TECHNOLOGY

Internet Privacy: New Browser Plugins Hide User Activity From ISPs By Creating Digital Noise

BY **AJ DELLINGER** ON 05/01/17 AT 7:20 PM

A decision earlier this year by the U.S. Congress to overturn rules adopted by the Federal Communications Commission that would have prevented internet service providers from collecting user information without permission has given people a new reason to be concerned about their online privacy.

It's worth noting, however, the protections were repealed before they ever took effect. ISPs have been able to collect sensitive user information, including browsing history and app usage data, without consent and selling it to advertisers for years. But it is never too late to start protecting yourself from prying eyes.

Read: *What Are VPNs, How Do You Use Them And Do You Need A Virtual Private Network?*

The best option for those concerned about invasive practices of ISPs is to pick up a virtual private network (VPN). These privacy tools connect a user's computer to a remote server which processes all requests from the user and responses from websites.

By acting as an intermediary, the VPN hides the identity of the user and sends all information via an encrypted connection that makes it unviewable and untrackable by the user's ISP — though that data is still accessible by the VPN provider, and users will want to examine the VPN's privacy agreement carefully to make sure their data is secure.

While VPNs may be the best option, they can also be a technical challenge for some because they can require a bit of effort to set up. For those looking for an option that is quicker and easier, there are several browser plugins that effectively hide a user's identity not by masking it, but by drowning it out with other information.

A number of browser extensions have recently appeared that operate as smoke screens for user information by creating a massive amount of digital static. They generate fake web activity — so much so that it becomes impossible to know what exactly the user is actually doing.

Read: *VPN Services Report Huge Increase In Downloads, Usage Since Broadband Privacy Rules Were Repealed*

One of the most popular of these new tools for privacy protection is Noiszy. The service's website says its purpose is to make data collected by ISPs "less actionable" by muddling the actual tracks and camouflaging true user behavior.

Noiszy works in the background of a user's browser, visiting hundreds or thousands of seemingly random and unrelated websites. All of that information, along with the user's actual activity, is all vacuumed up, but the real data is diluted to a degree that makes it useless. Attempts to create targeted advertising for the user is rendered ineffective.

Related Stories

- **VPNs See Spike In Downloads, Usage**
- **What Are VPNs And How Do You Use Them?**

A similar concept, known as RuinMyHistory, operates in a similar way. The script, available via GitHub, opens a new window and runs through a series of websites while the user browses the web normally.

A more controversial option that operates in the same vein is AdNauseam. The service has been available for some time, but gained prominence with the repeal of the Broadband Consumer Privacy Rules earlier this year.

AdNauseam toys with online advertisers in a disorienting way. Instead of blocking ads, the way a service like uBlock Origin does, AdNauseam instead clicks on everything to pollute the user's data and activity.

It's also worth noting AdNauseam's practice is an act of protest as much as it is a means of protection, and that protest violates the rules of some advertising platforms and has been accused of "click fraud" for clicking advertisements under false pretenses. For that reason, the service is banned from the Google Chrome Web Store though there are still ways to install it on Chrome and other browsers.