The Florida Senate

BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Committee on Commerce and Tourism

BILL:	SB 1722
INTRODUCER:	Senator Calatayud
SUBJECT:	Application Stores
DATE:	Febuary 3, 2026
REVISED:	

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	McMillan	McKay	CM	**Favorable**
2.			JU	
3.			RC	

I. Summary:

SB 1722 creates the "App Store Accountability Act," which requires application (app) store providers and developers to implement certain age verification and parental consent requirements for minors using such apps. Additionally, app stores and developers are required to protect user data.

A minor who has been harmed by a violation of the provisions in the bill, or such minor's parent, may bring a civil action against an app store provider or a developer. Further, a violation of the provisions in the bill is an unfair and deceptive trade practice actionable under part II of ch. 501, F.S., by the Department of Legal Affairs.

The bill takes effect on July 1, 2027.

II. Present Situation:

Application (App) Store Laws

Some states including Texas,[1] Utah,[2] and Louisiana[3] have passed laws to require app stores and developers to verify user age upon creating an account, as well as require verifiable parental consent for minors before they can download apps or make (in-app) purchases.[4]

In December of 2025, the United States District Court in the Western District of Texas granted preliminary injunctions in two cases blocking enforcement of the state's App Accountability Act

[1] *See* Tex. Bus. & Com. Code § 121.001 et seq.
[2] *See* Utah Code Title 13, Chapter 76.
[3] *See* Part II of Chapter 20-A of Title 51 of the Louisiana Revised Statutes (R.S. 51:1771 through 1775).
[4] *See* Tex. Bus. & Com. Code § 121.001 et seq., Utah Code Title 13, Chapter 76, and Part II of Chapter 20-A of Title 51 of the Louisiana Revised Statutes (R.S. 51:1771 through 1775).

that was scheduled to take effect on January 1, 2026.[5] The court found that the law is likely an unconstitutional restriction on free speech.[6] The Texas attorney general has filed a notice of appeal to the Fifth Circuit.

Florida's Age Verification Law

In 2024, the Legislature enacted laws to require age verification for online access to materials that are harmful to minors.[7]

Florida law requires a commercial entity that knowingly and intentionally publishes or distributes material harmful to minors on a website or application, if the website or application contains a substantial portion of material harmful to minors to use either anonymous age verification or standard age verification to verify that the age of a person attempting to access the material is 18 years of age or older and prevent access to the material by a person younger than 18 years of age.[8]

"Standard age verification" means any commercially reasonable method of age verification approved by the commercial entity.[9]

Any violation of the age verification law is deemed an unfair and deceptive trade practice, and the Department of Legal Affairs (department) has enforcement authority. In addition to the remedies under the Florida Deceptive and Unfair Trade Practices Act, the department may collect a civil penalty of up to $50,000 per violation and reasonable attorney fees and court costs for a violation by a third party.[10] A commercial entity that violates the age verification requirement is liable to the minor for such access, including court costs and reasonable attorney fees as ordered by the court. Claimants may be awarded up to $10,000 in damages. A civil action for a claim under this paragraph must be brought within 1 year from the date the complainant knew, or reasonably should have known, of the alleged violation.[11]

Florida law defines the term "anonymous age verification" as a commercially reasonable method used by a government agency or a business for the purpose of age verification which is conducted by a nongovernmental, independent third party organized under the laws of a state of the United States which:

- Has its principal place of business in a state of the United States; and
- Is not owned or controlled by a company formed in a foreign country, a government of a foreign country, or any other entity formed in a foreign country.[12]

A third party conducting anonymous age verification:

---

[5] *See Students Engaged in Advancing Texas cv. Paxton,* 2025 WL 3731733 (W.D. Tex. 2025). *See also Computer & Communications Industry Association v. Paxton,* 2025 WL 3754045 (W.D. Tex. 2025).
[6] *See id.* Additionally, the court found the law to be unconstitutionally vague.
[7] Ch. 2024-42, Laws of Fla.
[8] Section 501.1737, F.S.
[9] Section 501.1737, F.S., defines "commercial entity" as a corporation, a limited liability company, a partnership, a limited partnership, a sole proprietorship, and any other legally recognized entity.
[10] *Id.*
[11] *Id.*
[12] Section 501.1738, F.S.

