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 adblocker, hiding ads and blocking trackers. However, it provides two additional features. 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 conflict with privacy conceptions based on secrecy and concealment. While such tensions, and tradeoffs that result, 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 tensions we encountered during implementation; how they were resolved and our methods of evaluation on both technical and ethical dimensions. We discuss challenges of distribution, including Google's ban of AdNauseam from its Chrome store. These experiences in design, engineering, and distribution inspire concluding thoughts on the broader challenges of privacy tools which must operate within complex socio-technical contexts, especially those 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 [39] reflect wide ranging resistance to aspects of the online advertising landscape, specifically tracking, malware, annoyance, degradation of browser performance, bandwidth costs. A number of technical systems, utilizing diverse techniques, have addressed these issues in various combinations. AdNauseam, an open-source, cross-platform browser extension, contributes to this growing arsenal not only by hiding ads and blocking malware, but also by leveraging obfuscation to confound those seeking to profile users based on interests revealed through ad clicks. Specifically AdNauseam hides online ads while 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 multiple interactive displays designed to facilitate real-time understanding of the advertising system at work.

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 [16], [14], [27]. Throughout the planning, development, and testing phases, we have integrated values-oriented concerns as first-order "constraints" in conjunction with more typical engineering metrics such as efficiency, speed, and robustness. Specific instances of values-oriented constraints include *visibility and transparency* in interface, function, code, process, 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 have followed a number of strategies from the literature on privacy-by-design [21], [25], [22], [23], [6], specifically by including *Data Minimization Strategies*, *Legitimacy Analysis* and *Socially-informed Risk Analysis* as elements of our design process.

B. Design Goals and Constraints

The AdNauseam extension is designed to realize three tangible goals for users, each of which addresses privacy in the context of online tracking via advertising. The first is to offer *protection*; protection against malware and "malvertising" (malicious software that leverages advertising mechanisms to gain access to users' systems [36]), as well as protection against data aggregation and data profiling via clicks on advertisements. 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. In the case of AdNauseam, this expression has an interventional aspect, as the software actively attempts to disrupt the economic model that drives advertising surveillance. The third goal is to facilitate increased *understanding* of the complex advertising ecosystem—and the profiling on which it operates—by providing users with the ability to view the ads they are served in real-time, and later, to explore interactive visualizations of the ads collected over time. These mechanisms are augmented by in-interface links to additional learning resources.

C. Feature Mapping

The mapping of goals to features (and to the system modules described below) was relatively straightforward in AdNauseam. The goal of *protection* was implemented at a basic level by a) the clicking of collected ads, via the visitation module, and b) the blocking of non-visual trackers and malware, via the detection module. The former attempts to protect the user from data profiling via advertisements, and the latter from non-visual tracking and potential malware. *Expression* was realized through clicks, again via the visitation module, and also through our implementation of the EFF's Do Not Track (DNT) mechanism [12], [13]. With DNT enabled (the default setting), the DNT header is sent with all requests, and ads on DNT sites remain visible. Ads on these DNT pages are also not visited by AdNauseam. The goal of increased *understanding* is realized primarily in the visualization module, specifically via the real-time menu interface, where users can watch as new ads are discovered, then visited; the vault interface (descibed below), and a range of explanatory links embedded throughout AdNauseam's settings pages. Additionally, an in-depth Frequently-Asked-Questions (FAQ) list is linked from multiple locations within the interface, leading to over X carefully answered questions.

D. Data Minimization

Following a growing body of literature on privacy-by-design [21], [25], [22], [23], [6], our design and implementation process followed principles of data minimization, which played out in several ways. First off, AdNauseam was designed to function without ever communicating with a "home server" or sending user-data to any other entity, for any reason. Of course this meant that, as developers, we are unable to access usage patterns and related data, which may have yielded important insights. Yet, we felt that this a) clarified our own position in regard to privacy and data collection, and b) enabled us to sidestep potential problems of data leakage or interception in transit. Similarly, this principle helped us to identify 3 pieces of private information which might potentially be leaked during normal function of the tool, and to then expose these as user options, with defaults that would provide normal users with full protection, while allowing advanced users to opt-in to change these settings for higher performance. These data were all potentially exposed to third-parties (websites and advertising networks) as part of the normal HTTP headers sent with browser requests for ads being clicked; specifically page referer, user-agent, and cookies. From either the referer or cookies, an advertising network present on multiple sites sites (Google, for example, is estimated to have code running on 70% of websites [10]) could potentially recreate large portions of a user's click path, while the user-agent header could be used by malicious trackers attempting to perform browser fingerprinting [40]. Thus all such information was stripped from outgoing requests by default. As discussed below, this choice is not without its negative effects. Choosing to foreground the safety of user data in this way directly impacted AdNauseam's efficacy on other dimensions.

> *The application of data minimization does not necessarily imply anonymity, but may also be achieved by means of concealing information related to identifiable individuals* [21].

