



September 14th, 2026

Chairman Hughes and Members
Senate Committee on State Affairs
Texas Senate

RE: Written Testimony on Protecting Minors Online

Chairman Hughes and Members of the Committee,

Thank you for the opportunity to provide comments regarding the protection of minors on online gaming platforms.

Online grooming, sexual exploitation, sextortion, predatory communications, and exposure to violent or sexually explicit material are real threats. Parents should not be expected to confront sophisticated digital platforms and determined predators without effective tools or truthful information. Texas has a legitimate role in enforcing its criminal and consumer-protection laws. That role, however, should remain focused on actual harms rather than becoming a justification for universal identity verification, pervasive monitoring, or government control over lawful online activity.

The Committee's charge appropriately recognizes that gaming platforms can operate as more than games. Many now incorporate private messaging, voice and video chat, user-generated content, virtual marketplaces, and communities that connect minors with strangers. Other services, such as Discord, may not primarily be gaming platforms but are deeply embedded in gaming communities. Policy should therefore respond to particular platform features and demonstrated risks rather than relying solely on how a company markets or categorizes its product.

Texas's ongoing litigation against Discord offers a useful case study. The State alleges that Discord publicly represented its platform as safe while relying heavily on self-reported birthdates, allowing broad communications between adults and minors, placing significant responsibility on volunteer moderators, and failing to enable its strongest protections by default. The State's case is not based solely on the fact that criminals allegedly used the platform. Its central claim is that Discord's representations to parents and consumers did not match the design and operation of its product. In July, the State secured an agreed temporary injunction requiring Discord to extend certain age-assurance and default safety protections to Texas users while the lawsuit proceeds. The order does not constitute a final judgment that Discord violated the law, and both parties retain their claims and defenses. Nevertheless, the case illustrates an important distinction for lawmakers: Texas can use existing consumer-protection laws to challenge allegedly deceptive representations and unsafe business practices without presuming that every online user must surrender his identity to the government or a technology company.

The Discord case also highlights the difference between safety features being technically available and safety being the default. A platform may offer content filters, limits on direct messages, friend-request restrictions, server-verification settings, spam controls, activity alerts, or automated moderation tools. Those protections provide little benefit to a child or parent who does not know they exist, cannot understand how to activate them, or reasonably assumes that a service marketed as safe has already enabled them.

Platforms designed for or knowingly serving minors should be expected to make protective settings understandable and readily available. There is also a reasonable argument for applying stronger privacy and communication defaults to known minors, particularly where a platform permits unsolicited contact from unknown adults. Parents should receive clear information about what the platform allows, what protections are enabled, what information is collected, and how settings can be adjusted. Companies should be held accountable when they materially misrepresent those protections.

(Page One)



Lawmakers should remain cautious, however, about converting those expectations into broad age-verification mandates imposed on every user of a general-purpose platform. Verifying whether a user is a minor often requires collecting information from adults as well. Depending on the method, users may be asked to provide government identification, facial images, biometric information, financial records, or other sensitive data before accessing lawful content or communicating anonymously. That collection creates new targets for hackers, identity thieves, commercial profiling, and surveillance. A company cannot lose information it never collected. Once sensitive identifying information is gathered, assurances that it will remain secure or be deleted may provide little comfort after a breach or unauthorized use occurs. Requiring private companies or third-party vendors to assemble databases connecting Texans' identities with their online activities could create harms extending far beyond the original child-safety purpose.

Age verification is also not the same as preventing predatory conduct. An age gate may separate users into categories, but it does not necessarily determine whether an adult is dangerous, whether a minor is using someone else's credentials, or whether communications become exploitative. Lawmakers should not treat the collection of more personal information as proof that children are safer.

Texas has already enacted several major laws regulating online services. The SCOPE Act established new duties concerning minors' use of digital services. The App Store Accountability Act requires age verification and parental consent within the app-distribution ecosystem. Texas has also imposed age-verification requirements on certain websites distributing sexual material harmful to minors. These laws differ in scope, purpose, and constitutional posture, but collectively they represent a significant expansion of state authority over digital activity. Some provisions have already produced constitutional litigation, and important questions remain unresolved. Before adding another overlapping regulatory framework, the Legislature should determine what the existing laws actually require, what data companies are collecting to comply, whether that information is retained or shared, what measurable harms have been prevented, how smaller businesses are affected, and which provisions courts have found constitutionally suspect.