- May not retain personal identifying information used to verify age once the age of an account holder or a person seeking an account has been verified;
- May not use personal identifying information used to verify age for any other purpose;
- Must keep anonymous any personal identifying information used to verify age; and
- Must protect personal identifying information used to verify age from unauthorized or illegal access, destruction, use, modification, or disclosure through reasonable security procedures and practices appropriate to the nature of the personal information.[13]

Protection of Children in Online Spaces Law

Florida law provides that any online service, product, game, or feature likely to be predominantly accessed by children under 18 years of age may not, except under certain situations:

- Process the personal information of any child if the platform has actual knowledge or willfully disregards that the processing may result in substantial harm or privacy risk to children.
- Profile a child.
- Collect, sell, share, or retain any personal information that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged.
- Use a child's personal information for any unstated reason.
- Collect, sell, or share any precise geolocation of data of children.
- Use dark patterns to:
  - Lead or encourage children to provide personal information beyond what personal information would otherwise be reasonably expected to be provided for that online service, product, game or feature.
  - Forego privacy protections.
  - Take any action that the online platform has actual knowledge of or willfully disregards that may result in substantial harm or privacy risk to children.
- Use collected information to estimate age or age range for any other purpose or retain that personal information longer than necessary to estimate age.[14]

In 2024, the Legislature enacted a law to prohibit children under the age of 14 from creating a social media account.[15] A social media platform must do the following:

- Terminate any account held by an account holder younger than 14 years of age, including accounts that the social media platform treats or categorizes as belonging to an account holder who is likely younger than 14 years of age for purposes of targeting content or advertising, and provide 90 days for an account holder to dispute such termination.
- Allow an account holder younger than 14 years of age to request to terminate the account.
- Allow the confirmed parent or guardian of an account holder younger than 14 years of age to request that the minor's account be terminated. Termination must be effective within 10 business days after such request.
- Permanently delete all personal information held by the social media platform relating to the terminated account, unless there are legal requirements to maintain such information.[16]

[13] *Id.*
[14] Section 501.1735, F.S.
[15] Ch. 2024-42, Laws of Fla.
[16] Section 501.1736, F.S.

A social media platform must prohibit a minor who is 14 or 15 years of age from entering into a contract with a social media platform to become an account holder, unless the minor's parent or guardian provides consent for the minor to become an account holder.[17]

A social media platform must do the following:

- Terminate any account held by an account holder who is 14 or 15 years of age, including accounts that the social media platform treats or categorizes as belonging to an account holder who is likely 14 or 15 years of age for purposes of targeting content or advertising, if the account holder's parent or guardian has not provided consent for the minor to create or maintain the account. The social media platform must provide 90 days for an account holder to dispute such termination. Termination must be effective upon the expiration of the 90 days if the account holder fails to effectively dispute the termination.
- Allow an account holder who is 14 or 15 years of age to request to terminate the account. Termination must be effective within 5 business days after such request.
- Allow the confirmed parent or guardian of an account holder who is 14 or 15 years of age to request that the minor's account be terminated. Termination must be effective within 10 business days after such request.
- Permanently delete all personal information held by the social media platform relating to the terminated account, unless there are legal requirements to maintain such information.[18]

Any knowing or reckless violation of s. 501.1736(2) or (3), F.S., is deemed an unfair and deceptive trade practice, and the department has enforcement authority.[19] In addition to the remedies under the Florida Deceptive and Unfair Trade Practices Act, the department may collect a civil penalty of up to $50,000 per violation and reasonable attorney fees and court costs for a violation by a third party.[20] When the social media platform's failure to comply with the requirements is a consistent pattern of knowing or reckless conduct, punitive damages may be assessed against the social media platform.[21]

A social media platform that knowingly or recklessly violates s. 501.1736(2) or (3), F.S., is liable to the minor account holder, including court costs and reasonable attorney fees as ordered by the court. Claimants may be awarded up to $10,000 in damages. A civil action for a claim must be brought within 1 year from the date the complainant knew, or reasonably should have known, of the alleged violation.[22]

