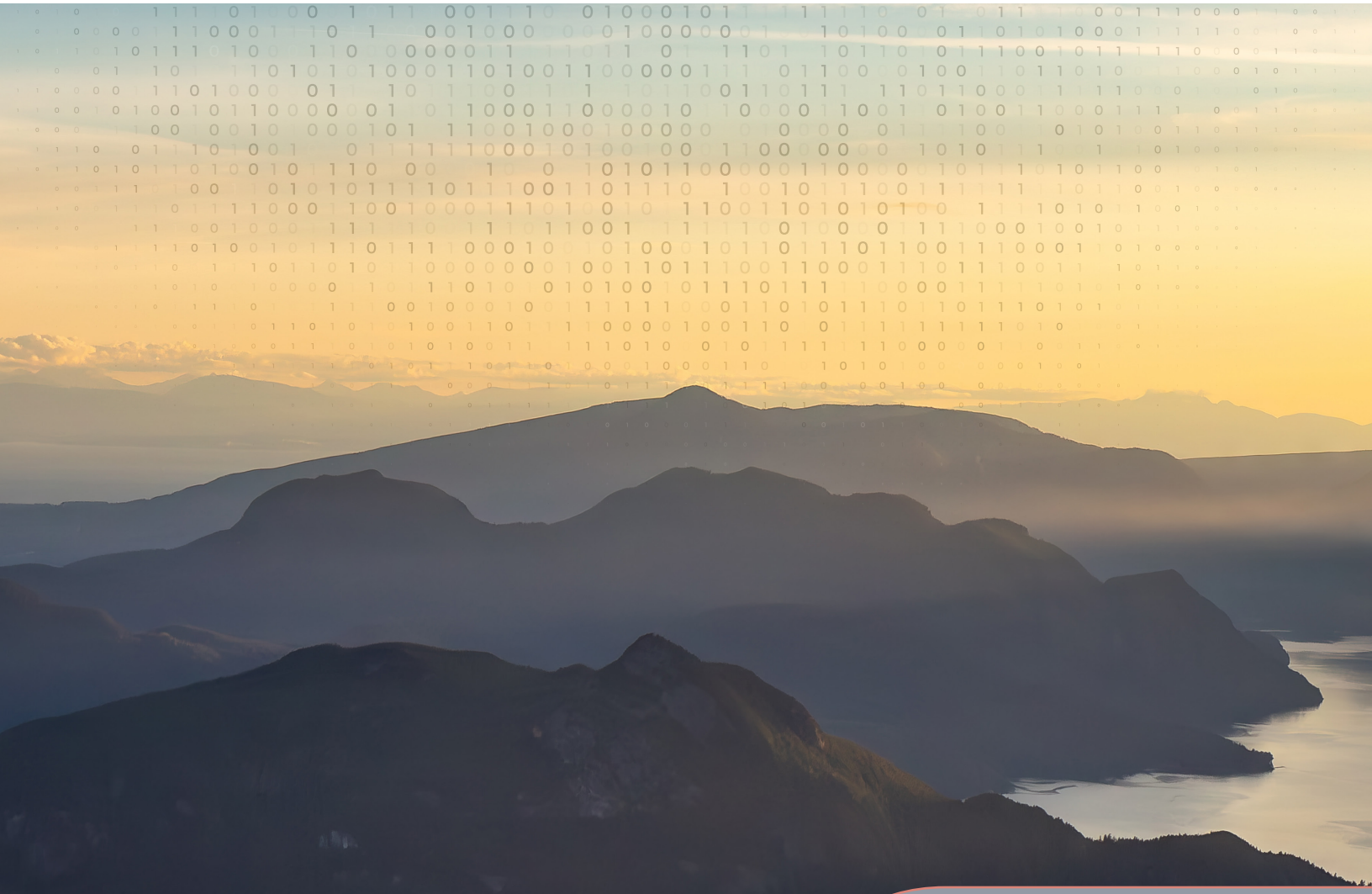
Computer & Communications Industry Association
Open Markets. Open Systems. Open Networks.