The fact that a law has taken effect does not establish that it is effective. Nor does the existence of continuing harm necessarily prove that government needs another mandate. It may instead reveal shortcomings in enforcement, platform compliance, parental awareness, or the design of the existing law. Legislating repeatedly before prior policies can be evaluated risks creating a fragmented system that gathers more information, imposes greater costs, and burdens lawful speech without meaningfully deterring predators.

The Legislature should also preserve the distinction between parents, platforms, and government.

Parents are the primary decision-makers regarding the applications, games, devices, and communications their children may use. Government can help ensure that parents receive honest information and usable tools, but it should not replace parental judgment with a single statewide determination of what every child may access. Families differ in maturity, circumstances, values, and tolerance for risk. A parent's decision to allow a teenager to use a communication platform should not automatically require every adult user of that platform to prove his identity.

Platforms are responsible for their product designs, public representations, data practices, and responses to reported abuse. A company that markets a service to children or assures parents that strong protections are in place should be expected to honor those claims. Platforms should provide accessible reporting systems, preserve relevant evidence when crimes are reported, cooperate with lawful investigations, and act against accounts used for exploitation or predatory conduct. They should not be permitted to hide unsafe practices behind vague disclosures or shift every burden to parents while advertising their products as safe. Government is responsible for defining prohibited conduct, enforcing the law, protecting due process, and punishing those who exploit children. Grooming, trafficking, stalking, sexual exploitation, and criminal solicitation should remain the central targets. Enforcement should be directed at predators and companies that violate clear legal duties, not at lawful users merely because they communicate privately or anonymously.

If the Legislature considers additional age-assurance requirements, those proposals should be narrowly tailored to demonstrated risks. They should collect the least information necessary, prohibit retention and secondary use, prevent the creation of centralized identity databases, require meaningful security protections, and provide accountability when sensitive information is misused or exposed. Lawmakers should also consider whether less intrusive methods can accomplish the same purpose and whether requirements would entrench the largest platforms by imposing costs that smaller competitors cannot bear.



Texas should avoid treating all digital services alike. A platform deliberately marketed to young children, a general-purpose communications service, an online game with public chat, and a private multiplayer game used among known friends do not present identical risks. Regulation based on specific features and conduct will be more effective and less intrusive than imposing the same identity and content controls across the entire Internet. The Committee should also resist proposals requiring platforms to inspect every private communication in search of potentially harmful content. Such mandates could weaken encryption, normalize mass surveillance, and expose intimate family communications to automated analysis or human review. Protecting children should not require eliminating privacy for everyone, including the children the policy is supposed to protect.

The Texas Liberty Compact similarly calls upon lawmakers to Protect Free Speech and Digital Expression. It recognizes that legitimate concerns involving child safety and harmful conduct do not justify blanket restrictions on lawful platforms or centralized government control over digital access. Consistent with the Compact, Texas should require narrow tailoring, preserve First Amendment safeguards, and prioritize targeted consumer protection over broad speech controls.

For the 90th Legislature, we recommend that lawmakers first evaluate the implementation, effectiveness, data practices, and constitutional consequences of laws already enacted. Any additional legislation should focus on harmful conduct, deceptive representations, unsafe defaults for known minors, parental tools, and the effective enforcement of existing criminal and consumer-protection laws. Broad identification mandates, generalized content controls, and systems requiring routine monitoring of private communications should be rejected.

Public safety, individual privacy, free expression, and parental authority are not mutually exclusive. Texas can protect minors by targeting predators, demanding honesty from technology companies, equipping parents with meaningful information and controls, and holding bad actors accountable. It can do so without constructing a digital identification infrastructure or using child safety as a pretext for expanding government authority over every Texan's lawful online activity.

Thank you for your consideration.

For Liberty, For Texas!

Jeremy D. Kitchen
President | Texas Policy Research Action (TPRA)