NetChoice

Congress should reject the anti-innovation language regarding cloud service providers in the Appropriations legislation

Summary:

While NetChoice and all its members oppose Child Sexual Abuse Material (CSAM) and work tirelessly to end it, the language in the Appropriations bill would do nothing to address the problem while eliminating America's ability to use reliable, home-grown, cloud service providers.

Under the proposed language, it would result in none of the leading American cloud service providers being able to enter into government contracts.

The language essentially eliminates the top four American-based cloud service providers from consideration for government contracts. This means that taxpayers will pay more for non-competitive contracts, and government clients will not be able to choose cloud services with features and performance that are superior.

The offending amendment:

What seems like reasonable amendment language would disqualify major competitors from providing cloud services to government:

> "Sec. 755. (a) Except as provided in subsection (b), none of the funds made available by this Act may be used to purchase remote computing services except remote computing services determined by the Government to--
>
> (1) not store or transmit images which depict apparent violations of section 2251, 2251A, 2252, 2252A, 2252B, or 2260 of title 18, United States Code, with respect to child pornography"

This language is designed to disqualify network providers with consumer users – who account for 97 percent of the market – even though these companies are among the most helpful at discovering and reporting Child Sexual Abuse Material (CSAM). Whenever CSAM is detected in user content, these companies take immediate action to remove and block that content.

However, battling CSAM content is a continuous *arms race* against users who apply new encryption hashes to disguise the content from recognition. While providers are continuously working to identify new hashes and improve technology for identifying and removing CSAM, it is impossible to have zero instances of illegal material at any time.

This would be akin to disqualifying all phone companies for government contracts since crimes were committed using a phone. Moreover, the amendment suggests "determined by the Government", without any process, right to appeal, or evidentiary standard.

There is a better way.

Government agencies already have the power to exclude any vendor who is found to have violated federal law, including laws regarding CSAM.

Cloud services are fighting online child sexual abuse and exploitation

America's leading cloud providers already take extraordinary measures to prevent their services from being used to spread child sexual abuse material (CSAM). They invest heavily in technology to detect CSAM, remove it, and report offenses to NCMEC (National Center for Missing and Exploited Children).

- During 2020, 21.7 million reports of child sexual exploitation went to NCMEC's CyberTipline, covering 65.4 million images, videos and other files. Of course this also creates a Catch-22 for platforms – if they report to NCMEC then they provide the evidence needed to disqualify them from procurement.
- In the second half of 2020, American tech platforms removed more than 6 billion posts for harmful content including CSAM.

Additional Resources

- NCMEC - CyberTipline Reporting Figures
- Google's efforts to combat online child sexual abuse material
- Amazon's commitment to fighting child sexual exploitation and abuse
- NetChoice content moderation transparency report
- Microsoft Digital Safety Content Report