ccianet.org

2025

State Landscape
Online Safety



2025 State Landscapes

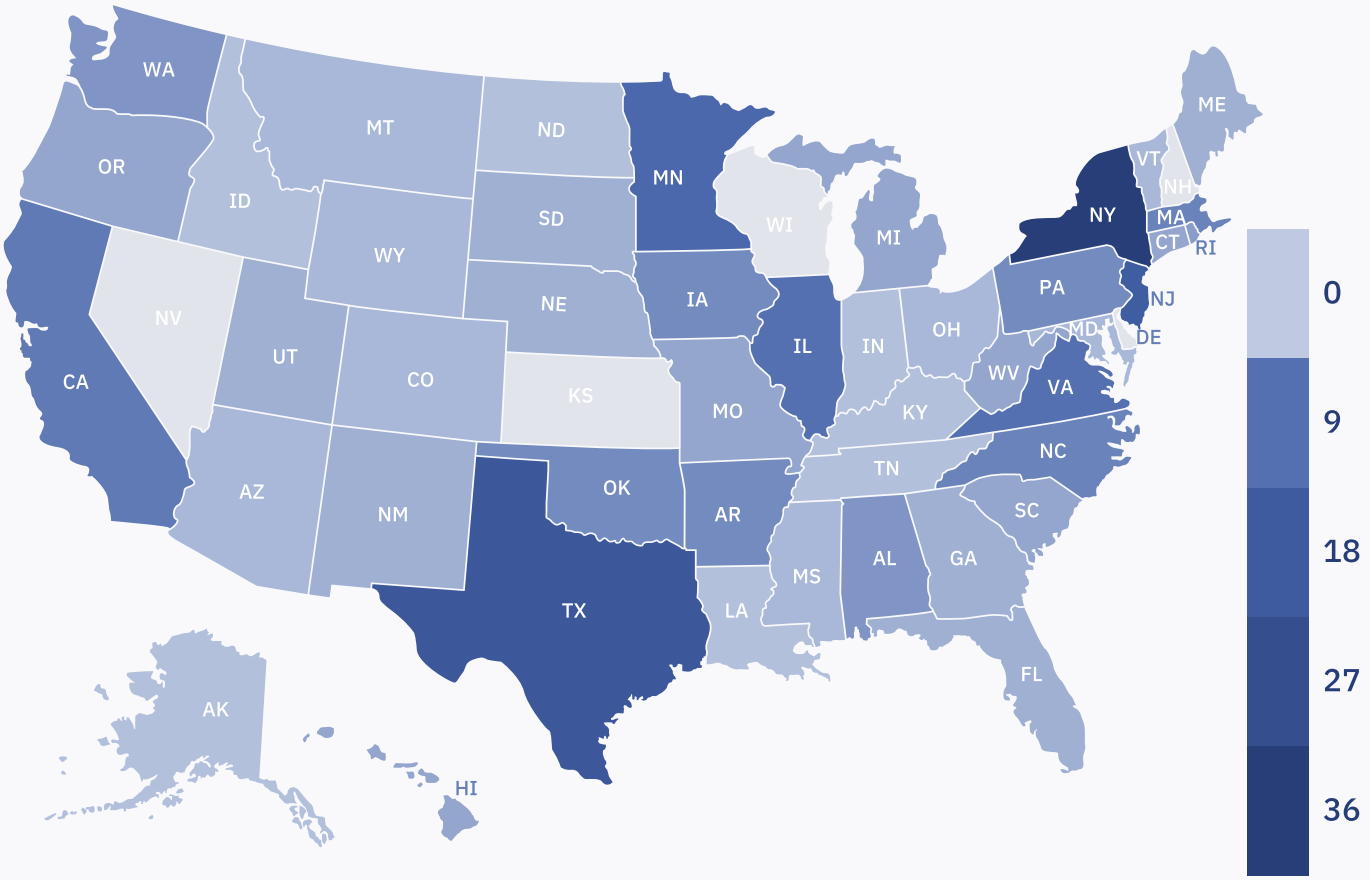
Online Safety

State Landscapes 2025

Each year, the Computer & Communications Industry Association (CCIA) State Policy Center releases a series of policy overviews. These overviews outline major trends across the 50 state legislatures and highlight key states expected to be active in the upcoming session. In recent years, many state legislatures have proposed various laws that would significantly impact the technology industry.

As legislators often borrow or mimic ideas and legislation from other states, observing this year's legislative trends will help predict future policy trends and opportunities for engagement. Such preparedness is particularly essential for policies that could threaten innovation and the tech ecosystem.

State Online Safety Landscape 2025



Includes carryover legislation from 2024 and new legislation in 2025. Data current through 9/30/2025.

Numerous court rulings and state legislative proposals have shaped online safety policy in 2025. While Congress grapples with how best to create a safer online ecosystem, states continue to advance new laws and regulations that attempt to create more guardrails online.

Judicial Developments

Recent federal court rulings on these new laws have sent ripples through the online safety legislative landscapes. *NetChoice v. Bonta* provided another preliminary injunction in March against California's AB 2273 (2022), which required age verification for online services that were "likely to be accessed by children." The ruling highlighted that the government cannot dictate what lawful speech Americans see, interact with, or post online, while posing another necessary check on states' ability to pass Age-Appropriate Design Code (AADC) legislation. *NetChoice v. Griffin* permanently enjoined Arkansas's SB 396 (2023), further enshrining First Amendment rights and restricting states from requiring their citizens to disclose sensitive age verification information to access protected speech. More wins on age verification followed — *NetChoice v. Yost* soon followed the Griffin decision, permanently blocking Ohio's age verification mandate. In Georgia, *NetChoice v. Carr* provided a preliminary injunction against the age verification mandate in SB 351.

These holdings placed several notable restraints on states' ability to institute age verification mandates. *Yost and Carr* reaffirmed that states cannot "prevent children from hearing or saying anything without their parents' prior consent," *Griffin* held that age verification mandates impermissibly burdened the right to anonymous speech, and *Yost and Griffin* held that states cannot regulate websites differently based on vague criteria like their "predominant function" or "primary purpose." *Yost* further affirmed that states cannot differentiate online services differently based on vague or subjective factors such as whether an online service is "likely to be accessed by children" (also affirmed in the *Bonta* AADC case) or considered "established and widely recognized."

