



September 30th, 2026

Utah Department of Commerce
Division of Consumer Protection
Heber M. Wells Building, 2nd Floor
160 East 300 South
Salt Lake City, Utah 84111

Re: Notice of Proposed Rulemaking R152-78B. Liability for Publishers and Distributors of Material Harmful to Minors Rule:

Dear Director Hass,

I write today on behalf of the Electronic Frontier Foundation (EFF)¹ to respond to the Utah Department of Commerce, Division of Consumer Protection Notice of Proposed Rulemaking (NPRM) to implement SB 73 (2026 General Session), published in the Utah State Bulletin on September 1, 2026.

EFF strongly opposes these proposed rules. Virtual Private Networks (VPNs) are fundamental security tools that protect network traffic, safeguard user anonymity, and shield individuals from malicious actors.

The Division's mandate requiring websites to identify Utah residents using VPNs demands a technical impossibility. By routing internet traffic through intermediary servers, VPNs intentionally obscure a user's actual geographic origin, and present only the server's IP address to destination websites—analogous to using a P.O. Box to maintain physical address privacy. Websites have no reliable, deterministic mechanism to distinguish whether a VPN connection originates from Salt Lake City, Seattle, or Shanghai. The technology simply does not support location-based detection of this nature. Thus, websites subject to this proposed law are left an impossible choice: either cease operation in Utah, or block all VPN users, everywhere, just to avoid legal liability in the state.

By effectively penalizing the use of VPNs and mandating age verification, this framework forces invasive data collection, relies on technically flawed detection methods, and ultimately creates a situation where users must sacrifice their digital security to access protected speech. Some of the major issues present in the proposed rules are as follows:

1. The Danger of Mandated Geolocation Obfuscation Detection (R152-78B-201)

These proposed rules establish an invasive, active data-collection regime that impacts internet users both within Utah and far beyond its borders. The proposed rule compels commercial entities to implement a “commercially reasonable geolocation obfuscation detection system.”

¹ The Electronic Frontier Foundation is a San Francisco-based, non-profit organization that works to protect civil liberties in the digital age. EFF represents more than 35,000 active donors and members, including thousands of supporters in Utah.

This mandate forces websites to actively collect sensitive device and network information on every visitor, including those they previously did not track.

The suggested heuristics for detecting obfuscation are highly unreliable. Latency, for example, is a crude signal influenced by numerous benign factors, including general network conditions, routing protocols, ISP setup, poor cellular coverage, and network congestion. Similarly, device or browser time zones are easy to manipulate and offer no definitive proof of location. Furthermore, the rule's vague directive to analyze “other relevant data transmitted by the device or browser” encourages a dragnet approach to data collection. To determine if a user is *really* in Utah, websites will be forced to scrutinize all traffic, inevitably leading to widespread misclassification and the unwarranted blocking of users both inside and outside the state.

Moreover, individuals anywhere in the world could be swept into this regulatory mandate, subjected to invasive data collection, and misclassified by unreliable detection heuristics. Because a website must first ascertain a visitor's physical location to enforce these restrictions, it must actively inspect and analyze device information from every incoming user, particularly targeting those utilizing privacy-preserving tools like VPNs.

2. Flaws in the Proposed Safe Harbor Provisions (R152-78B-202)

The safe harbor provisions in the proposed rules demand false-positive percentages that are highly infeasible to guarantee. To accurately place users into granular age groups, a system must collect highly specific, exact-age data. No commercially available age verification solutions can provide this degree of specificity in a manner that is safe, reasonable, or privacy-preserving.

Additionally, the proposed appeals process is severely deficient. Simply requiring a commercial entity to provide a “reasonable means by which a Utah user may challenge an incorrect age verification result” is far too vague. This, again, burdens users with no clear appeals process, time frame for resolution, or consequences for the commercial entity.

3. Age Verification Data Retention and Disposal Concerns (R152-78B-203)

Under the proposed rules, a commercial entity must “comply with a consumer's request to delete in accordance with Section 13-61-203”², referencing the consumer’s rights to personal data in the Utah Consumer Privacy Act (UCPA). This framework shifts the burden entirely onto the user, forcing them to jump through administrative hoops and potentially expose even more of their personal identity to a website hosting adult content—just to exercise their right to data deletion under the UCPA. Sensitive information collected for age or location verification should never be stored indefinitely by default.

Under this statutory framework, a business is also not required to delete data unless it can authenticate the request, empowering adult content platforms to demand additional personally identifiable information (such as a legal name, email address, or government ID) to verify

² https://le.utah.gov/xcode/Title13/Chapter61/C13-61-S203_2022050420231231.pdf

ownership of a record. A user who originally accessed a site anonymously or through privacy-preserving tools is thus forced to surrender far more sensitive real-world identity data to exercise their right to data removal. Compounding this threat, the social stigma associated with adult content creates a significant chilling effect, driving users to forgo formal administrative requests out of fear or embarrassment and effectively granting platforms permission to retain detailed user profiles by default.

Furthermore, relying on this framework exposes consumers to severe security risks by sanctioning the prolonged retention of sensitive data. Section 13-61-203 of the UCPA allows entities up to 90 days to fulfill deletion requests and includes broad exemptions for requests deemed "technically infeasible." These provisions risk turning age verification checks into long-term data honeypots. Holding granular location data, device identifiers, and age records for months creates an attractive target for data breaches, leaks, and potential extortion. This approach completely reverses fundamental data minimization principles, which dictate that age and location checks must be processed ephemerally and automatically destroyed the instant an access decision is rendered.

4. Conclusion

VPNs are fundamental security tools that millions of people use to protect their network traffic, obfuscate their location from bad actors, and preserve their anonymity. This NPRM needlessly vilifies essential privacy tools and guarantees a high rate of false positives, ultimately resulting in less online privacy for everyone. When a U.S. state advances policies that mirror the web-censorship tactics of authoritarian governments, the ultimate achievements of such a framework must be seriously questioned. As is the case in heavily censored regions, VPN services and obfuscation tools will simply adapt, making this framework fundamentally unsustainable.

Users should have the right to consent to what information they share online. Classifying adult websites as high-risk environments, while simultaneously mandating that those same websites needlessly collect invasive device and location data, turns genuine privacy concerns into mere compliance theater. We urge the Division to reconsider these rules and prioritize the security and privacy of all web users. If you have any questions or need further clarification, please feel free to reach out to rin@eff.org.

Sincerely,



Rindala "Rin" Alajaji
Associate Director of State Affairs
Electronic Frontier Foundation (EFF)