Additionally we have applied the principle of data minimization to our ad export feature, which allows users to export their aggregate ad collection (as JSON) in order to sync or migrate between machines, to backup, or to share. From our experiences user-testing this feature, we noted that such exports contained potentially sensitive data, specifically users' click trails (stored as the locations for found ads), possibly over months or even years. When considering how to handle this data we noted that it also existed in the browser's local storage, which could potentially be accessed by a malicious actor. Thus we subsequently implemented encryption for this data, both in memory and in storage, as well as offering the user the option, before each export, to redact all ad locations if desired.

E. Legitimacy Analysis

A critic might ask: why click? Why not simply hide ads from users and hide users from trackers? There are two reasons. First, AdNauseam is inspired by the path-breaking work of Priscilla Regan, who argued in her book, "Legislating Privacy", that beyond its protection of individual interests, privacy serves social ends [44]. In one version of this argument, privacy functions much like a collective good, such as clean air or national defense. As a non-excludable, indivisible collective good, privacy is not doled out individually. Although, in certain situations it may be allocated according to individual needs and preferences, or even willingness to pay, and for these situations, privacy tools have been developed for individuals to use, one-at-a-time. AdNauseam, however, embodies Regan's notion of privacy as a collective good. As such, it fills the need of individual users, but also attempts to infuse privacy throughout a system. This commitment to privacy as a collective good presents different and interesting engineering and evaluation challenges, which, in our view, have not received adequate attention. Thus AdNauseam may stimulate deliberation not only on its particular architecture and features, but may draw attention to the conception of privacy it seeks to promote. A second reason for clicking, as opposed to simply blocking, is that AdNauseam seeks concurrently to achieve the goal of expressive resistance to tracking through protest. And since protest generally involves being vocal, AdNauseam's design seeks to give voice to users. It does not promote the conception of privacy as secrecy or concealment, as many other tools do, by enabling individuals to act stealthily and hide their tracks. Instead, it provides a means for users to express, in plain sight, their dissent by disrupting the dominant model of commercial surveillance.

> *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* [30].

Critics have warned that approaches such as AdNauseam's harm "independent content producers who can no longer support their sites." As this critique touches a broad array of tools, including standard ad blockers, it will take us too far afield to address it in full here. However, setting aside the rejoinder which points out that these sites are enabling surveillance, or more harshly, are "selling out" their visitors, the hope is that loosening the chokehold of tracking over Web and mobile domains, will allow other business models to flourish. Toward this end we have enabled support in AdNauseam for the EFF's Do Not Track mechanism, a machine-verifiable (and potentially legally-binding) assertion on the part of websites that commit to not violating the privacy of users who choose to send the Do Not Track (DNT) header [12], [13]. The basic mechanism of the EFF's DNT Policy is a machine-verifiable text file that domains can post publicly to unilaterally commit to respecting a meaningful version of Do Not Track (DNT), in such a way that other software can tell they have done so. Once posted, the sites are bound (often legally, depending on jurisdiction) to follow the specified practices for themselves and for 3rd party affilitiates. For websites that make this commitment, AdNauseam does not (by default) hide or black their ads and other resources nor do we simulate clicks on their ads.

F. Socially-informed 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 be exposed when browsing the web using an unmodified browser, in comparison to the degree of exposure while using AdNauseam. Finally we considered their exposure using existing alternatives, adblockers like AdBlock Plus [1] or wide-spectrum blockers like uBlock [19]. The following risks were identified:

- Increased tracking by advertisers and other data-gathers
- Personal data Leakage (via clicks, via hiding rather than blocking, via ad 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, the open-source blocker with the best performance metrics, 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 the current state-of-the art blocker (e.g., uBlock), which does not have such a constraint. Notice that we refer specifically here to "'risk for *the individual*', a distinction we return to below. In all cases (see *Comparative Evaluation* below), we were able to verify that the risk to users on each of the dimensions listed above was strictly diminished by using AdNauseam, both in comparison to the no-blocker case, and to the most popular ad-blocker, AdBlock Plus [41].

G. Design Tensions

1) Indistinguishability vs. Data Leakage: For obfuscation to function effectively as a means of counter-surveillance, the noise generated must exhibit a 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 from the data it is attempting to collect. [17], [3] Thus we strive to make AdNauseam visit requests indistinguishable from a those sent for manual requests. However, there are cases where this goal comes into tension with other aims of the software, specifically that of protection (both from malware and from data leakage). For example, when crafting a visit request, we must 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 match these exactly then our request is indeed indistinguishable (assuming the browser is not modified to hide such details), and thus more difficult for an adversary to filter. However, this may also leak information to advertising networks that a user considers private, e.g., the URL of the page the ad was found on, the type of browser, operating system, etc. they are using. Similarly, we must decide whether to block incoming cookies from AdNauseam visits, whether the DOM of incoming request should be parsed and executed, and whether client-side scripts should be allowed to run. While we can provide user configurable settings for all these parameters, we must still, for each case, consider the appropriate defaults by weighing risks to the user against potential gains in obfuscatory power (see *Risk Analysis*). For AdNauseam, we have decided on default setting that maximize 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 visits are implemented via AJAX requests, a DOM is not constructed from the response and client-side scripts are not executed. While protection is maximized here, obfuscatory power may be diminished. For example, one vector of attack we have noted 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 user data and is cross-platform. For the moment we leave this as future work.