While there have been some strong wins in the space, there have also been some losses: In November, an Eleventh Circuit panel stayed the preliminary injunction against Florida's HB 3 in *CCIA v. Uthmeier*, allowing the law's age verification and parental consent provisions to stand during litigation. *NetChoice v. Skrmetti* saw another setback in the legal fight against age verification laws, as a federal district court found that a challenge to Tennessee HB 1891 had failed to show immediate harm. Similarly, in *NetChoice v. Bonta* (not to be confused with the above case of the same name), the Ninth Circuit found that a challenge to California SB 976's age verification requirements was unripe and declined to block the law. The Supreme Court also declined to block Mississippi's age verification law in *NetChoice v. Fitch*, although Justice Kavanaugh's concurrence stated that the challenge was likely to ultimately succeed.

Legislative Developments

2025 has also seen robust legislative activity on online safety. Protecting children from harmful content online has remained a pressing concern for lawmakers, especially over the past five legislative sessions. Digital service providers share this commitment to online safety and are continuously improving their parental tools to better safeguard young users. Today, businesses provide a range of proactive tools at the application, device, and internet service provider (ISP) levels to block inappropriate or dangerous material and create a safer online experience for children.

However, while much of the recent state legislation aims to strengthen online protections for children, it often creates new privacy concerns and bars access to important communities and information online. The rush of AADC legislation has slowed after multiple legal victories, but has not stopped entirely: Nebraska LB 504 and Vermont S 69 were both enacted this year. Illinois, Rhode Island, North Carolina, and Texas also introduced AADC bills that failed to reach their respective Governor's desks.

While CCIA maintains that all forms of age verification are problematic, legislators are debating the most effective means and environment to place the responsibility of age assurance. In 2025, legislators have increasingly attempted to assign this responsibility to application stores. Alabama, Hawaii, California, Louisiana, Michigan, New Jersey, New Mexico, Ohio, Texas, and Utah all introduced legislation that would require some form of app store age verification. Louisiana HB 570, Texas SB 2420, California AB 1043, and Utah SB 142 have since passed and been enrolled. These types of statutes, too, will likely face litigation. In fact, CCIA just filed a first-ever First Amendment challenge to Texas's SB 2420 establishing app store age verification requirements.

Lawmakers continue to introduce increasingly intrusive mandates, such as for default "content filters" on smartphones and tablets, which are often technologically unworkable. These laws raise significant concerns about data privacy, unrestricted access to online information, and government overreach. While framed as efforts to prevent minors from accessing pornography and other digital services that lawmakers deem inappropriate, they would limit internet access more broadly and impose child-specific controls on devices frequently purchased by adults. Existing tools, including parental settings and controls, already address many of these safety concerns without infringing on the online freedoms of others.

Given the steady momentum across state legislatures to create new online safety legislation, in Democrat- and Republican-led states alike, states will almost certainly continue to advance online safety laws. Such laws will likely cover devices, application stores, digital service providers, and ISPs, and all members will likely be impacted. It remains to be seen whether these new laws will align with existing frameworks or diverge and further fragment the regulatory landscape, complicating businesses' efforts to comply. CCIA will remain deeply involved in the state legislative process across all 50 states to ensure that members' voices are heard and considered during these policy discussions.

Types of State Online Safety Measures

1 Age Verification

In 2025, several states enacted laws requiring digital services to implement age verification measures. These laws often require collecting additional personal information such as uploading a driver's license, credit card, or parental consent documentation to verify users' ages. While some third-party vendors offer verification services, none have proven capable of delivering a solution that is reliable, broadly accessible, and protective of individual privacy, data, and security. At least 24 states have enacted some form of age verification law, but many now face constitutional challenges, particularly around free speech and due process.

Examples:

- UT SB 142
- TX SB 2420
- CA AB 1043
- LA HB 570

CCIA Engagement:

CCIA Veto Request on LA HB 570, CCIA Comments on MA S 335, CCIA Comments on MA H 666, CCIA Comments on OH HB 226, CCIA Veto Request Letter on TX SB 2420, CCIA Public Comments on TX HB 186, CCIA Written Comments on NV SB 63, CCIA Written Veto Request on CO SB25-086, CCIA Written Comments on CO HB25-1287, CCIA Written Comments on NM HB 313, CCIA Written Comments on AL SB 187, CCIA Written Comments on AL HB 317, CCIA Written Comments on WA HB 1834, CCIA Written Comments on UT SB 142, CCIA Written Comments on VA SB 854, CCIA Written Comments on SD SB 180, CCIA Written Comments on AK HB 46, CCIA Written Comments on SC HB 3405

Impact:

In practice, verifying users' age and residency online would require businesses to collect additional sensitive information such as government IDs, geolocation data, or other personal details, undermining data minimization principles and increasing privacy risks for both children and adults. These requirements may also compel parents or guardians to submit financial or personal data to consent on behalf of minors. Moreover, mandatory age verification can chill lawful speech and access to information, thus infringing on the First Amendment right to anonymous speech.

