

March 27, 2023

**RE: Opposition – SB 1515, Civil liability for publishing or distributing material harmful to minors on the Internet**

Dear Governor Youngkin,

I write today on behalf of The Free Speech Coalition, the national trade association for the adult industry, to express our opposition to SB 1515 and share our desire to collaborate on a better solution.

We whole-heartedly support the goal of protecting young people from material that is age-inappropriate or harmful. Unfortunately, SB 1515 has significant practical, technical and legal problems that will undermine its effectiveness in protecting children, create serious privacy risks and infringe on Virginians' Constitutional rights.

**SB 1515 Will Not Prevent Minors from Accessing Adult Content**

The only way that a website can determine whether a user is located in Virginia is to use the geolocation data provided by the user's device. It is extremely simple to use a Virtual Private Network (VPN) to make it appear as though a user is located elsewhere, thereby evading age checks. In fact, a recent study of middle schoolers (youth aged 11-14) found that 41% of them use a VPN to browse the internet.<sup>1</sup>

Additionally, Common Sense Media (the nation's leading nonprofit source for media recommendations and advice for families) released a report in January indicating that 58% of teens aged 13-17 have seen adult content accidentally – 18% of which reported that it was on social media.<sup>2</sup> Because this bill only applies to websites where more than one third of the content meets the definition of material harmful to minors, it will do nothing to protect those young people.

The Common Sense report also revealed that 41% of teens reported seeing online pornography during the school day, with a shocking 44% indicating that they had seen it on a school-issued device.

### **SB 1515 Will Endanger Virginians' Private Information**

Compliance with SB 1515 requires a user to transmit extremely sensitive data – digitized copies of their government-issued identification, biometric scans, or other forms of data used by commercial age verification software providers – over the internet.

While the bill laudably bars companies from retaining this information, that does not mitigate the dangers of transmitting it in the first place. The mere collection of this information opens Virginians up to the risk of data breaches. Even good actors and governments struggle to secure this type of data, as we've seen countless times in recent years.

In addition to the risks inherent in transmitting this data to reputable age verification providers, the introduction of this kind of scheme creates a massive opportunity for criminals. Personal information regarding sex and sexuality is highly sensitive, and criminals are adept at exploiting this. In fact, one common extortion tactic reported by the FTC employs a threat to disclose a person's adult website browsing behavior.<sup>3</sup>

Even more troublingly, we are already receiving reports in Louisiana of potential identity theft, as criminals set up phishing scams where they pose as an adult site and solicit the upload of identification documents. We expect Virginians to be victimized with increasing frequency by criminals should the law pass.

### **SB 1515 Will Result in Exposure to Illegal Content**

Websites that are not bound by U.S. law will be the primary beneficiaries of this bill. Legal adults, when confronted with a governmental request to verify identity during a visit to an adult site will either need to subject themselves to the privacy risks outlined above or go elsewhere. Minors who do not use a VPN to evade the law will do the same.

This will simultaneously punish responsible sites that comply with the law and boost the growth of illicit websites and pirate platforms where they are at an enormous risk of encountering dangerous illegal content such as child sexual abuse material (CSAM) and non-consensual intimate imagery ("revenge porn"). Children will run the risk of becoming victimized themselves.

### **SB 1515 is Unconstitutional**

Adult content – even material harmful to minors – is First Amendment-protected speech and the Supreme Court has ruled repeatedly that restrictions on its production and consumption face the highest legal bar: strict scrutiny.

In *Reno v. ACLU* (1997), the Court struck down the statutory provisions of the Communications Decency Act (CDA) requiring use of age verification software as an unconstitutional content-based blanket restriction on speech:

“In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and address to one another.”<sup>4</sup>

The Court found that the burdens posed by online age verification unnecessarily suppress access to protected speech, and that “less restrictive alternatives” — such as device-level filters — “would be at least as effective” at barring minors from seeing adult material. The Court pointed to parental controls/filters as a preferred method because they respect parents’ authority to determine what content is appropriate for their children.

### **How to Keep Children Safe**

To be clear: the adult industry does not want minors on its sites. This is why we utilize the “Restricted to Adults” (RTA) label on our sites and platforms. It was created by the nonprofit Association of Sites Advocating Child Protection (ASACP) to standardize a single, consistent, universally recognizable tag for adult material that allows it to be automatically blocked by device-level parental control and filtering software.

Parental controls and device-level filters are effective tools if parents and schools are willing to use them. Many of us use them in our own households to protect the young people in our lives from accessing adult content, even when using a VPN. This technology not only puts power where it should be – in the hands of parents and caregivers – it is widely available, fully supported by industry, and endorsed by the Supreme Court.

If your goal is to keep minors from accessing adult content, our industry is willing and enthusiastic to work with you to achieve it. We understand the technology, the consumer landscape, and the practical solutions that can keep minors from encountering adult material while preserving the safety and privacy of Virginians and avoiding costly, time-consuming constitutional challenges.

In recent discussions with Free Speech Coalition members, many expressed eagerness to find a self-regulating solution that would encourage wider adoption by consumers. The history of these efforts have taught us that an effective system must:

*Use a Shared Standard*

The system must be consistent across platforms and across states

*Safeguard Privacy*

The system must not be vulnerable to hacking or disclosure.

*Not Overly Burden Consumers*

Technologies that are familiar and easy-to-use encourage compliance. Overly burdensome technologies encourage traffic to illegal and pirate sites.

Unfortunately, we do not believe SB 1515 meets these criteria and we fear that consumers will at best simply evade the measures, or at worst fall prey to criminals eager to rob and extort them.

The Free Speech Coalition counts many age verification software providers among our members and has engaged a working group of websites, platforms, payment processors, technologists, and business owners to devise workable solutions. Our goal is to provide the greatest degree of reliable age verification with the least amount of risk to the largest number of people. No system will be perfect, but we are confident that we can make significant progress toward keeping children safe online.

We are eager to work with you to find a solution and look forward to discussing the issue further.

Sincerely,

Alison Boden

*Executive Director*

alison@freespeechcoalition.com

**Citations**

1. Santer, N. D., Manago, A., Starks, A., & Reich, S. M. (2021). Early Adolescents' Perspectives on Digital Privacy. In *Algorithmic Rights and Protections for Children*.  
<https://doi.org/10.1162/ba67f642.646d0673>
2. Robb, M.B., & Mann, S. (2023). *Teens and pornography*. San Francisco, CA: Common Sense.  
<https://www.common sense media.org/research/teens-and-pornography>
3. Small, Bridget. (2020) Scam emails demand Bitcoin, threaten blackmail. Federal Trade Commission.  
<https://consumer.ftc.gov/consumer-alerts/2020/04/scam-emails-demand-bitcoin-threaten-blackmail>
4. *Reno v. ACLU*, 521 U.S. 844 (1997)