> *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 nonidentifiability 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* [46].

2) 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 [28], a tool that obfuscates users' interests by automatically sending fake search queries to Web search engines, also embodies subtle interactions between protection and expression. After 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 [17] 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.

II. Architecture

A. Overview

The AdNauseam 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 requests following a user-initiated page view. Such requests, most often made to 3rd-parties, 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 [50]. This module is reponsible for determining requests that can be blocked, and those that must be allowed; and in the latter category, between those that yield visual page components and those used only for tracking.

In order to categorize 3rd-party requests (and the resources they return), we leverage the capabilities of the open-source uBlock-Origin [19] project, described by its authors as a "wide-spectrum blocker". uBlock is a configurable, list-based "blocker", that is effective and efficient [50]. Like other blockers, uBlock allows users to specify publicly accessible lists of resources to be blocked and/or allowed. Each list contains syntactic matching rules for the retrieval of resources by the browser. For each request, the software first determines whether it should be blocked or allowed, and if it is allowed, whether it 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 made invisible to the user via a content-script. 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). Rules are included from widely distributed lists that are updated and maintained by individuals and communities (e.g, "EasyList" [9], or "Peter Lowe's ad server list [33]"). Additionally, users can augment these lists with custom rules they create, either to block or hide new content, or to whitelist a page, site or element.

Requests marked as blockable are disallowed at the network level, mimicing the behavior of other existing blockers (uBlock, AdBlock Plus, Adblock, Adguard, etc.) which perform blocking on some percentage of requests and hiding on some percentage of the remainder. The only difference for AdNauseam is that a subset of requests which may possibly be blocked in other blockers must be allowed in AdNauseam; specifically those that result in, directly or indirectly, visual advertisements. [1] At the element hiding level, the detection module is invoked incrementally, via content-scripts, as page elements are loaded (or dynamically generated) and inserted into the DOM. Elements marked for hiding are assigned a CSS class that sets their display to invisible, and the surrounding DOM is collapsed so as not to leave blank space on the page. Each hidden element, generally a visual ad, is then passed to the *Extraction* module for further processing.

C. Extraction

Once a visual element has been detected and hidden, the system must 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 must therefore 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 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 such 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 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

[1] Interestingly it is this standard combination of functions—hiding and blocking—that Google claims violates its Terms of Service, a claim discussed below in the *Distribution* section.

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.

E. *Visitation*

This module simulates visit on each collected ad, with the intention of appearing to the serving website (and the ad-network) as if it had been manually clicked. Currently, these clicks are implemented via AJAX, which simulates 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 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 *Design Tensions* section. What are the expected results of visiting some (or all) of users' collected ads? There are a number of potential outcomes of this behavior. 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 individual user (assuming they have clicked or may click some ad in the future) as well as 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 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 protected the user against tracking. However this strategy has also attracted critics. Below we argue that this approach, although contentious, is ethically justified (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.

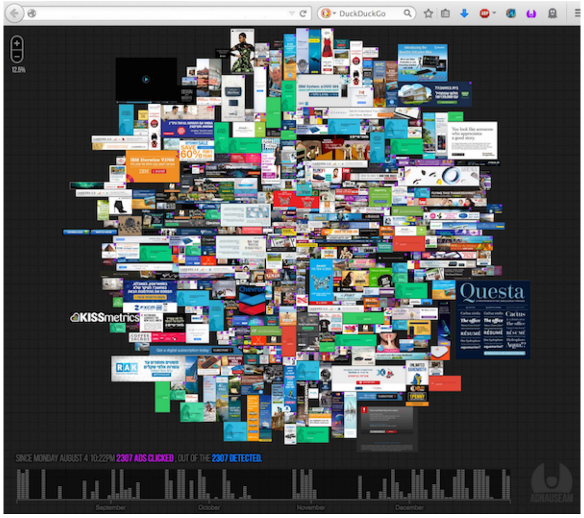
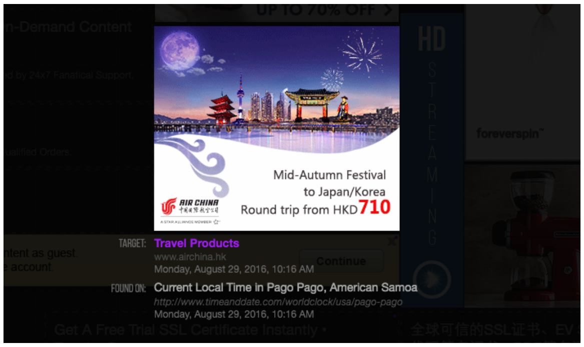

SINCE MONDAY AUGUST 4 10:22PM 2307 ADS CLICKED, OUT OF THE 2307 DETECTED.
September
October
November
December
ADNAUSEAM
Questa
KISSmetrics

