3/12/2019

Internet Service Providers Offering Internet Service to Residents of Tennessee

Regarding: Tennessee's resolution relative to a safer internet for children

Background

Over the last year, our organization, along with Robert W. Peters, Esq. President Emeritus of National Center on Sexual Exploitation, the National Center on Sexual Exploitation, Enough is Enough, Ernie Allen, former President & CEO of the National Center for Missing & Exploited Children, Concerned Women for America of Missouri and other groups and individuals played a pertinent role in the development of this state resolution. In researching how Internet service providers can play role in helping create a safer Internet for children, we've found much evidence from countries taking action, tech companies providing technology to ISP's, and ISP's taking voluntary initiative all over the world. A copy of most of our findings can be found at https://decencyusa.org/internet-service-providers-can-help-stop-the-health-crisis-of-pornography/ and more on our website at www.decencyusa.org.

This resolution recognizes that:

"Technology is available for internet service providers to protect children and families from the instant access to internet pornography on fixed and mobile devices through various proprietary and cloud-based solutions" and does not require the "use of additional hardware and software."

Technology is available for Internet service providers to protect children and families from instant access to Internet pornography. Over the last year, we spoke with many filtering companies and tech experts to discover the role an Internet service provider can play in creating a safer Internet. One DNS filter company, SafeDNS, initially shared with us this analogy, "Just as the flow of water can be manually shut off at many points from the water plant facility to a home faucet, so can the flow of pornography be shut off at many points from the Internet service provider to a customers device." SafeDNS is a team of IT and web security experts that offer web filtering service used by more than

4,000 organizations and tens of thousands of private users across US, UK, the Middle East, Eastern Europe, and the Far East.

They explained that their service, through a method of filtering called DNS, equips ISP's, big or small, through cloud-based technology to filter a "near-perfect 98.3% of requests to adult content" on the Internet before it reaches a customers device. On their website[1], they shared with us various case studies from around the world where they have uniquely helped Internet providers, both fixed connection and mobile alike, to provide Internet filtering solutions tailored to the ISP's needs, including the blocking of pornographic websites to give parents greater instrumentality over the kinds of content available to children.

Ken Carnesi, CEO of DNSFilter, a company based in Washington D.C. that serves over 6,000 organizations worldwide in a $4B market, and in 2018 was named Top Emerging Security Vendor explained, through their technology, an ISP, big or small, with 250 or 25 million subscribers, can provide a service to customers that filters pornography, with the same process applying to both fixed and mobile Internet services. He also noted that ISP's can even re-brand their service offering the entire service supplied by DNSFilter as a brand of their own.

This technology is also available for mobile phones as well. Carnesi explained that DNS based technology used to block the transmission of pornography websites works the same for mobile phones. SafeDNS also shared a detailed case study of a major mobile phone service provider in Ukraine in deploying for them a tool "to make the internet cleaner and safer for kids and adults alike."[2] One of the largest known online pornography sites recorded that 61% of their pornographic material is viewed by mobile phones, and that percentage is increasing.[3]

Today's technology for ISP's to block pornography for customers is done effectively without the use of additional hardware and software. DNS filtering (or Domain Name System filtering) is a technique of blocking access to certain websites, web pages, or IP addresses. DNS is what allows domain names to be used, such as www.decencyusa.org, rather than typing in a very difficult to remember IP address. With DNS filtering in place, rather than the DNS server returning the IP address, the user will be directed to a local IP address that will display a block page explaining that the site cannot be accessed. This control could be applied at the router level, via your ISP, or a third party – a web filtering service provider. An ISP can redirect their DNS server to a

[1] https://www.safedns.com/en/safe-internet-for-telecoms-and-isps/
[2] https://www.safedns.com/userfiles/uploads/files/SafeDNS_Case-Study_InterTelecom_Ukraine.pdf
[3] https://memeburn.com/2017/01/pornhub-2016-devices-platforms/

dedicated server that is designed to filter pornography for every customer in their network. This is all cloud-based, without the use of additional hardware and software.[4]

Michael Davies, co-founder of RDI, a company based in the U.K. that has serviced 100's of WiFi and Internet service providers in the U.K. and all over the world with their Friendly Wifi seal,[5] shared with us that, along with ISP's own proprietary solutions, DNS filtering is the primary medium Internet and public WiFi providers use to protect from pornographic material.

