



ILLUSTRATION CREDIT: MUSHON ZER-AVIV/USAF

**The Big Story: Opinion**

---

# **We tested a tool to confuse Google's ad network. It works and you should use it.**

Current privacy laws don't shield people from the pervasive surveillance of Big Tech. Guerrilla tactics are all we've got.

We've all been there by now: surfing the web and bumping into ads with an uncanny flavor. How did they know I was thinking about joining a gym? Or changing careers? Or that I need a loan? You might wonder if Google can read your mind. Google even boasts that it knows you better than you know yourself.

Google can't read your mind, of course. But it can read your search history. It tracks a lot of your web browsing, too. Google has an enormous amount of data about its users, and it uses that data to make an unimaginable amount of money from advertising: over \$120 billion a year. The company runs a vast profiling machine, fitting people into categories that say who they are, what they're worth, and how they're expected to act. Google isn't just organizing the world's information; it's sorting the world's populations.

Many of the digital devices and platforms people use every day are built to make users transparent to the companies who want to predict, influence, and evaluate user behavior. This surveillance advertising has major social costs. Just for starters: it erodes privacy, perpetuates forms of discrimination, and siphons money away from the public-interest journalism that democracies need to survive. Lawmakers have not acted decisively to mitigate these costs.

Some activists, frustrated by the inability of regulators to effectively constrain Google's actions, have taken matters into their own hands. Back in 2014, Daniel Howe, Mushon Zer-Aviv, and Helen Nissenbaum released a browser extension called AdNauseam that automatically clicks on web ads to interfere with behavioral tracking and profiling. Nissenbaum heads a research group at Cornell Tech, which I'm a part of.

AdNauseam is a tool of obfuscation. Obfuscation tactics are a sort of guerrilla warfare approach to the lack of privacy protections. Since it's not possible to hide from Google's surveillance, these tactics introduce inaccurate or excessive information to confuse and ultimately sabotage it.

This isn't a new idea. As Nissenbaum wrote with Finn Brunton in a 2019 essay, "We are surrounded by examples of obfuscation that we do not yet think of under that name." It can be something as simple as adding extra items to a shopping cart at the pharmacy to distract from something that might bring unwanted judgement. The Tor browser, which aggregates users' web traffic so that no individual stands out, is perhaps one of the most successful examples of systematic obfuscation.

AdNauseam is like conventional ad-blocking software, but with an extra layer. Instead of just removing ads when the user browses a website, it also automatically clicks on them. By making it appear as if the user is interested in everything, AdNauseam makes it hard for observers to construct a profile of that person. It's like jamming radar by flooding it with false signals. And it's adjustable. Users can choose to trust privacy-respecting advertisers while jamming others. They can also choose whether to automatically click on all the ads on a given website or only some percentage of them.

Google, unsurprisingly, does not like AdNauseam. In 2017, it banned the extension from its Chrome Web Store. After Nissenbaum gave a lecture on AdNauseam in

2019 at the University of California, Berkeley, skeptics in the crowd, including Google employees, dismissed her effort. Google’s algorithms would, they said, easily detect and reject the illegitimate clicks—AdNauseam would be no match for Google’s sophisticated defenses.

Nissenbaum took this as a challenge. She began a research effort, which I later joined, to test whether AdNauseam works as designed.

We would publish a website and buy ads on the same site on a “cost-per-click” basis—meaning the advertiser pays each time a user clicks on the ad—so we could see whether the clicks generated by AdNauseam were credited to the publisher and billed to the advertiser.

Our testing established that AdNauseam does indeed work, most of the time. But as the experiment developed, it became about more than settling this narrow question. We wanted to try to understand what’s going on inside the black box of Google’s incredibly lucrative advertising sales platforms in a way that nobody else outside the company had ever done.