Age-Appropriate Design Code/Age Estimation

In 2022, California Governor Gavin Newsom signed AB 2273, the "Age-Appropriate Design Code" (AADC), into law. Based on the United Kingdom's AADC, this framework has been introduced in other states, with Maryland following suit in 2024 and now Nebraska and Vermont have both enacted their own forms of AADC laws. There have been many legal challenges around this concept. The AADC requires businesses offering online services likely accessed by children to "estimate the age of child users with a reasonable level of certainty." To comply, some third-party vendors offer age estimation services using facial analysis and technological means. These technologies are not fully accurate, and risk classifying adults as minors, or vice versa.

Examples:

- NE LB 504
- VT S 69

CCIA Engagement:

CCIA Written Comments on NE LB 504, CCIA Written Comments on VT H 210, CCIA Written Comments on IL SB 50, CCIA Written Comments on RI H 5830, CCIA Written Comments on SC S. 268, CCIA Comments on VT S 69, CCIA Comments on SC HB 3431, CCIA Veto Request Letter on VT S 69, CCIA Comments on GA Senate Subcommittee

Impact:

There are serious concerns about how third-party age estimation vendors collect, store, and use personally identifiable information (PII), including the use of facial recognition technology. Because age estimation is not entirely accurate, businesses may feel compelled to instead use age verification to ensure compliance with legal requirements. This creates additional costs for large, medium, and small businesses alike, particularly when adapting to the complex obligations of an Age-Appropriate Design Code. Furthermore, mandates such as conducting a "data protection impact assessment" (DPIA) before launching new features could inadvertently stifle innovation and limit free expression online.

Child Sexual Abuse Material (CSAM)/Nonconsensual Deepfakes

Child sexual abuse material (CSAM) is illegal and must be removed from all websites immediately upon discovery. Many services work closely with the National Center for Missing and Exploited Children (NCMEC) and use advanced AI and hash-matching technology to identify and prevent the spread of this content. Legislation banning explicit deepfakes, especially those involving minors, has been enacted across the country. While these measures mark progress, the need to combat CSAM remains a collective responsibility that requires ongoing vigilance and innovation. Legislators have begun including all pornographic deepfake technologies regardless of age in their bills as they prioritize cracking down on nonconsensual intimate deepfakes (NCID). More states will likely follow in 2026.

CSAM Examples:

- MS HB 599
- WV SB 198
- TX SB 20
- TX HB 581
- NV SB 263
- NE LB 383

NCID Examples:

- MI HB 4047
- TX HB 3133
- FL SB 1400
- CA AB 621

CCIA Engagement:

TechNet Led Coalition Letter on CA AB 1137, CCIA Veto Request on NE LB 383

Impact:

These policies often fail to consider the practical capabilities of stakeholders, rendering many compliance requirements unrealistic for online businesses. They also place liability on websites rather than on the individuals who create or distribute CSAM content. This approach frequently neglects to address the bad actors creating and distributing the content– neglecting to combat the core issue while blaming the services trying their best to moderate is an inherently flawed solution.

4 Parental Consent/Access

Some proposals would require anyone under 18 to get a parent or guardian's permission before creating a social media account or accessing certain features. Suggested ways to confirm the parent-child relationship include parents providing a government-issued ID, signing and returning a consent form, or calling or video conferencing with a central office. Laws like these have already been passed in some states, but they are increasingly facing legal challenges over constitutional concerns. For example, CCIA's suit against Texas's SB 2420 also challenges the parental consent provisions in the Act, as well as its age verification requirements.

Examples:

- LA HB 37
- NE LB 383
- VA SB 854

CCIA Engagement:

CCIA Written Comments on VA SB 783, CCIA Veto Request on VA SB 854, CCIA Written Comments on NV SB 63, CCIA Written Comments on AR HB 1717, CCIA Written Comments on FL SB 1438, CCIA Written Comments on SC HB 3431, CCIA Veto Request on NE LB 383, CCIA Comments on MA H 666, CCIA Comments on MA S 335

Impact:

Forcing online services to collect more data about minors and their parents conflicts with data minimization principles ingrained in standard federal and international privacy and data protection compliance practices. Determining a user's age and verifying parental consent inherently requires collecting additional sensitive data from those users, and any document capable of verifying a user's age will likely contain sensitive information. Additionally, not all minors will have a parent or guardian who can provide verifiable consent (such as adopted children, children in foster care, or those whose parents have remarried). Excessive monitoring has also been shown to negatively affect young people's mental health and development.

Additionally, as discussed above, many federal courts have blocked mandatory parental consent laws on First Amendment grounds, as they impose content-based barriers to protected speech on both children and adults. Two federal courts ruled this year that governments lack "the power to prevent children from hearing or saying anything without their parents' prior consent."

5 Device Filtering

These bills mandate that manufacturers of internet-connected smartphones and tablets automatically activate a filter designed to block access to online material classified as "harmful to minors," commonly referred to as an "obscenity filter." If a manufacturer fails to comply and a minor gains access to such material, the device manufacturer can face penalties including civil fines for each device sold without the filter pre-enabled.

