Malheiros, M., Jennett, C., Patel, S, Brostoff, S. and Sasse, M. A. (2012). "Too close for comfort: A study of the effectiveness and acceptability of rich-media personalized advertising". In *Proceedings of the 2012 ACM annual conference on human factors in computing systems*. (pp. 579-588).
- [40] Mansfield-Devine, S. (editor). "When advertising turns nasty". In *Network Security*, Volume 2015, Issue 11, November 2015, Pages 5-8.
- [41] Meyerowitz, Joseph and Choudhury, Romit Roy. "Hiding stars with fire-works: Location privacy through camouflage." *Proceedings of the 15th annual international conference on Mobile computing and networking*, New York, NY: ACM, 2009.
- [42] Mozilla. "LightBeam." 2016. <https://www.mozilla.org/en-US/lightbeam/>.
- [43] The New York Times. The Ad Blocking Wars. <http://nyti.ms/1Qs20YB>, 2016.
- [44] Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Cambridge: Harvard University Press
- [45] Roesner, F., Kohno, T., and Wetherall, D. (2012). Detecting and defending against third-party tracking on the web. In *Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation* (pp. 12-12). USENIX Association.
- [46] Schulze, H. and Mochalski, K. *Internet Study, 2008/2009, IPOQUE Report*: <[http://www.ipoque.com/resources/internet-studies/internet-study-2008\\_2009](http://www.ipoque.com/resources/internet-studies/internet-study-2008_2009)>.
- [47] Spiekermann, S. and L. F. Cranor. "Engineering privacy." *IEEE Transactions on software engineering* 35.1 (2009): 67-82.
- [48] Tsai, J., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research*, 22(2), (pp. 254-268).
- [49] Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research*, 51(5), (pp. 546-562).

- [50] Turow, J., King, J., Hoofnagle, C. J., Bleakley, A., and Hennessy, M. (2009). Americans reject tailored advertising and three activities that enable it. Available at SSRN 1478214.
- [51] Vallina-Rodriguez, N., Shah, J., Finamore, A., Grunenberger, Y., Pagiannaki, K., Haddadi, H., and Crowcroft, J. (2012). Breaking for commercials: characterizing mobile advertising. In Proceedings of the 2012 ACM conference on Internet measurement conference (pp. 343-356). ACM
- [52] Wills, Craig E., and Doruk C. Uzunoglu. What Ad Blockers Are (and Are Not) Doing.' (2016).