Litigation Status

In October of 2024, the Computer and Communications Industry Association and NetChoice (Association) filed a lawsuit in the U.S. District Court for the Northern District of Florida to challenge Florida's social media law that among other requirements, requires certain social media platforms to prohibit minors under age 14 from becoming an account holder or

[17] *Id.*
[18] Section 501.1736(4), F.S., provides that if a court enjoins the enforcement of this section, then this section should be severed and s. 501.1736(4), F.S., will take effect, which prohibits a minor who is 14 or 15 years of age from entering into a contract with a social media platform to become an account holder.
[19] Section 501.1736, F.S.
[20] *Id*.
[21] *Id*.
[22] *Id*.

maintaining an account on such platforms, and in June of 2025, the district court granted the Association's motion for a preliminary injunction.[23] Florida appealed this decision and requested that the Eleventh Circuit "stay" the injunction to allow the law to take effect while the appeal continues.[24] In November of 2025, the Eleventh Circuit granted Florida's motion for a "stay," which allows Florida to enforce the law while the appeal proceeds.[25] The case is currently pending before the Eleventh Circuit.[26]

The Digital Bill of Rights

In 2023, the Legislature passed the "Florida Digital Bill of Rights,"[27] which created a unified scheme to allow Florida's consumers to control the digital flow of their personal information.[28] The "Florida Digital Bill of Rights" gives Florida consumers the right to:

- Confirm and access their personal data;
- Delete, correct, or obtain a copy of that personal data;
- Opt out of the processing of personal data for the purposes of targeted advertising, the sale of personal data, or profiling in furtherance of a decision that produces a legal or similarly significant effect concerning a consumer;
- Opt out of the collection or processing of sensitive data, including precise geolocation data; and
- Opt out of the collection of personal data collected through the operation of a voice recognition or facial recognition feature.

The data privacy provisions of ch. 501, part V, F.S., generally apply to "controllers," businesses that collect Florida consumers' personal data, make in excess of $1 billion in global gross annual revenues, and meet one of the following thresholds:

- Derives 50 percent or more if its global gross annual revenues from the online sale of advertisements, including from providing targeted advertising or the sale of ads online;
- Operates a consumer smart speaker and voice command component service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation; or
- Operates an app store or digital distribution platform that offers at least 250,000 different software applications for consumers to download and install.

A controller who operates an online search engine is required to make available an up-to date plain language description of the main parameters that are most significant in determining ranking and the relative importance of those main parameters, including the prioritization or deprioritization of political partisanship or political ideology in search results. A controller must also conduct and document a data protection assessment of certain processing activities involving personal data. Additionally, a controller is required to provide consumers with a reasonably accessible and clear privacy notice, updated at least annually.

[23] *CCIA & NetChoice v. Uthmeier*, 2025 WL 1570007 (N.D. Fla. June 3, 2025).
[24] *CCIA & NetChoice v. Uthmeier*, 2025 WL 3458571 (11th Cir. 2025).
[25] *Id.*
[26] *Id*.
[27] *See* ch. 2023-201, Laws of Fla. *See also* part V of ch. 501, F.S.
[28] *Id.*

Additionally, a controller in procession of deidentified data must do the following:

- Take reasonable measures to ensure that the data cannot be associated with an individual.
- Maintain and use the data in deidentified form. A controller may not attempt to reidentify the data, except that the controller may attempt to reidentify the data solely for the purpose of determining whether its deidentification processes satisfy the requirements of s. 501.714, F.S.
- Contractually obligate any recipient of the deidentified data to comply with the Florida Digital Bill of Rights.
- Implement business processes to prevent the inadvertent release of deidentified data.

Section 501.702(13), F.S., defines "deidentified data" as data that cannot reasonably be linked to an identified or identifiable individual or a device linked to that individual.

The Florida Digital Bill of Rights may not be construed to require a controller or processor[29] to do any of the following:

- Reidentify deidentified data or pseudonymous data.
- Maintain data in an identifiable form or obtain, retain, or access any data or technology for the purpose of allowing the controller or processor to associate a consumer request with personal data.
- Comply with an authenticated consumer rights request under s. 501.705, F.S.,[30] if the controller:
    - Is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data;
    - Does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data or associate the personal data with other personal data about the same specific consumer; and
    - Does not sell the personal data to a third party or otherwise voluntarily disclose the personal data to a third party other than a processor, except as otherwise authorized.