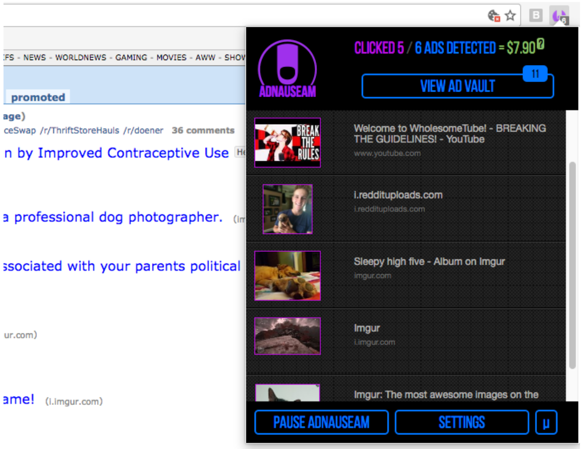
Fig. 1. AdNauseam's AdVault visualization.



TARGET: Travel Products
www.airchina.hk
Monday, August 29, 2016, 10:16 AM

FOUND ON: Current Local Time in Pago Pago, American Samoa
http://www.timeanddate.com/worldclock/usa/pago-pago
Monday, August 29, 2016, 10:16 AM

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



CLICKED 5 / 6 ADS DETECTED = $7.90

Welcome to WholesomeTube! - BREAKING THE GUIDELINES! - YouTube
www.youtube.com

i.reddituploads.com
i.reddituploads.com

Sleepy high five - Album on Imgur
imgur.com

Imgur
i.imgur.com

Imgur: The most awesome images on the

Fig. 3. Estimated cost to advertising networks.

F. *Distribution*

Although not a typical concern in the engineering context, issues surrounding the distribution of AdNauseam highlight a issues we imagine will become only more relevant as corporate players exert a growing influence over the software ecosystem. The prototype for AdNauseam was initially developed as a Firefox-only extension available in the Mozilla's addon store. In our production release, we added Opera and Chrome support and made the extension available in the Opera and Chrome stores respectively. We distributed approxiamtely 50,000 copies of the software over the subsequent 6 months with the majority of downloads coming from Google's Chrome store. On January 1, 2017, we learned that Google had banned AdNauseam from the Chrome store, and further, had begun disallowing users from manually installing or updating AdNauseam, effectively locking them out of their own saved data, all without prior notice or warning.

We wrote to Google requesting the reason for the removal, and they responded that AdNauseam had breached the Web Stores Terms of Service, stating that "An extension should have a single purpose that is clear to users."[2] The purpose of AdNauseam was never obscured however; namely to resist the non-consensual surveillance conducted by advertising networks, of which Google is a prime example. Of course we can understand why Google would prefer users not to install AdNauseam, as it opposes their core business model, but the Web Store's Terms of Service do not (at least thus far) require extensions to endorse Google's business model. Moreover, this is not the justification cited for the software's removal.

Whether or not you are an advocate of obfuscation-based tools, it is disconcerting to know that Google can quietly make a privacy extension, along with saved data and preferences, disappear at any moment, without even a warning. Here we see a counter-surveillance tool that is disabled; will it be a secure chat app, or password manager tomorrow? For developers, who, incidentally, must pay a fee to post items in the Chrome store, this should be cause for concern. Not only can one's software be banned and removed without warning, with thousands of users left in the lurch, but all comments, ratings, reviews, and statistics are deleted as well.

III. Comparative Evaluation

Qualitative 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 considerations, the second on ethics.

A. Technical

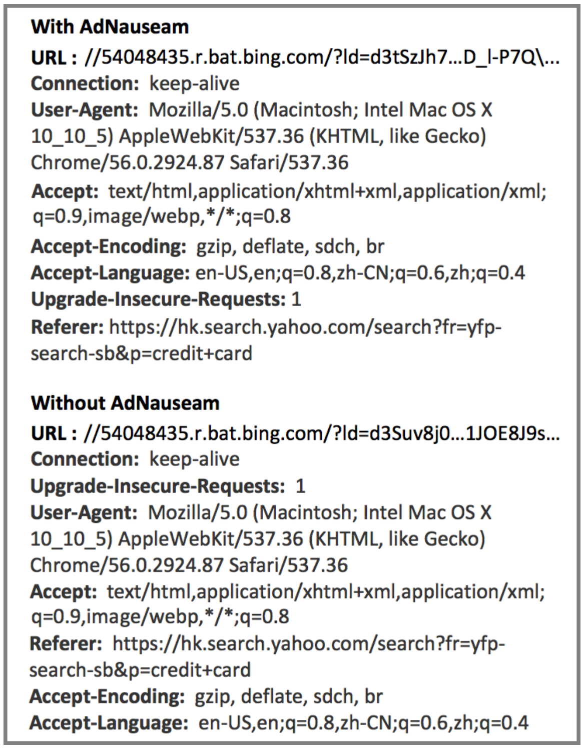
Evaluation of the obfuscation-based strategies for counter-surveillance is often a relatively straight forward challenge. As an example, consider the case of obfuscation in web search. To begin one might extract logs of queries from users, which contain both true queries and software-generated queries and run best-practice machine-learning (or other) algorithms to attempt to separate the two sets. Although one may never know the actual capabilities of an adversary (especially those, like Google, with vast resoures at their disposal), one can make educated guesses as to the type of attacks that might be performed, whether, for the search case, based on timing attacks, query content, side channel, or other means (for specific details of such evaluations in the search case, see [17], [3], [43]). If we find that the adversary can differentiate true queries with a high degree of accuracy, then the generated queries can be easily filtered and, at least from a protection standpoint, the tool has failed[3].

