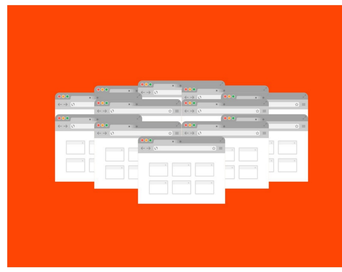
EMILY DREYFUSS BUSINESS 03.29.17 7:11 PM

WANNA PROTECT YOUR ONLINE PRIVACY? OPEN A TAB AND MAKE SOME NOISE



GETTY IMAGES

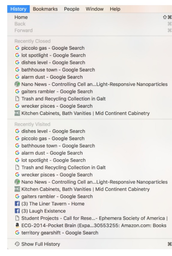
I JUST GOOGLED "alarm dust," "alibi sweatshirt," and "sleuth intelligence." Then I shopped for industrial dehydrators, scanned a Pinterest page for concrete decks, and read something about nuclear war.

The thing is, I'm not in the market for a new dehydrator. Concrete decks aren't really my style, and I still have no idea what "alarm dust" is. I didn't visit any of these web sites of my own volition—a website called Internet Noise did, all to obscure my real browsing habits in a fog of fake search history.

Yesterday, the House of Representatives voted to let internet service providers sell your browsing data on the open market. This decision angered a lot of people, including programmer Dan Schultz. After reading about the vote on Twitter at 1 AM, he turned off Zelda and coded this ghost currently opening tabs on my machine.

Internet Noise acts like a browser extension but is really just a website that auto-opens tabs based on random Google searches. Schultz isn't a hacker but a concerned do-gooder trying to get Americans to understand how much their online privacy is at risk. "I cannot function in civil society in 2017 without an internet connection, and I have to go through an ISP to do that," he says.

To counter that threat, Schultz wants to make it impossible for ISPs or anyone they've sold your data to accurately profile you. The vote yesterday implicitly legalized such tracking by explicitly rescinding rules against it. By muddying your online identity, advertisers can't accurately target you, and authorities can't accurately surveil you. To create noise that blocks your signal, Schultz googled "Top 4,000 nouns" and folded the list into his code. When you hit the "Make some noise" button on his site, it harnesses Google's "I'm Feeling Lucky" button to search those phrases, then opens five tabs based on the results. Every ten seconds it does another search and opens up five more. Within minutes, my entire browser history was a jumble. Internet Noise will keep going until you hit the "STOP THE NOISE!" button. Schultz envisions you running this while you sleep.



This is a snapshot of my browsing history a minute after running Internet Noise.

This signal-jamming offers just one modest example of the larger theory of obfuscation, the idea that if you can't disappear online at least you can hide yourself in a miasma of noise. Adnauseam.io is a plug-in currently banned by Google that works in a similar way, except instead of just opening pages and jamming your history, it actually clicks on random ads. In the process, it's directly targeting the ad model that underpins so much of the internet, and it can be pretty effective. I am not building a deck or in the market for a manual regenerative hydrator, but now that Internet Noise search for those things ads for both will likely appear in my Facebook feed, and I'm cool with that. Internet Noise tries to throw them off my trail by creating a fake path to follow. That's the key to successful signal-jamming: You can't just generate random sounds. You have to generate a second song.

Risks and Limitations

What if it's not an advertiser looking at your web data, though, but a spy agency or some other authority drawing conclusions about your browsing? From my test run, someone might conclude something causal between my googling of industrial equipment, chemical companies, nuclear proliferation, sleuth intelligence, and cancer. Sketchy! Schultz himself hasn't evaluated all 4,000 search words (and the 16,000,000 results their two-word combinations can generate)[1] to determine whether they might raise red flags for anyone spying on my habits.

But I can take some comfort in the fact that right now, Schultz's site isn't that effective at truly jamming my signal. It's actually too random. It doesn't linger on sites very long, nor does it revisit them. In other words, it doesn't really look human, and smart-enough tracking algorithms likely know that.

"The main problem with these sorts of projects is that they rely on your being able to generate plausible activity more reliably than your adversaries," says privacy expert Parker Higgins, formerly of the Electronic Frontier Foundation. "That's a really hard problem."

Schultz says the main point of Internet Noise for now is to raise awareness, though the open source project has the potential to evolve into a real privacy tool. People have already reached out to fix minor problems and suggest ways to make it more effective. In the meantime, anyone truly concerned about their privacy needs to stay savvy about the technical limitations of the tools they choose, including Internet Noise. "I fear that any of these cool hacks will give people a false sense of security," says EFF privacy researcher Gennie Gebhart, who is working with her team to create a broad toolkit of how to protect yourself from ISP tracking. "There is no one click that will protect you from all the kinds of tracking."

Not that privacy-minded programmers will stop trying. Internet Noise may be the first grassroots hack created in direct response to yesterday's vote. But a sizable collection of similar tools offers a sobering reminder that companies were already tracking and selling your data. Geeks may not have the political clout to stop such infringements of online freedom, but they do have the advantages of speed and passion. As long as they have keyboards, internet fighters will try to drown out Washington with the roar of their code.

[1]*Updated to include how many different search results the noun combinations could generate.*

#CONGRESS #DATA #ISPS #PRIVACY