**We wanted to try to understand what’s going on inside the black box of Google’s incredibly lucrative advertising sales platforms in a way that nobody else outside the company had ever done.**

---

The first step in the experiment involved setting up a website and an AdSense account. Google AdSense is a sales service for small publishers who don’t have the wherewithal to attract advertisers on their own. For a 32% commission, Google handles the whole process of monetizing a website’s traffic: it sells the ads, counts impressions and clicks, collects and makes payments, and keeps a lookout for fraud. If the skeptics at Nissenbaum’s talk were right, we reasoned, AdSense should smell something fishy with AdNauseam clicks and toss them back overboard.

Next, we created a campaign to advertise on the site using Google Ads, the service that buys inventory for advertisers. Google Ads is to advertisers what AdSense is to publishers. Small advertisers tell Google what sorts of people they’d like to reach and how much they’re willing to pay, and then Google finds those people as they browse a range of sites. In this case, the campaign was set up to run only on our site and to outbid any competing advertisers. We set it up this way because we wanted to be careful not to profit from it or draw unknowing bystanders into our experiment.

Positioned now on both sides of an advertising transaction, we were ready to observe the life cycle of an ad click from end to end. We invited individual volunteers to download AdNauseam and visit our site. Soon we had recorded a few dozen successful AdNauseam clicks—billed to our team’s advertiser account and credited to the publisher account. AdNauseam was working.

But this only proved that Google did not discard the *very first* click on an ad generated by a *brand new* AdNauseam user recruited specifically for the experiment. To silence the skeptics, we needed to test whether Google would learn to recognize suspicious clicking over time.

So we ran the experiment with people who had already been using AdNauseam for some time. To anyone watching for very long, these users stick out like a sore thumb, because with AdNauseam’s default settings they appear to be clicking on 100% of



the ads they see. Users can adjust the click rate, but even at 10%, they'd be way outside the norm; most people click display ads only a fraction of 1% of the time. This test, then, was designed to check if Google would disregard AdNauseam clicks from a browser with a long-standing record of astronomical click rates. If Google's machine learning systems are so clever, they should have no trouble with that task.



An image of the AdNauseam "ad vault" collected by the automated Selenium browser.

ILLUSTRATION CREDIT: MUSHON ZER-AVIV

We tested this in two ways.

First, with people: we recruited long-standing AdNauseam users to go to our website. We also invited new AdNauseam users to use the clicking software for a week in the course of their normal web browsing, in order to establish a history, and then to participate in the test.

Second, with software: we conducted an automated test using a software tool called Selenium, which simulates human browsing behavior. Using Selenium, we directed a browser equipped with AdNauseam to automatically surf the web, navigating across sites and pages, pausing, scrolling, and clicking ads along the way. Basically, this let us quickly build up a record of prolific clicking activity while tightly controlling variables that might be relevant to whether or not Google classifies as a click as "authentic." We set up four of these automated browsers and ran them respectively for one, two, three, and seven days. At the end of each period, we sent the browsers to our experimental site to see whether AdSense accepted their clicks as legitimate. The Selenium browser that ran for seven days, for example, clicked on more than 900 Google ads, and almost 1,200 ads in all. If Google's systems are indeed sensitive to suspicious clicking behavior, this should have set off alarm bells.

Most of our tests were successful. Google filtered out clicks on our site by the automated browser that ran for three days. But it did not filter out the vast majority of the other clicks, either by ordinary AdNauseam users or even in the higher-volume automated tests, where browsers were clicking upwards of 100 Google ads per day. In short, Google's advanced defenses were not sensitive to the sort of clicking behavior typical of AdNauseam use.

Soon we had \$100 in our AdSense account, enough to trigger Google to mail us a check. We weren't sure what to do with it. This money wasn't ill-gotten, by any means. We were just getting back our own money that we had invested in the advertiser account—less the 32% cut banked by Google. We decided not to cash the check. It was enough to know we'd proved that—for now, at least—AdNauseam works. The check was like a certificate of success.