At first glance, evaluating AdNauseam seems similarly straightforward: at what degree of accuracy can an adversary, using state-of-the-art techniques, distinguish user clicks from AdNauseam-generated clicks? However, the question is confounded by the fact that for the majority of users (those who enable the recommended ad hiding function and have disabled whitelisting for DNT sites), there are no true clicks to distinguish. No ads are seen, and thus none are ever clicked. At the same time, due to the frequency of clicks issued, an adversary will be able to readily ascertain that a user has installed AdNauseam. Given this information, we must ask what avenues are open to the adversary, whether technical or otherwise, and given these, what evaluation metrics might be applicable? One option is that all data for the user in question is discarded. From the user's perspective this may be considered a victory, as, at least in terms of clicks, they are no longer being profiled. However, since the data is discarded, there is also no net gain in privacy when considered from a communcal perspective.

But what if the user does not hide all Ads? Here there are two cases we must consider: the user who chooses to disable hiding altogether, and the user who selects a subset of ads to see, whether by whitelisting pages and sites by hand and/or by maintaining the default option to view ads from DNT-respecting sites. The former case, where a user goes through the trouble to install an adblocker, but continues to view all ads, we imagine to be vanishingly small, so we focus on the latter, which consists of 2 sub-cases: the DNT case, and the non-DNT case. As DNT sites have made a binding commitment not to track users (and not to allow their 3rd-parties to track users), protection is not needed, and generated clicks are thus not issued. In the user-whitelisting case, we find the situation that most closely the resembles the case of web search, where some subset of clicks are true and some generated. However the scenario is still different as here ALL

[2] In the one subsequent email we received, a Google representative stated that a single extension should not perform "both blocking and hiding", an assertion that is difficult to accept at face value as nearly all ad blockers (including uBlock, AdBlock Plus, Adblock, Adguard, etc.) also perform blocking and hiding of ads, trackers, and malware, and have not been banned. As of February 17, 2017, it had been over a month month since we have heard back from Google in response to our queries for clarification.

[3] We may still argue that the tool is successful in terms of expresssion, but this is a different concern.



```
With AdNauseam
URL : //54048435.r.bat.bing.com/?ld=d3tSzJh7...D_l-P7Q\...
Connection:  keep-alive
User-Agent:  Mozilla/5.0 (Macintosh; Intel Mac OS X
10_10_5) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/56.0.2924.87 Safari/537.36
Accept:  text/html,application/xhtml+xml,application/xml;
q=0.9,image/webp,*/*;q=0.8
Accept-Encoding:  gzip, deflate, sdch, br
Accept-Language: en-US,en;q=0.8,zh-CN;q=0.6,zh;q=0.4
Upgrade-Insecure-Requests: 1
Referer: https://hk.search.yahoo.com/search?fr=yfp-
search-sb&p=credit+card

Without AdNauseam
URL : //54048435.r.bat.bing.com/?ld=d3Suv8j0...1JOE8J9s...
Connection:  keep-alive
Upgrade-Insecure-Requests:  1
User-Agent:  Mozilla/5.0 (Macintosh; Intel Mac OS X
10_10_5) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/56.0.2924.87 Safari/537.36
Accept:  text/html,application/xhtml+xml,application/xml;
q=0.9,image/webp,*/*;q=0.8
Referer:  https://hk.search.yahoo.com/search?fr=yfp-
search-sb&p=credit+card
Accept-Encoding:  gzip, deflate, sdch, br
Accept-Language:  en-US,en;q=0.8,zh-CN;q=0.6,zh;q=0.4
```

Fig. 4. Header Comparison: AdNauseam click vs. manual request

ads are clicked (the corollary would be if a user could issue all possible queries to a search engine). Thus for an adversary to distinguish true clicks, there must be some element of the click request itself on which to filter (the question of *indistinguishability* discussed above). Thus we must verify that the formatting of our requests, including HTTP headers, cookies and other accompanying data, are identical for true and generated requests (Figure 4 below). As such requests vary by browser, operating system, even by site, and may change over time (with or without action on the part of the adversary), this is not a one-time operation. Instead, we must test these values continuously (in the case of AdNauseam, we leverage an automated testing setup that tests a range of OS/browser/page combinations on a daily basis). Even if requests are indistinguishable, however, and the software is successful in frustrating filtering for passive adversaries, there a still side-channels available to a more determined adversary. One such attack, for which we have not thus far found a solution that adequately protects users from malicious code in the content of requested ads (e.g., malvertising), is presented in the *indistinguishability* section above.

