Adults and Children Continuously Targeted for Data Extraction, Surveillance and Censorship

Description

It isn't an exaggeration to say that not a single day goes by without a new data exploit, hack, breach, leak, or scandal involving censorship by private companies and government agencies. Of course, this is all compounded even further by the fact that more devices contain more sensors that connect to the internet than ever before, offering many new methods for targeting groups and individuals. It has been estimated that by 2030 there could be *125 billion devices* — potentially 15 per user — that in some way will comprise the ever-expanding Internet of Things ecosystem.

Amid this sea of two-way data traffic, we have a massive amount of targeted advertising and personally identifiable information extraction that has shown very often to all be done without users' consent. If there is consent at all, it very likely is through lenthy and confusing Terms and Conditions that almost no one reads in their entirety. Worse still is the proven targeting of children's data. Lawmakers continue to attempt to rein in these consumer-unfriendly practices, but their current proposals will likely do more harm than good. At this point it should be obvious that even if legislative measures are effectively created, such a waiting game only leaves all of us, including our kids, increasingly vulnerable at any given moment. People want – and deserve – to become personally responsible for their own security and privacy.

Fortunately, there are residential proxy providers on the opposing side that understand the rising awareness by the public of these data violations and creepy intrusions. These companies are doing everything they can to offer the tools necessary for individuals to protect their family's data and privacy, while also offering increasing freedom to reach the websites that we do want to visit.

The main issue when browsing the open internet, or transmitting data through your connected devices, is the clearly established two-way connection between your IP address and the final destination. This information is easily recorded and databased, then potentially given to third parties beyond what the user intended, or flat-out intercepted by those with mal intent. As one company stated:

> (B)rowsing the internet with your IP address in the open is the same as displaying your

social security number, credit card, or passport everywhere you go. This way, hackers can use any IP address to track you or break into your device. Scary, huh?

It is also easy to block traffic and impose a range of restrictions, including geo-location simply by the IP identifier. Residential proxies have been developed to alleviate core cybersecurity vulnerabilities as well as info blockades.

In essence, a residential proxy is a secure gateway between any IP address in your home and the wider internet at large. These systems have become nearly seamless to use, even for the non-tech savvy, and work perfectly well alongside the browsers we are all familiar with on our desktop or mobile devices. The reassignment of address also re-opens the internet to be the true global source of information and business that it was originally intended to be.

As we've seen over the last several years particularly, political or economic conflict that has little to do with the decisions of ordinary citizens has often resulted in a blanket stifling of the information the global population is permitted to see. These conflicts also have been used as justification for further surveillance by government in the name of protecting the public. The combination of these measures has been described as a "Balkanization of the internet."

The world of information that the average user actually wants, however, is one where their security is fully decentralized, but all barriers to entry for business and the pursuit information remain completely open. At this point, we have the exact opposite when we interact with the internet in the traditional manner. Most people remain unaware of how easily attainable a restoration of their personal right to choose what information they receive can be. With the full range of proxy services designed to return anonymity and security to our data, there is simply no longer a reason to pay the high price of remaining vulnerable while utilizing the powerful features of communication and business that the internet provides.

Image: [Pixabay](#)

By Steven Maxwell

Category

1. Freedom-Free speech-Resitance & H-rights
2. Main

Date Created
04/21/2022