Examples:

- AL SB 186
- CA SB 50
- ID S 1158 *(Failed)*

CCIA Engagement:

CCIA Written Comments on SC HB 3399, CCIA Written Comments on NH HB 293, CCIA Written Comments on ID S. 1158, CCIA Veto Request on Alabama SB 186, CCIA Comments on NH HB 293, CCIA Comments on NH HB 293 for Subcommittee

Impact:

Requiring a state-specific default filter would create substantial technical hurdles for businesses. Since internet service providers (ISPs) generally determine which websites users can access, it is unclear how such a mandate would work for devices without precise location tracking or those that connect solely through Wi-Fi. Such laws also fail to specify manufacturers' obligations regarding devices purchased online from other states or through the secondary market. Moreover, mandatory device filters would deny users and their guardians the ability to tailor content and service settings to their individual preferences.

6 Social Media Warning Labels

Social media warning labels are designed to interrupt users' experience with clear, unavoidable reminders about potential risks tied to prolonged or harmful use. Modeled after public health warnings on products like tobacco, these labels are typically displayed prominently, using bold text or large screen takeovers to stress concerns such as mental health impacts, misinformation, or addictive design. The intent is to raise awareness and prompt more cautious engagement, though some critics see them as more symbolic than effective.

Examples:

- NY A 5346
- MN HF 2
- CA AB 56

CCIA Engagement:

TechNet Led Coalition Letter on CA AB 56, CCIA Veto Request on NY A 5346, CCIA Public Comments on NY A 3411, CCIA Public Comments on NY A 5346

Impact:

The impact of social media warning labels appears largely ineffective, with mounting evidence suggesting they fail to meaningfully alter user behavior while potentially creating a false sense of security. Users quickly develop "warning fatigue," reflexively dismissing these alerts much like cookie banners or pop-up advertisements, rendering them virtually invisible to habitual social media users who scroll past without genuine consideration. Despite these significant limitations, proponents argue that warning labels can raise some awareness about digital well-being risks and may encourage more thoughtful conversations between parents and children about social media use.

7 Duty of Care to Prevent Harm and Liability

These bills aim to regulate online speech by targeting digital services' designs, algorithms, or features that "know or reasonably should have known" might cause harm to children. Such harms are defined to include risks like self-harm, eating disorders, or social media "addiction." Many proposals also require services to conduct "audits," meaning systematic reviews of both existing and planned features to identify potential violations and plans to address potential risks. Violators may face large monetary penalties for any alleged infraction.

Examples:

- CA SB 771 *(Failed)*
- LA HB 37
- MT SB 297

CCIA Engagement:

CCIA Comments on CA AB 2, CCIA Veto Request on AR SB 612, TechNet Led Coalition Letter on CA SB 771, CCIA Veto Request on LA HB 37

Impact:

Protecting children online should not provide governments with unrestricted authority to limit information access. When legislation employs vague language and enables private litigation, companies face strong incentives to exclude minors entirely rather than risk costly legal proceedings and substantial penalties. Speech restrictions should not be justified under the guise of child protection, nor should state authorities determine what information young people may access. Given the absence of medical consensus on potential harms and significant individual variation in responses, companies cannot reliably evaluate what content may be detrimental. Additionally, these legislative proposals fail to account for the content moderation systems and other online safety mechanisms that websites have already implemented.

8 Digitial Stewardship and Online Safety Education

Typically a bipartisan policy, digital citizenship bolsters industry efforts to support youth safety and privacy online by providing educational curricula focused on how to be a good online citizen. This policy provides a more holistic approach to fostering children's online safety by teaching students how to properly identify standards of appropriate, responsible, and healthy online behavior, including cyberbullying prevention and response. This type of curriculum also teaches social-emotional skills like empathy, kindness, and personal responsibility to enhance online interactions. Many of these safety demonstrations also offer parents the opportunity to listen in and attend workshops, helping them better understand the safety features available and how to effectively guide their children in an online environment.

Examples:

- IL SR 5
- AL HB 166
- TN HB 825
- VA HB 2460

Impact:

Given the complexity of these issues, pairing existing industry safeguards with educational programs on responsible online behavior can deliver real benefits. Social media and other digital services provide immense value by helping people stay connected, pursue education, and access vital resources. This makes it even more important to teach young people how to navigate these spaces wisely. Empowering them with the skills to manage risks is far more effective than simply restricting access. By building awareness of potential harms and practical strategies to address them, we can prepare young users to participate safely and productively in the digital world, which is increasingly central to both the economy and the modern workforce.

Key States

California

California has consistently led the nation in proposals to regulate digital services. In 2025, CCIA tracked nearly 60 new bills in the state aimed at governing various aspects of the digital ecosystem. This year, California lawmakers passed significant measures addressing children's online safety, data privacy, and artificial intelligence. The California Privacy Protection Agency will likely continue proposing online safety regulations. While some of these initiatives raised concerns around Constitutionality and federal preemption, state lawmakers are expected to advance similar proposals in 2026.

Florida

While CCIA achieved a significant victory in federal court with the granting of a preliminary injunction suspending the ban on 14-year-olds from having accounts on several widely used online services in its challenge to Florida's HB 3 (2024), an Eleventh Circuit panel stayed the injunction in November and allowed the law to remain in place during litigation. Florida's legislative activity on digital services was relatively limited this year, with only two bills CCIA tracked passing; both focused on the removal of sexually explicit content. Despite the slower pace, Florida is expected to remain an important player in the digital services landscape in 2026.