Further, a controller that discloses deidentified data must exercise reasonable oversight to monitor compliance with any contractual commitments to which the data or information is subject and must take appropriate steps to address any breach of contractual commitments.[31]

A violation of the "Florida Digital Bill of Rights" is an unfair and deceptive trade practice actionable under ch. 501, part II, F.S., to be enforced by the Department of Legal Affairs (DLA).

---

[29] Section 501.702(24), F.S., defines "processor" as a person who processes personal data on behalf of a controller.

[30] Section 501.705, F.S., provides that a consumer is entitled to the following upon request: (1) to confirm whether a controller is processing the consumer's personal data and to access the personal datal (2) to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data; (3) to delete any or all personal data provided by or obtained about the consumer; (4) to obtain a copy of the consumer's personal data in a portable and, to the extent technically feasible, readily usable format if the data is available in a digital format; (5) to opt out of the processing of the personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of a decision that produces a legal or similarly significant effect concerning a consumer; (6) to opt out of the collection of sensitive data, including precise geolocation data, or the processing of sensitive data; and (7) to opt out of the collection of personal data collected through the operation of a voice recognition or facial recognition feature.

[31] Section 540.714(4), F.S.

The DLA may provide a right to cure a violation of ch. 501, part V, F.S., by providing written notice of the violation and then allowing a 45-day period to cure the alleged violation. The DLA is required to make a report publicly available by February 1 each year on the DLA's website that describes any actions it has undertaken to enforce ch. 501, part V, F.S.

Florida Deceptive and Unfair Trade Practices Act

History and Purpose

The Florida Deceptive and Unfair Trade Practices Act (FDUTPA) became law in 1973.[32] The FDUTPA is a consumer and business protection measure that prohibits unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in trade or commerce.[33] The FDUTPA is based on federal law, and s. 501.204(2), F.S., provides that it is the intent of the Legislature that due consideration and great weight must be given to the interpretations of the Federal Trade Commission and the federal courts relating to section 5 of the Federal Trade Commission Act.[34]

The State Attorney or the Department of Legal Affairs may bring actions when it is in the public interest on behalf of consumers or governmental entities.[35] The Office of the State Attorney may enforce violations of the FDUTPA if the violations take place in its jurisdiction.[36] The Department of Legal Affairs has enforcement authority if the violation is multi-jurisdictional, the state attorney defers in writing, or the state attorney fails to act within 90 days after a written complaint is filed.[37] Consumers may also file suit through private actions.[38]

Remedies under the FDUTPA

The Department of Legal Affairs and the State Attorney, as enforcing authorities, may seek the following remedies:

- Declaratory judgments.
- Injunctive relief.
- Actual damages on behalf of consumers and businesses.
- Cease and desist orders.
- Civil penalties of up to $10,000 per willful violation.[39]

Remedies for private parties are limited to the following:

- A declaratory judgment and an injunction where a person is aggrieved by a FDUTPA violation.

---

[32] Ch. 73-124, Laws of Fla.; codified at part II of ch. 501, F.S.

[33] *See* s. 501.202, F.S. Trade or commerce means the advertising, soliciting, providing, offering, or distributing, whether by sale, rental, or otherwise, of any good or service, or any property, whether tangible or intangible, or any other article, commodity, or thing of value, wherever situated. "Trade or commerce" shall include the conduct of any trade or commerce, however denominated, including any nonprofit or not-for-profit person or activity. *See* s. 501.203(8), F.S.

[34] *See* s 501.204(2), F.S.

[35] *See* ss. 501.203(2), 501.206, and 501.207, F.S.

[36] Section 501.203(2), F.S.

[37] *Id.*

[38] Section 501.211, F.S.

[39] Sections 501.207(1), 501.208, and 501.2075, F.S. Civil Penalties are deposited into general revenue. Section 501.2075, F.S. Enforcing authorities may also request attorney fees and costs of investigation or litigation. Section 501.2105, F.S.