---

**Google's advanced defenses were not sensitive to the sort of clicking behavior typical of AdNauseam use.**

Nevertheless, our experiment can't answer some other important questions. If you use AdNauseam, how do the clicks it makes affect the profile Google has built on you? Does AdNauseam successfully shield individuals, and the populations they may be sorted into, from being targeted for advertising? (After all, even if you use the extension, Google can still collect masses of data from your email, search history, and other sources.) Even answering our simple original question—whether the software works at all—required substantial effort. Answering those other questions would require insider access across many more nodes in online advertising.

In fact, we can't even know conclusively *why* our test worked—why Google did not detect these AdNauseam clicks. Was it a failure of skill or a failure of will?

A failure of skill would mean that Google's defenses against automated ad-clicking are less sophisticated than the company claims. However, as flattering as it would be to conclude that our small team outmaneuvered one of the most powerful companies in history, that seems farfetched.

A more likely explanation is a failure of will. Google makes money each time an ad is clicked. If advertisers found out they were being billed for phony clicks, that would of course undermine confidence in the online ad business. But advertisers can't validate those suspicions unless they can look from both ends of the market, as we did. And even if they could, [Google's market dominance](#) makes it hard for them to take their business elsewhere.

In a statement, Google spokeswoman Leslie Pitterson wrote, “We detect and filter the vast majority of this automated fake activity. Drawing conclusions from a small-scale experiment is not representative of Google's advanced invalid traffic detection methods and the ongoing work of our dedicated technology, policy, and operations teams that work to combat ad fraud every day.” She added, “We invest heavily in detecting invalid traffic—including automated traffic from extensions such as AdNauseam [*sic*][—to protect users, advertisers, and publishers, as ad fraud hurts everyone in the ecosystem, including Google.](#)”

**AdNauseam might adapt to skirt Google's counteroffensive, but an arms race will obviously favor Google.**

If, contrary to Pitterson's claims, the results of our experiment do hold up at scale, it may be bad news for advertisers, but it's good news for internet users. It means that AdNauseam is one of the few tools ordinary people currently have at their disposal to guard against invasive profiling.

All the same, it is a temporary and imperfect defense. If Google finds a way—or the will—to neutralize AdNauseam, then whatever utility it has might be short-lived. AdNauseam might adapt to skirt Google's counteroffensive, but an arms race will obviously favor Google.

Governments and regulators have generally failed to either craft or enforce rules preventing commercial surveillance. It's true that some recent laws, like the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act, have somewhat limited companies' abilities to sell or share personal data to third parties. However, these laws don't constrain Google's ability to be a *first-party* observer to lots of internet activity and many advertising transactions. In fact, Google may benefit from these privacy laws, since they limit the ability of rivals and customers to acquire the data it has gained. Google keeps watching, and advertisers get more dependent on what it knows.

AdNauseam doesn't stop Google from doing this, but it does let individuals protest against these cycles of surveillance and behavioral targeting that have made much of the online world into a privacy nightmare. Obfuscation is an act of resistance that serves to undermine confidence in tracking and targeting, and to erode the value of data profiles, in the hope that advertisers and ad tech companies might begin to find it impractical and unprofitable to spy on people. Anyone who wants a less invasive online advertising business can give AdNauseam a try.

Another important benefit of using AdNauseam is that, to the extent it succeeds at obfuscation, it helps protect the privacy of *everyone*, not just the people using it. This is because personal information is not strictly personal; information about me can feed into inferences about people I associate with or people who share something in common with me. If you and I go to the same websites, marketers might use what they know about me to make a judgment about you, perhaps labeling you as valuable, risky, or likely to click on one ad or another. AdNauseam users, by disguising their own preferences, make it harder for Google to profile and evaluate other people in their orbits. And so the profiling and prediction engines of surveillance advertising become less reliable.

But, in some ways, the skeptics are right: a few programmers and researchers can't go toe-to-toe with technological titans. Obfuscation is no substitute for an organized and energetic movement, backed by the force of law, to counteract the surveillance advertising that governs so much of the internet. Thankfully, some governments are filing antitrust suits against Google and Facebook, launching investigations into companies' data practices, issuing fines for transgressions, and working on potentially stronger privacy protections. But for now, guerrilla tactics like AdNauseam are the weapons we've got.