1) Comparative Analysis: To further evaluate the performance of AdNauseam, we compare it, on several dimensions (number of 3rd-parties blocked, page-load-times, and memory-use), to 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 [1], currently the most widely installed adblocking extension, then with uBlock-Origin [19], the open-source content-blocker on which AdNauseam is based, and finally with Privacy Badger [11], 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 5) in terms of the number of 3rd parties interacted with, their memory efficiency (Figure 6), and their page-load speed (Figure 7). 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.

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 have attempted to evaluate AdNauseam on various technical criteria and have compared 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 [31]), and instead focus on whether the obfuscating strategy of clicking 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.

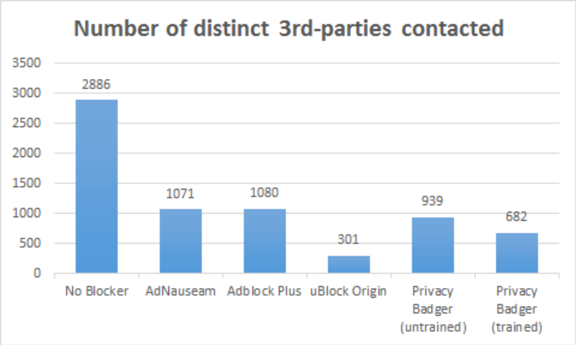


Fig. 5. Number of distinct 3rd-parties contacted.

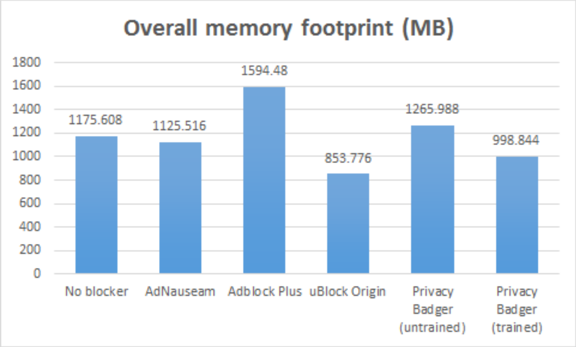


Fig. 6. Overall memory footprint (MB).

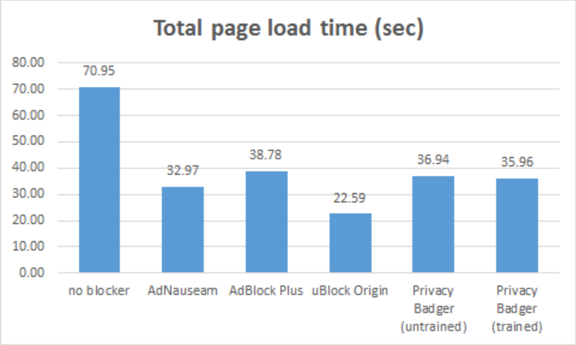


Fig. 7. Total page load time (sec).

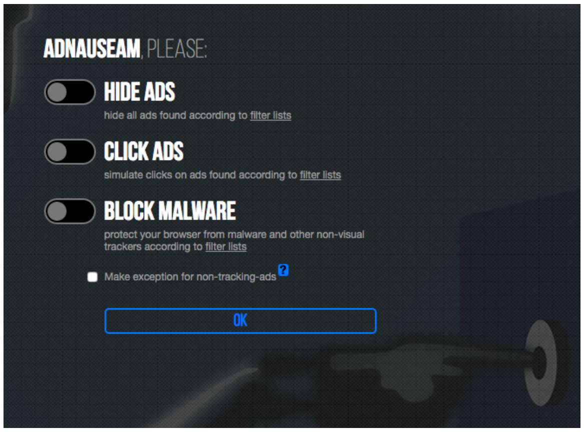
Addressing these issues in *Obfuscation: A User's Guide to Privacy and Protest* [5], the authors charge creators of obfuscating systems to answer two questions: first, whether their aims are laudable; and second, whether alternative approaches exist which might achieve these aims at lesser cost. Because 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. [49], [18], [35], [47], [48] 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 [42]). 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 [5].) 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" [32] 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 [4], 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." [7] While elements of the above definitions ovelrap 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-threatening cost to the environment posed by increasing data traffic [24]. 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 [5]. 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 8); AdNauseam's visitation and visualization modules work equally well whether the user elects to view ads or hide them.



ADNAUSEAM, PLEASE:

HIDE ADS
hide all ads found according to filter lists

CLICK ADS
simulate clicks on ads found according to filter lists

BLOCK MALWARE
protect your browser from malware and other non-visual trackers according to filter lists

□ Make exception for non-tracking-ads ?

Fig. 8. Opt-in sliders on first install page.

IV. Related Work

The strategy of obfuscation has been broadly applied–in search [28], location tracking [37], social networks [34], anonymity [8], [45], etc.–and, as such, has been recognized as an important element of the privacy engineer's toolbox. A range of obfuscation-based projects have been described in [5], including FaceCloak [34], which obfuscates data profiles on the Facebook server, while the "true" profile is visible only to friends also using FaceCloak, BitTorrent Hydra [45], which encourages the proliferation of torrent sites to serve as decoys for anti-BitTorrent efforts, and CacheCloak [37], which sends GPS queries to mobile apps from diverse locations to mask users' actual locations. There have also been a number of obfuscation schemes for the web search case, five of which are detailed in Balsa et al [3].