Louisiana

Louisiana was one of the busiest states in the country regarding online safety. The legislature passed an application store age verification bill, HB 570, containing age verification and parental consent provisions. It also passed HB 37, which created a new duty of care for digital services that contract with children under 16. Lawmakers in Louisiana will continue to push new online safety legislation.

Montana

Montana has been especially active in the digital space, often positioning itself at the forefront of state-level efforts to address how digital services govern speech and information. Lawmakers have advanced measures aimed at increasing transparency, creating liability for moderation practices, and adding more legislative safeguards for user content. Montana has sought more active oversight of the digital environment, and its policy approaches may influence debates well beyond the state's borders.

Key States

Texas

Texas passed SB 2420, one of many app store bills with age verification and parental consent provisions passed across the country. On October 16, 2025, CCIA sued Texas in the U.S. District Court for the Western District of Texas seeking to enjoin nearly all of SB 2420 under the First Amendment and Commerce Clause of the U.S. Constitution. Texas also actively combatted CSAM online, with a particular focus on deepfake technology.

Utah

The Utah Legislature took big swipes at online safety legislation in 2025. The Legislature passed SB 142, one of the nation's first app store level bills with age verification and parental consent provisions. They later proposed HB 418, the first of several state attempts to require data interoperability. The state appears poised to continue introducing ideas that could become popular across the country.

Vermont

In 2024, the Vermont Legislature advanced a version of an Age-Appropriate Design Code bill (H.121) that garnered wide support in both houses, but ultimately failed because of Senate objections to the comprehensive privacy bill paired with it. However, after separating the two bills, Vermont was able to pass a revised version of the AADC law, Vermont S 69, in 2025, and may look to build on this effort in 2026.

Virginia

Virginia passed a number of laws regarding online safety, including SB 854, which revived the state's 2024 efforts to require age verification, parental consent, and set time limits for minors on covered websites. There was also a strong focus on cracking down on digital replicas; however, Governor Youngkin vetoed two of these measures. The Governor was not afraid of using his veto powers this Legislative Session, so the legislature will likely take up these initiatives again in 2026.

Litigation Likely to Drive State-Level Discourse

Arkansas

Summary:

***NetChoice v. Griffin* (2023):** In June 2023, NetChoice filed suit against the Arkansas Attorney General over a children's online safety law, Act 689, arguing that the law violates the First Amendment and other provisions of the Constitution. The law required age verification and parental consent for covered websites.

***NetChoice v. Griffin* (2025):** In June 2025, NetChoice again filed suit to block a new online safety bill, Act 901, which created a private right of action against online services whose design features "facilitated the immediate connection" between minors and various types of content designated as harmful. The law also imposed civil penalties against such services.

Status:

***NetChoice v. Griffin* (2023):** On March 31, 2025, the U.S. District Court for the Western District of Arkansas ruled for NetChoice that the law is indeed unconstitutional and permanently blocked Act 689 from being enforced. The state appealed, and the case is now pending in front of the U.S. Court of Appeals for the Eighth Circuit.

***NetChoice v. Griffin* (2025):** NetChoice's challenge to Act 901 is currently pending in the Western District of Arkansas.

California

Summary:

***NetChoice v. Bonta* (California Speech Code):** In December 2022, NetChoice filed suit against the California Attorney General over a children's online safety bill, AB 2733, arguing that it violates the First Amendment, Fourth Amendment, Due Process, Commerce Clause, and the Supremacy Clause.

***NetChoice v. Bonta* (SB 976):** In November 2024, NetChoice again sued California regarding a different online safety bill, SB 976, on First Amendment grounds. The bill required covered online services to obtain parental consent before they provide "addictive feeds" to minors, show the number of likes on minors' posts, or turn off the private setting on a minor's account.

Status:

***NetChoice v. Bonta* (California Speech Code):** On March 13, 2025, the U.S. District Court for the Northern District of California once again granted NetChoice's request for a full preliminary injunction against AB 2733, misleadingly titled the "CA AADC." The law compels websites and digital services to serve as roaming online censors for the state and introduces significant cybersecurity risks for Californians and their families. California has appealed this ruling to the U.S. Court of Appeals for the Ninth Circuit.

***NetChoice v. Bonta* (SB 976):** On September 9, 2025, the Ninth Circuit partially reversed the preliminary injunction NetChoice had obtained against SB 976 in January. The Ninth Circuit enjoined the regulation of like counts but allowed the other challenged provisions to stand during litigation. NetChoice has moved for a rehearing *en banc*.

Colorado

Summary:

NetChoice v. Weiser: In August 2025, NetChoice filed suit against Colorado's Attorney General over a social media warning label bill, HB 24-1136, arguing that the legislation infringes on First Amendment protections and violates sections of federal law.

Status:

NetChoice v. Weiser: The case is pending before the U.S. District Court for the District of Colorado.

Florida

Summary:

CCIA v. Uthmeier: CCIA has challenged Florida's HB 3 for broadly infringing on First Amendment rights of both minors, adults, and websites whose content is being targeted. The bill would require covered online services to ban users under 14, require parental consent for users aged 14-15, and terminate the accounts of users under 16 upon parental request. CCIA won a partial injunction to prevent the most objectionable provisions of HB 3 from becoming effective on January 1, 2025.

