VPN Dilemma: Anonymous Expression Vs. Anonymous Defamation

Related Attorneys

Adam C. Sherman

Related Services

Technology Transactions

AUTHORED ARTICLE | 7.19.2016
Technology Law360

Adam Sherman, a partner in the Vorys Cincinnati office and a member of the technology and intellectual property group, authored an article for *Technology Law360* titled "VPN Dilemma: Anonymous Expression Vs. Anonymous Defamation." The full text of the article is included below.

--

VPN Dilemma: Anonymous Expression Vs. Anonymous Defamation

Since the general public started using the internet, it has made people feel anonymous. After all, it is the land of screen names, handles and avatars. But there were always limits. Websites and internet service providers (ISPs) keep logs of their users. By putting these logs together, it is possible to identify internet posters most of the time. At least, that used to be true.

Today, many free or low-cost services provide near total anonymity. Anyone using these services can post anything they want with no risk of being identified. These services are called virtual private networks (VPNs). If the internet was viewed as a new Wild West in its early days, that view is now accurate for anyone who wishes it. And this is not always a good thing. Due to a combination of cheap or free VPNs and federal law that protects websites from liability, a person harmed by defamatory or harassing internet content often has no way of having it removed.

While anonymity may encourage free expression, there is also a dark side. A VPN user can defame or harass anyone with no accountability. The popularity of social media and gripe sites makes the problem worse. The most popular sites appear at the top of search-engine results. For many businesses and individuals, gripe sites appear on the first page of their search results. Negative search results are such a concern that an entire industry has formed to address the problem.

Before VPNs, those harmed by defamatory or harassing posts had legal recourse. For example, harmed individuals could file a John Doe lawsuit and use subpoenas to identify internet posters. Often this is a two-step process. The first subpoena goes to the website hosting the content. The website will typically provide the poster's internet protocol (IP) address, which is an alpha-numeric code that identifies a device on the internet. The poster's IP address will usually lead to an ISP. A second subpoena to the ISP provides the subscriber's real name and contact information. But when a poster uses a VPN, this process is ineffective.

VPNs are a simple, cheap way to become truly anonymous on the internet. A device using a VPN transfers encrypted data over the internet to the VPN service. Once the device connects to the network, the VPN assigns a new IP address and sends the data on its way. To the outside world, only the VPN's IP address is visible. And only the VPN provider has the potential to connect the device's actual IP address with the IP address assigned by the VPN. But most anonymous VPN services do not create or maintain logs that would allow anyone to connect the two IP addresses.

In other words, a VPN is a middleman that allows users to access the internet by taking on the middleman's identity. To the outside world, all internet activity comes from the middleman. And there is no way to find out on whose behalf the middleman is working.

While this may sound complicated, from the user's standpoint it's as simple as installing a small computer program or smartphone app. The software takes care of the rest. Once activated, the software is transparent, directing all internet traffic through the VPN. Because of this, anyone can become truly anonymous online with no technical knowledge or expertise.

While VPNs protect those causing harm on the internet, a victim could, in theory, seek recourse or removal from the website hosting the content. But, in the United States, there is no legal recourse against website. They're protected by federal law.

In part to protect freedom of expression on the internet, Congress adopted Section 230 of the Communications Decency Act of 1996 (CDA). In simple terms, Section 230 protects websites from liability for publishing third-party content. Websites are immune from liability for content posted or provided by their users, with a few exceptions. For example, a site that hosts reviews by its users is not liable for defamatory reviews. Neither is a site that solicits content from users and then decides what to publish. Without this immunity, these sites may not exist. They would be easy targets for lawsuits. A plaintiff could sue the site for a false review rather than try to find the anonymous poster. Websites would have little incentive to defend these lawsuits and would likely remove the content instead. The immunity provided by the CDA is important to keep these websites operating. At least some of the services they provide are valuable.

The problem is that with the combined protections of the CDA and VPNs, there is no help for those harmed by unlawful content. VPN users can post defamatory, harassing or other unlawful content with total confidence that they will not be identified. Now that VPN services are easy to use and inexpensive, anyone can post online with impunity. The CDA means that a website is immune from liability for content posted by its users. The damaging information will appear on the internet for as long as the website chooses. Victims of online attacks have no recourse.

Of course, websites can remove content voluntarily. And many do. But they all have different standards and processes. Some will not remove anything. Others will remove content posted by an IP address associated with a VPN service. Some will remove content if presented with a court order finding it unlawful. The problem is there are no standards, and for many victims there is nothing they can do.

The combination of technology and law — VPNs and Section 230 of the CDA — can cause serious problems for victims of online attacks. It will only get worse as VPNs become more popular and more known to internet users. This is a situation where technology is outpacing the law, and it needs to be addressed. The question is: How? Most solutions have faults.

One possibility is for gripe sites to refuse content from known VPN IP addresses. This is possible and already being done in other contexts. For example, Netflix recently started banning the use of VPN IP addresses to prevent users from accessing content that Netflix has not made available in their countries of residence. But Netflix has taken this action because it benefits Netflix. In contrast, gripe sites benefit from negative content, which drives page hits, which in turn provide advertising revenue. Gripe sites have no incentive to restrict content for anonymous VPN users. Also, the United States recognizes a right to anonymous speech. And while a private website refusing content from VPNs is not a First Amendment issue, it may inhibit speech.

Some gripe sites will voluntarily remove content posted by VPN users if requested to do so. Typically, this arises when a site is served with a subpoena to identify the IP address associated with defamatory content. Sites that follow this approach will remove the content if the IP address is for a VPN. This approach takes into account the fact that a plaintiff has no recourse against a poster using a VPN. But the content remains up until litigation is filed and a subpoena is issued. And this approach is followed by only a few sites.

The challenge is to find a solution that respects speech rights but also protects against the injuries that can be caused by anonymous online attacks. Currently, we are a patchwork of different practices followed by various websites and search engines. From a legal standpoint, the balance is strongly in favor of allowing anonymous speech. But as businesses' and individuals' online reputations become more and more important, the balance needs to be adjusted.