Other relevant work, described in [29], has come from the art/tech community. "I Like What I See" is a Web browser extension that automatically clicks all "'Like' links on Facebook to obscure user' interests. "ScareMail" [20] is an extension built atop Gmail that append an algorithmically-generated narrative containing NSA search terms to the end of each composed email. "Invisible" extends obfuscation genetic privacy to the terrestrial world via a spray that obfuscating traces of DNA to frustrate identification.

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 [2] replaces blocked ads with user-configurable art, while AdLiPo [26] replaces ads with constraint-based poetry, both offering playful alternatives to all-or-nothing ad blockers, while still providing relative awareness of ad content on pages. Lightbeam [38] launched by Mozilla in 2013, provides displays of users' 3rd party connections when browsing the Web, including advertising networks (though not advertisements themselves). Floodwatch [15], 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 [11], described as an extension that "'blocks spying ads and invisible trackers' warrants mention in that it is the only other tool we have found that proposes a minimal avenue of resistance for users. The tool works to block 3rd party-requests, 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 the EFF's DNT header 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 DNT).

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 better answer 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

AdNauseam operates in an environment that is not only technologically, but socially complex. Advertising mechanisms operate in a complex, volatile, and competitive marketplace in which user data is percieved as 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 represents is not only a source of individual vulnerability, but also interferes with the rights to free and autonomous inquiry, association, and expression that are essential to a healthy democratic society, a distinction we explore above in our conception of privacy as a collective good. Consequently, there remain tensions between individual users, collective social and political values, and the economic interests of publishers and advertisers. 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 from advertisers that privacy will ever trump the pursuit of direct profit. In light of this, trust-based mutual accommodation of necessity gives way to an adversarial relationship, one in which we must, as privacy engineers, leverage all the strategies at our disposal, across the range of contexts in which privacy is threatened. Our success in this endeavor will depend in part on how well we share our experience applying known strategies to new contexts, in concrete and specific detail, according to an evolving set of best practices. This is what we have attempted to do above.

We conclude with a philosophical point. In some of the most revealing exchanges we have had with critics, we note a palpable sense of indignation, one that appears to stem from the belief that human 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, average users should control 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] AdBlock Plus. "AdBlock Plus." n.d. https://adblockplus.org/.

[2] AddArt. "AddArt." n.d. http://add-art.org/.

[3] Balsa, Ero, Carmela Troncoso, and Claudia Diaz. "OB-PWS: Obfuscation-Based Private Web Search." ***IEEE Symposium on Security and Privacy (SP)***. IEEE, 2012.

[4] Battelle, John. ***The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture***. Nicholas Brealey Publishing, 2011.

[5] Brunton, Finn, and Helen Nissenbaum. ***Obfuscation: A User's Guide for Privacy and Protest***. MIT Press, 2015.

[6] Cavoukian, Ann, and Michelle Chibba. “Cognitive Cities, Big Data and Citizen Participation: The Essentials of Privacy and Security”. ***Towards Cognitive Cities***. Springer International Publishing, 2016. 61-82.

[7] Click Fraud. (n.d.). In Wikipedia. Retrieved August 1, 2016. https://en.wikipedia.org/wiki/Click_fraud

[8] Chakravarty, Sambuddho, et al. “Detecting Traffic Snooping in Anonymity Networks Using Decoys.” (2011).

[9] “EasyList.” 2016. https://easylist.to/

[10] Englehardt, Steven, and Arvind Narayanan. “Online Tracking: A 1-million-site Measurement and Analysis.” ***Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security***. ACM, 2016.

[11] Electronic Frontier Foundation. “Privacy Badger.” n.d. https://www.eff.org/privacybadger.

[12] Electronic Frontier Foundation. “Do Not Track.” n.d. https://www.eff.org/issues/do-not-track.

[13] Electronic Frontier Foundation. “A privacy-friendly Do Not Track (DNT) Policy” n.d. https://www.eff.org/dnt-policy.

[14] Flanagan, Mary, Daniel C. Howe, and Helen Nissenbaum. “Embodying Values in Technology: Theory and Practice.” ***Information technology and moral philosophy***. (2008): 322-353.

[15] Floodwatch. “FloodWatch.” n.d. https://floodwatch.o-c-r.org/.

[16] Friedman, Batya, Daniel C. Howe, and Edward Felten. “Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design”. ***Proceedings of the 35th Annual Hawaii International Conference on System Sciences***. IEEE, 2002.

[17] Gervais, Arthur, et al. “Quantifying Web-Search Privacy.” ***Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security***. ACM, 2014.

[18] Goldfarb, Avi, and Catherine Tucker. “Shifts in Privacy Concerns.” ***The American Economic Review*** 102.3 (2012): 349-353.

[19] Gorhill. “uBlock Origin - An efficient blocker for Chromium and Firefox.” 2016. https://github.com/gorhill/uBlock

[20] Grosser, Ben. “ScareMail.” 2013.
Web http://bengrosser.com/projects/scaremail/.