- Actual damages, attorney fees, and court costs, where a person has suffered a loss due to a FDUTPA violation.[40]

III. Effect of Proposed Changes:

The bill creates s. 501.1733, F.S., to be entitled the "App Store Accountability Act."

Definitions

The bill creates the following definitions:

- "Account holder" means an individual associated with a mobile device.
- "Age category" means one of the following categories of individuals, based on age:
  - A child, which means an individual who is under 13 years of age;
  - A younger teenager, which means an individual who is at least 13 years of age and under 16 years of age;
  - An older teenager, which means an individual who is at least 16 years of age and under 18 years of age; or
  - An adult, which means an individual who is at least 18 years of age.
- "Age category data" means information about an account holder's age category collected by an app store provider and shared with a developer.
- "Age rating" means one or more classifications that assess the suitability of an app's content and functions for different age categories.
- "App" means a software application or electronic service that a user may run or direct on a mobile device. The term includes preinstalled applications.
- "App store" means any publicly available website, software application, or electronic service that allows an account holder to download an app from a third-party developer onto a mobile device.
- "App store provider" means a person that owns, operates, or controls an app store.
- "Content description" means a description of the specific content elements or functions that informed an app's age rating.
- "Department" means the Department of Legal Affairs (DLA).
- "Developer" means a person that owns or controls an app made available through an app store or an app preinstalled onto a mobile device.
- "Knowingly" means to act with actual knowledge or to act with knowledge fairly inferred based on objective circumstances.
- "Minor" means, unless the individual is married or legally emancipated, an individual under 18 years of age.
- "Minor account" means an account with an app store provider, established by an individual who is a minor, which is affiliated with a parent account.
- "Mobile device" means a phone or general-purpose tablet that:
  - Provides cellular or wireless connectivity;
  - Is capable of connecting to the Internet;
  - Runs a mobile operating system; and
  - Is capable of running apps through the mobile operating system.

[40] Section 501.211(1) and (2), F.S.

- "Mobile operating system" means software that:
  - Manages mobile device hardware resources;
  - Provides common services for mobile device programs;
  - Controls memory allocation; and
  - Provides interfaces for apps to access device functionality.
- "Parent" means, with respect to a minor, an individual reasonably believed to be a parent, a legal guardian, an individual with legal custody, or any other individual who has the legal authority to make decisions on behalf of the minor under applicable state law.
- "Parent account" means an account with an app store provider which:
  - Is verified to be established by an individual who the app store provider has determined is at least 18 years of age or married or emancipated through the app store provider's age verification methods; and
  - May be affiliated with one or more minor accounts.
- "Parental consent disclosure" includes the following information:
  - If the app store provider has an age rating for the app or in-app purchase, the app's or in-app purchase's age rating;
  - If the app store provider has a content description for the app or in-app purchase, the app's or in-app purchase's content description;
  - A description of:
    - The personal data collected by the app from an account holder in compliance with, if applicable, part V of ch. 501, F.S.; and
    - The personal data shared by the app and the methods implemented by the developer to protect the personal data, including, if the app meets the definition of a controller under s. 501.702, F.S., the methods implemented by the developer to comply with part V of ch. 501, F.S.; and
  - Whether personal data is collected by the app and the methods implemented by the developer to protect the personal data, and, if the app meets the definition of a controller under s. 501.702, F.S., the methods implemented by the developer to comply with part V of ch. 501, F.S.
- "Preinstalled application" means any app, or portion thereof, which is present on a mobile device at the time of purchase, initial activation, or first use by the consumer, including browsers, search engines, and messaging, but excluding core operating system functions, essential device drivers, and applications necessary for basic device operation such as phone call, settings, and emergency service applications. The term includes apps, or portions thereof, installed or partially installed by the device manufacturer, wireless service provider, retailer, or any other party before purchase, initial activation, or first use by the consumer and which may be updated thereafter.
- "Significant change" means a material modification to an app's terms of service or privacy policy which:
  - Changes the categories of data collected, stored, or shared;
  - Alters the app's age rating or content descriptions; or
  - Introduces in-app purchases where in-app purchases were not previously present or introduces advertisements where advertisements were not previously present in the app.
- "Verifiable parental consent" means authorization that:
  - Is provided by a parent account;

- Is given after the app store provider has clearly and conspicuously provided the parental consent disclosure as part of the app download, purchase, or in-app purchase process; and
- Requires the parent to make an affirmative choice to grant consent or decline consent.