The technology "is reasonably and commercially unburdensome."

This statement implies the financial reasonableness of such technology. Our group has been in contact with a number of tech companies able to supply ISP's with the technology according to the requests of the resolution. Regarding a model currently introduced in the Missouri legislature, SB382, DNSFilter hinted that for their company to supply 100% of the provisions of the bill that the cost could be less than $0.50 per subscriber per month. The Missouri law can easily be viewed as a compliance model for ISP's regarding this resolution. SafeDNS elected to offer first three months free in contracting with ISP's. Also, Sky Broadband when initiating default filtering in the U.K. for their six million subscribers, they did not charge extra to do so.[6] Other companies such as Clean Browsing and Titan HQ are offering their services to ISP's in compliance with the resolution's requests. Regarding the reasonableness of such technology, Davies shared that equipping ISP's and public WiFi providers with complying technology "takes only minutes". The ease of which the technology can be implemented naturally reflects a lesser burden of cost. Our organization will be available to present compliance models from such companies following the passage of this resolution.

"Internet service providers could help significantly reduce children's exposure and access to internet pornography were they to voluntarily block access to internet pornography by default but allow adult customers to opt-out of protections."

Current technology can equip Internet providers to reduce children's exposure to pornography. Mr. Davies explained that there are companies that provide categorical lists of websites like gambling, pornography, child sex abuse images, and more for other companies to purchase. DNS filtering companies purchase lists created by these

[4] https://www.spamtitan.com/web-filtering/how-does-dns-filtering-work/
[5] https://www.friendlywifi.com/
[6] https://www.ispreview.co.uk/index.php/2015/01/sky-broadband-shield-clarifies-uk-adult-internet-filtering-policy.html

companies in order to have the ability to filter certain categories. “The entire technology,” he said, “to block categories, like pornography, is comprised of lists provided by third party companies that daily update as new material emerges on the Internet.”

We also spoke with Ralph Yarro, an early developer and contributor to web filtering technologies such as Blue Coat and K9 Web Protection shared with us that through “facial recognition technology” companies are able to capture obscene material on the Internet much faster. He elaborated to explain that the past problems of over-blocking and under-blocking (not blocking enough) through filtering are obsolete with modern technology. He pointed us to K9 Web Filtering, an advanced Web filtering technology used by enterprise and government institutions worldwide, that, with a user-friendly interface, allows you to control Internet use in your home and enter specific URL’s to block or unblock.

DNSFilter, SafeDNS, Clean Browsing, TitanHQ, and Friendly WiFi are all companies that shared with our organization, first hand, that they can supply technology to ISP’s that will shut off much of the flow of pornography on the internet and provide adult customers that ability to opt-out of protections.

This resolution requests for Internet service providers to:

“Voluntarily utilize the most effective and affordable technology now available to block access to internet pornography by default but allowing adult customers to opt-out of protections that block access to content that is protected by the Constitution.”

Every able person or entity should voluntarily play a role in protecting children from harmful material. By ISP’s voluntarily blocking Internet pornography by default for customers, they can create a safer Internet for children. Such technology for ISP’s to do so is widely-used, is very effective in blocking material that is harmful to minors, can be financially reasonable, and is easily implemented.

How We Can Help

Following the passage of this resolution, along with the help of kind legislators, we’ll be presenting to ISP’s a variety of companies that are able to help supply technology according to the requests of the resolution.

Contact info:

Ricky Darr
ricky@decencyusa.org
National Decency Coalition
615-640-2429

Tiffany Leeper
media@decencyusa.org
National Decency Coalition
615-640-2429