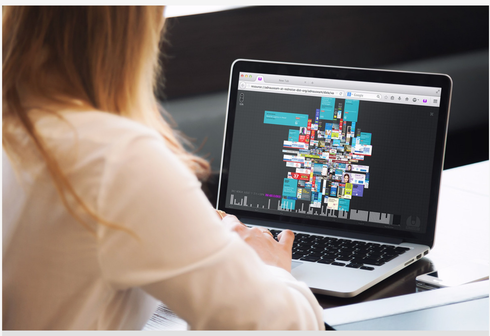
HOW DO WE END THE ADVERTISING ARMS RACE? START THINKING LIKE HUMANS

By **Douglas Rushkoff** — November 12, 2016 3:00 AM



Fighter jets launch flares to flummox heat-sinking missiles by hiding the real target in a sea of decoys. The same strategy, designed to thwart advertisers, may be coming to a web browser near you.

Advertisers and internet users have been trying to outwit each other since the first banner ad hit the web back in 1994. As websites display ads in increasingly unavoidable ways, users develop new strategies for keeping them at bay. But what began as a low-stakes game of cat and mouse has since escalated. With the arrival of targeted advertising and analytics-based tracking software, avoiding ads means avoiding annoyance or distraction; it means preserving basic privacy, security, and human autonomy.

A new kind of ad-blocker called AdNauseam leaves a trail of "flares" for heat-seeking advertisers by clicking on every ad you see in the background. But what will advertisers escalate to next, and where does the constant one upmanship lead us?

Click 'em all

Ad-blockers were once the hottest weapon in this ever-accelerating arms race. But they're far from perfect, as advertisers have already begun to find ways of getting around them by paying to white label their ads, employing software that "reinstalls" ads, or simply denying service to browsers with ad-blocking extensions.

> Behind the scenes, the application is clicking on every single ad offered up.

AdNauseam's creators, Helen Nissenbaum, Daniel C. Howe, and Mushon Zer-Aviv, believe they have provided consumers with the best countermeasure to advertisers' new arsenal. On the face of things, the app – which works on computer-based browsers as well as on iOS or Android – is yet another ad blocking extension, albeit a bit more elegantly designed than most. Install it and you'll see fewer ads, enjoy speedier page loads, and surrender less personal data to click-snooping trackers. The application hides ads from your browser interface, so that they don't distract you for a moment from all the slideshows and listicles the web has to offer. That's the defense.

Where Ad Nauseum breaks new ground is on offense: Behind the scenes, the application is clicking on every single ad offered up. It creates a cloud of data behind you that confuses anyone – or anything – trying to make sense of what you're actually doing online. Your consumer profile becomes one, big, almost random mess.

Privacy through obfuscation

It's a novel approach to protecting user privacy online. Before now, privacy-guarding applications worked to obscure or eliminate *signal*. That is, they tried to prevent your valuable data from falling into the hands of advertisers or snoops. Failing that, the idea is to prevent your valuable data from being tied back to you and your device. Ad blockers have attempted the former, cutting off communication between online trackers and your device. Meanwhile, VPNs like Tor have gone the latter route, hiding your identity behind a succession of proxy IP addresses.

AdNauseam takes the entire opposite tack by doubling down on *noise*. The idea is that your device is sending out so much data that trackers can't distinguish the actionable from the irrelevant clicks. The result is what Zer-Aviv calls "privacy through obfuscation."

Like the ironic punishment in some lost *Twilight Zone* episode, it gives ad vendors and trackers everything they ever asked for. "*So you like clicks, eh? Have all the clicks in the world!*" And like some debonair Mephistopheles, AdNauseam is trying to make a bigger point here.

AI, meet my AI

In the current advertising-publishing ecosystem, it doesn't *matter* whether it's an actual human or a drinking bird toy clicking those banner ads. And yet, to participate in this ecosystem is to submit to be profiled by click-tracking analytics companies and exposing ourselves to the risks of malvertising. Meanwhile, the companies who actually make those products real enough to be worth advertising must pay, regardless of whether their advertisements are clicked by interested consumers or click-juicing fraudbots. On either end of this equation, it's humans who are paying steeper and steeper prices to subsidize the absurd theater of AIs talking to one another.

> If publishers can't advertise, someone has to pay for their content or they can't produce any.

For the time being, ad vendors and browser developers will have nothing to complain about. For their part, publishers are less likely to ban AdNauseam because they're still getting paid for displaying ads on a fee-per-click basis. With everyone clicking on everything, websites will be earning more than ever. But whether as a statement of protest or a functional application, AdNauseam is at best a temporary solution. It may represent a minor win in the ongoing war between web users, advertisers, and big data. But countermeasures will be taken and new advertising algorithms written to recognize AdNauseam's fake clicks and, eventually, even defeat its ad-blocking.

Besides, if publishers can't advertise, someone has to pay for their content or they can't produce any. In the long run, we will have to figure out a way to subsidize the content we enjoy online without surrendering to a life bereft of privacy and security.

If we can't do that, then expect a future with two different internets. One will be composed of all the websites, applications, and media companies that operate on a subscription or pay-per-use basis. The other will finance itself by methods resembling our current broken system — tracking, data mining, targeted advertising, and any other creepy innovations that come along.

Only the wealthy will be able to live exclusively on the pay-for-privacy side of the web. The very poor will have no choice but to "opt-in" for constant observation and intrusion on the part of advertisers. Most of us will fall somewhere in between, paying for a few premium services here and there, but otherwise submitting to the trackers. Unfortunately, it doesn't take much surveillance to build a precise profile of a web user. Privacy really is an all-or-nothing proposition when it comes to tracking and big data.

Think of the humans

Only last week, we learned that Google would reverse its longstanding policy of anonymizing user data. That's a big deal. Google will no longer attribute all those shirtless Taylor Lautner searches to a faceless machine named aa28:2d15:a2f0:2efc:6696:532e:5f60:3c3721e5:c3d9:48b0:3836:5596:4ca9:d70c:82af. From now on, it reserves the right to connect those clicks with the name your mother – and government – calls you.

Perhaps when this becomes the norm, web users will finally confront the fact that our refusal to pay the people who create our content is inextricably tied to this effort to identify *us* as people, instead. In other words, their human need to get paid for their work is not entirely disconnected from our human need for privacy. As the battle between these two populations escalates, we all turn to bots to do our bidding for us. This only dehumanizes us all further.

Just as we readers may come to recognize the human workers on the other side of our algorithmically chosen content, advertisers may even be convinced that taking the side of their fellow humans is the only step to ensure that their ads will actually be noticed, and not merely registered by a swarm of bots.

If we can all just stop cooperating with robots against real-life people, we may finally end the arms race.

The views expressed here are solely those of the author and do not reflect the beliefs of Digital Trends.