Status:

CCIA v. Uthmeier: In June 2025, Judge Walker granted our requested injunction against several provisions, including banning 14- to 15-year olds from having accounts without parental consent and banning all minors under 14. However, on November 25, 2025, the United States Court of Appeals for the Eleventh Circuit halted the preliminary injunction, allowing the law to remain in place during litigation.

Georgia

Summary:

NetChoice v. Carr: On May 1, 2025, NetChoice filed suit in the U.S. District Court for the Northern District of Georgia challenging SB 351 on First Amendment grounds. The law would require covered websites to institute age verification and to require parental consent for users under 16.

Status:

NetChoice v. Carr: On June 26, 2025, the District Court issued a preliminary injunction against the law, finding that its age verification and parental consent requirements "cannot comport with the free flow of information the First Amendment protects."

Louisiana

Summary:

NetChoice v. Murrill: On March 18, 2025, NetChoice filed a complaint seeking to block Louisiana SB 162 on First Amendment grounds. The law would require covered online services to implement age verification and parental consent mechanisms.

Status:

NetChoice v. Murrill: On December 15, 2025, the law was permanently enjoined.

Maryland

Summary:

NetChoice v. Brown: On February 3, 2025, NetChoice filed a complaint seeking to block Maryland's Age-Appropriate Design Code Act on First Amendment grounds. The law would mandate certain design features and default settings for online services that were "reasonably likely to be accessed by minors."

Status:

NetChoice v. Brown: The case is currently pending before the the U.S. District Court for the District of Maryland.

Mississippi

Summary:

NetChoice v. Fitch: On June 7, 2024, NetChoice filed a complaint in the U.S. District Court for the Southern District of Mississippi, seeking a preliminary injunction to block HB 1126. This law not only mandates age verification and parental consent for digital services—violating privacy and restricting the free exchange of ideas—but also includes a unique provision with sweeping content moderation requirements that could lead to extensive online censorship.

Status:

NetChoice v. Fitch: On August 14, 2025, the Supreme Court declined to block the Mississippi social media age-verification law. In a ruling following an emergency petition, the Justices denied NetChoice's request to reinstate the lower court's order against the law. However, Justice Kavanaugh's concurrence that while "NetChoice has not sufficiently demonstrated that the balance of harms and equities favors it at this time," HB 1126 "is likely unconstitutional."

Ohio

Summary:

NetChoice v. Yost: On January 5, 2024, NetChoice filed a complaint in the District Court for the Southern District of Ohio against the Social Media Parental Notification Act, alleging that the law violated the First and Fourteenth Amendments. The law required parental consent for users under 16 to access covered online services.

Status:

NetChoice v. Yost: On April 16, 2025, Judge Marbley granted a permanent injunction against the Social Media Parental Notification Act. Marbley was clear that the intention of the bill was noble, but that the Ohio Legislature must try to achieve this goal through Constitutional means. He also noted that "nearly all of the research showing any harmful effects" for minors on social media "is based on correlation, not evidence of causation." Ohio has appealed this ruling to the United States Court of Appeals for the Sixth Circuit.

Tennessee

Summary:

NetChoice v. Skrmetti: NetChoice is seeking to block HB 1891, a law requiring parental consent and age verification for covered online services.

Status:

NetChoice v. Skrmetti: On June 20, 2025, the US District Court for the Middle District of Tennessee denied NetChoice's request for a preliminary injunction. The court's opinion highlighted that the Plaintiff did not establish enough requirements for a preliminary injunction, specifically the point that they failed to demonstrate that anyone will suffer irreparable harm if no injunction is granted. NetChoice has appealed this ruling to the Sixth Circuit.

Texas

Summary:

NetChoice v. Paxton: Along with NetChoice, CIA is challenging Texas HB 20, which attempts to prevent certain websites from moderating the content on their service.

***CCIA v. Paxton* (2024):** CCIA is also challenging Texas HB 18, the Securing Children Online Through Parental Empowerment (SCOPE) Act, which attempts to age-gate the internet.

***CCIA v. Paxton* (2025):** CCIA is also the plaintiff in a challenge to Texas's SB 2420, also known as the App Store Accountability Act, which requires app stores and app developers to verify the ages of users and ensure that minor users obtain parental consent for downloads and in-app purchases. In addition, SB 2420 mandates that app developers rate the age-appropriateness of their apps and that app stores display these ratings, among others.

Status:

NetChoice v. Paxton: In August 2025, CCIA filed a Second Amended Complaint in the U.S. District Court for the Western District of Texas seeking to permanently enjoin HB 20. The Supreme Court sent this case back to the Texas courts after finding that "The government may not, in supposed pursuit of better expressive balance, alter a private speaker's own editorial choices about the mix of speech it wants to convey". CCIA expects this case to play out in the remainder of 2025 and potentially into 2026. The case is currently on remand in the Western District of Texas.