[21] Gürses, Seda, Carmela Troncoso, and Claudia Diaz. “Engineering Privacy by Design.” ***Computers, Privacy & Data Protection*** 14.3 (2011).

[22] Gürses, Seda, Carmela Troncoso, and Claudia Diaz. “Engineering Privacy by Design Reloaded.” ***Amsterdam Privacy Conference***. 2015.

[23] Hansen, Marit, Meiko Jensen, and Martin Rost. “Protection Goals for Privacy Engineering.” ***Security and Privacy Workshops (SPW)***. IEEE, 2015.

[24] Hazas, Mike, et al. “Are there limits to growth in data traffic?: On time use, data generation and speed.” ***Proceedings of the Second Workshop on Computing within Limits***. ACM, 2016.

[25] Hoepman, Jaap-Henk. “Privacy Design Strategies.” ***IFIP International Information Security Conference***. Springer Berlin Heidelberg, 2014.

[26] Howe, Daniel C. “AdLiPo” 2014. http://rednoise.org/adlipo/.

[27] Howe, Daniel C. and Helen Nissenbaum. “TrackMeNot: Resisting Surveillance in Web Search.” ***Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*** 23 (2009): 417-436.

[28] Howe, Daniel C. and Nissenbaum, Helen. “TrackMeNot” New York University Computer Science Aug. 2006. Software/browser extension http://cs.nyu.edu/trackmenot/

[29] Howe, Daniel C. “Surveillance Countermeasures: Expressive Privacy via Obfuscation”. APRJA, A Peer-Reviewed Journal About Datafied Research 4.1 (2015).

[30] Iachello, Giovanni, and Gregory 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.

[31] Johnston, Casey. “Why Facebook Is Really Blocking the Ad Blockers” ***The New Yorker***, 12 Aug. 2016.

[32] Liu, De, Jianqing Chen, and Andrew B. Whinston. “Current Issues in Keyword Auctions”. ***Business Computing (Handbooks in Information Systems, Vol. 3)*** (2009): 69-97.

[33] Lowe, P. “Peter Lowe’s Adserver List.” 26 August 2016. http://pgl.yoyo.org/adservers/.

[34] Luo, Wanying, Qi Xie, and Urs Hengartner. “FaceCloak: An Architecture for User Privacy on Social Networking Sites” ***International Conference on Computational Science and Engineering***, 2009.

[35] Malheiros, Miguel, et al.“Too close for comfort: A study of the effectiveness and acceptability of rich-media personalized advertising”. ***Proceedings of the SIGCHI conference on human factors in computing systems***. ACM, 2012. (pp. 579–588).

[36] Mansfield-Devine, Steve. “When advertising turns nasty”. ***Network Security*** 2015.11 (2015): 5-8.

[37] Meyerowitz, Joseph and Romit Roy Choudhury. “Hiding stars with fireworks: Location privacy through camouflage.” ***Proceedings of the 15th annual international conference on Mobile computing and networking***. ACM, 2009.

[38] Mozilla. “LightBeam.” 2016. https://www.mozilla.org/en-US/lightbeam/.

[39] Murphy, Kate. “The Ad Blocking Wars.” ***The New York Times***, 20 Feb. 2016.

[40] Nikiforakis, Nick, et al. “Cookieless monster: Exploring the ecosystem of web-based device fingerprinting.” ***IEEE symposium on Security and privacy (SP)***. IEEE, 2013.

[41] PageFair, Adobe “The cost of ad blocking–PageFair and Adobe 2015 Ad Blocking Report.” (2015)

[42] Pasquale, Frank. ***The black box society: The secret algorithms that control money and information.*** Harvard University Press, 2015.

[43] Peddinti, Sai Teja, and Nitesh Saxena. “On the Privacy of Web Search Based on Query Obfuscation: A Case Study of TrackMeNot.” ***International Symposium on Privacy Enhancing Technologies Symposium***. Springer Berlin Heidelberg, 2010.

[44] Regan, Priscilla M. ***Legislating privacy: Technology, social values, and public policy.*** Univ of North Carolina Press, 1995.

[45] Schulze, Hendrik, and Klaus Mochalski. “Internet Study 2008/2009.” ***Ipoque Report*** 37 (2009): 351-362.

[46] Spiekermann, Sarah, and Lorrie Faith Cranor. “Engineering Privacy.” ***IEEE Transactions on software engineering*** 35.1 (2009): 67-82.

[47] Tsai, Janice Y., et al. “The effect of online privacy information on purchasing behavior: An experimental study.” ***Information Systems Research*** 22.2 (2011): 254-268.

[48] Tucker, Catherine E. “Social networks, personalized advertising, and privacy controls.” ***Journal of Marketing Research*** 51.5 (2014): 546-562.

[49] Turow, Joseph, et al. “Americans reject tailored advertising and three activities that enable it.” (2009).

[50] Wills, Craig E., and Doruk C. Uzunoglu. “What Ad Blockers Are (and Are Not) Doing." ***Fourth IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)***. IEEE, 2016.