FREEDOM FROM PRIVACY

How to Protest Online Trackers Without Leaving Your Chair

By Brady Dale • 07/25/16 9:33am

The birds have no idea what the trackers do with data about their behavior. (Photo: Ernesto Benavides/Getty)

Imagine that someone called you every five minutes and said, “Tell me what you are doing right now.” And then imagine that for some reason you were compelled to answer the question. That’s what tracking software does to people browsing the web. When visiting a site, third party ads query browsers constantly, and browsers happily answer all those questions.

Many users simply block these trackers, using software like AdBlock Plus, Ghostery or uBlock, but some want a way to strike back against an industry that’s become much too forward. “Ignoring ads is no longer enough,” Daniel Howe, a developer who created a new strategy to undermine trackers said in a release. “People want their objections heard by the corporations involved.”

> *‘It’s slightly less safe than just using uBlock in the same way that attending a protest is less safe than sitting at home and watching TV.’*

This weekend at the HOPE XI hacker conference in Manhattan, Howe debuted AdNauseum 2.0, a browser extension that runs in the background and virtually clicks on every single ad that sites serve a user. This muddles the tracking companies’ record of a people’s real activity by adding phony behaviors. The Observer previously reported on similar efforts to obscure browser fingerprinting.

Howe and his collaborator, NYU’s Dr. Helen Nissenbaum, first released AdNauseum as a prototype for Firefox in 2014. With this new release, it now also works in Chrome and Opera browsers. Chrome and Firefox, it’s worth noting, take very different approaches to user privacy.

Many privacy proponents at this weekend’s conference wondered whether or not there might be a way in which sending false clicks to trackers could give those companies a way to identify users. “It’s slightly less safe than just using uBlock in the same way that attending a protest is less safe than sitting at home and watching TV,” Howe replied.

AdNauseum isn’t for people who just want to be anonymous online. Howe and Nissenbaum created AdNauseum for users that want to actively undermine the business of watching what people do with their computers.

The software imposes costs on the industry, as Howe explained in an interview with the Observer. “All this noise is written into their logs,” he said. Staff at these companies have to sit down and have meetings about the bad data. Developers need to take time to find workarounds. Chunks of the database have to be flagged or deleted as useless.

In the best case scenario, AdNauseum could be adopted so widely that it actually makes the business of putting trackers into ads unprofitable. As unlikely as that might be, Howe believes the worst case scenario for users isn’t that bad. “If they filter out these clicks, they are kind of ignoring you as a user,” he said.

For more detail on Howe’s approach, he has a paper called “Surveillance Countermeasures” available at the APRJA journal.

Previously, Howe and Nissenbaum built TrackMeNot, another obfuscation technique that sends a slew of false searchers to Google, Bing and AOL, for every real search a user enters. More than a million users have installed that extension, according to Howe. The Observer previously reported on another data pollution project, Data Arbitrage, which seeks to create a network of robot social media profiles the dilute insights about the behavior of humans.