***CCIA v. Paxton* (2024):** In August 2024, CCIA filed another suit in the Western District of Texas seeking a preliminary injunction of HB 18. On August 30, Judge Pitman partially granted that motion, enjoining the provision of HB 18 requiring monitoring, filtering, and blocking of online content. Texas has appealed that decision to the U.S. Court of Appeals for the Fifth Circuit. Oral argument was held on November 3, 2025.

***CCIA v. Paxton* (2025):** On October 16, 2025, CCIA filed a third suit in the Western District of Texas seeking a preliminary injunction to halt the violative portions of SB 2420. The case has been assigned to Judge Robert Pitman, who is also overseeing the litigation against HB 20 and HB 18.

Utah

Summary:

NetChoice v. Brown: In May 2024, NetChoice filed suit in the U.S. District Court for the District of Utah to block implementation of the Utah Minor Protection in Social Media Act on First Amendment grounds. The law required covered online services to institute an age assurance mechanism and obtain parental consent before processing minor's data.

Status:

NetChoice v. Brown: The District Court granted a preliminary injunction against the law in September 2024. Utah has appealed this ruling to the U.S. Court of Appeals for the Tenth Circuit.

Virginia

Summary:

NetChoice v. Miyares: In November 2025, NetChoice filed suit to block SB 854 on First Amendment grounds. The law, which is scheduled to take effect on January 1, 2026, would require covered online services to verify every user's age and prohibit any user under 16 from accessing social media sites for more than an hour a day without parental consent.

Status:

NetChoice v. Miyares: The case is currently pending before the U.S. District Court for the Eastern District of Virginia.

2025 State Landscape
Challenges Presented by Proposed Bills

U.S. Constitutional and Federal Preemption

While safeguarding children online is an admirable objective, such protection cannot serve as broad justification for censoring ideas or content. The mere fact that lawmakers consider certain speech or images inappropriate for minors does not permit its suppression, provided that content is not obscene to children or otherwise prohibited by valid legal restrictions. These legislative proposals, despite their well-intentioned goal of protecting young internet users, present significant constitutional challenges under the First Amendment and create complications regarding Section 230 protections.

Litigation Costs

At least fifteen online safety bills are currently being challenged in court. Reporters in 2022 found that Florida alone had spent around $3 million litigating a single case—before the U.S. Supreme Court had even granted certiorari. Third-party estimates from 2021 for Texas' legal costs defending its unconstitutional statute are at least $1 million as well. Lawmakers should avoid enacting bills that will not only make the internet less safe but will waste millions of taxpayer dollars in litigation fees.

Regulatory Consistency

Online businesses require consistent and predictable regulatory frameworks that operate uniformly across the country. When state and local governments implement vague or conflicting regulations, businesses cannot be certain of their legal obligations. Such fragmented regulatory approaches can discourage new companies from entering the market, ultimately reducing competition and harming consumer interests. Small businesses face the greatest consequences, as they often cannot afford to navigate fifty separate regulatory schemes. To address these concerns, state legislators should ensure that their proposals are compatible with existing federal regulations and other states' frameworks. This approach promotes regulatory compatibility, reduces compliance costs, and helps consumers better understand their legal protections.

Establish a Risk-Based Approach

Effective online child safety legislation should adopt a risk-assessment framework that tailors protections to specific age groups. The cognitive development, emotional maturity, and life experiences of younger teenagers differ dramatically from those of older adolescents—a 13-year-old and a 17-year-old have fundamentally different capacities and needs. Requiring all websites to accommodate the youngest possible users across every age bracket may prove unrealistic and impractical to implement.

Target Specific Harms

It is crucial to enact legislation targeting tangible harms, as abstract definitions of "harms" may inadvertently encompass content, such as world news or historical art, that is not universally harmful to young users. Affixing these poorly defined terms to private rights of action open state courthouses to plaintiffs advancing frivolous claims with little evidence of actual injury. Such claims will disproportionately impact smaller businesses, as they can bear fewer litigation costs.

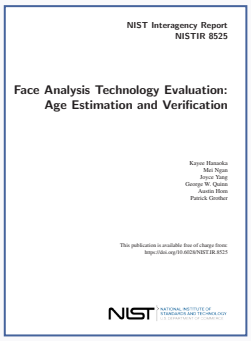
Collected Analysis

DTSP Safe Framework Specification

June 2025 | The Digital Trust & Safety Partnership (DTSP)

The full report is available here.

The Safe Framework Specification was formally published as an international standard. DTSP was created to help standardize digital services' response to online harms, as existing rigid regulatory methods were often either too broad, too narrow, or counterproductive While other fields like information security had flexible, adaptable frameworks, but trust and safety lacked sufficiently concrete standards that organizations could tailor to their specific contexts and risks. The Safe Framework Specification aims to balance reducing harmful content and behavior with preserving users' fundamental rights to expression, commerce, and community participation.



Face Analysis Technology Evaluation: Age Estimation and Verification

July 2025 | National Institute of Standards and Technology (NIST)

The full report is available here.

NIST updated a study assessing the accuracy of software designed to estimate a person's age based on facial characteristics in photos. The study evaluated six algorithms voluntarily submitted by developers following a call for submissions in September 2023 and has now been updated with four new algorithms.

The new study continues NIST's first venture into age estimation verification (AEV) evaluation. NIST seeks to further update the study in late 2025.