App Store Providers

An app store provider is required to do all of the following:

- At the time an individual located in Florida creates an account with the app store provider, or for existing accounts, by July 1, 2028, request age category information from the individual and verify the individual's age category using:
  - Commercially available methods reasonably designed to ensure accuracy; or
  - An age verification method or process that complies with department rule.
- If the app store provider determines the individual is a minor, require that the account be affiliated with a parent account and obtain verifiable parental consent from the holder of the affiliated parent account each time before allowing the minor to download an app, purchase an app, or make an in-app purchase.
- After receiving notice of a significant change from a developer, notify the account holder of the significant change and, for a minor account, notify the parent account and obtain renewed verifiable parental consent before providing access to the significantly changed version of the app.
- Provide to a developer, in response to a request, age category data for an account holder located in Florida and the status of the verifiable parental consent for a minor located in Florida.
- Provide a mechanism for a parent account to withdraw consent and notify a developer when a parent revokes verifiable parental consent.
- Protect age category data and any associated verification data by:
  - If applicable, complying with s. 501.1735, F.S.;
  - Limiting collection and processing to data necessary for verifying an account holder's age category, obtaining verifiable parental consent, or maintaining compliance records; and
  - Transmitting age category data using industry-standard encryption protocols that ensure data integrity and data confidentiality.
- For preinstalled apps, provide available age category information in response to a request from a developer and take reasonable measures to facilitate verifiable parental consent for use of the app in response to a request from a developer.

An app store provider may not:

- Enforce a contract or terms of service against a minor unless the app store provider has obtained verifiable parental consent;
- Knowingly misrepresent the information in the parental consent disclosure; or
- Share age category data and any associated data except as required by the provisions in the bill or otherwise required by law.

Developers

A developer must:

- Verify through the app store's data-sharing methods the age category data of account holders located in Florida, and for a minor's account, whether verifiable parental consent has been obtained;
- Notify app store providers of significant changes to an app;
- Use age category data received through the app store's data-sharing methods to enforce any developer-created, age related restrictions, safety-related features, or defaults, and to enforce compliance with applicable laws and regulations; and
- Request any age category data or verifiable parental consent at the time an account holder downloads an app, purchases an app, or launches a preinstalled app for the first time; when implementing a significant change to the app; or to comply with applicable law.

A developer may request age category data:
- No more than once during each 12-month period to verify the accuracy of age category data associated with an account holder or the continued account use within an age category;
- When there is reasonable suspicion of an account transfer or misuse outside of the age category; or
- At the time an account holder creates a new account with the developer.

When implementing any developer-created, age-related restrictions, safety-related features, or defaults, a developer must use the lowest age category indicated by age category data received through the app store's data-sharing methods or age data independently collected by the developer.

A developer may not:
- Enforce a contract or terms of service against a minor unless the developer has verified through an app store's data sharing methods that verifiable parental consent has been obtained;
- Knowingly misrepresent any information in the parental consent disclosure; or
- Share age category data with any person.

Enforcement

A minor who has been harmed by a violation of the provisions in the bill, or such minor's parent, may bring a civil action against an app store provider or a developer. In such action, the court must award a prevailing plaintiff:
- The greater of actual damages or $1,000 for each violation;
- Reasonable attorney fees; and
- Litigation costs.

A violation of the provisions in the bill is an unfair and deceptive trade practice actionable under part II of ch. 501, F.S., by the DLA. The DLA may bring an action against an app store provider or a developer to:
- Recover a civil penalty not to exceed $7,500 for each violation;
- Restrain or enjoin the app store provider or developer from violating the provisions in the bill;
- Seek injunctive relief;

- Recover reasonable attorney fees; and
- Recover litigation costs and the costs of investigating the violation.

For the purpose of bringing an action pursuant to the provisions in the bill, ss. 501.211 and 501.212, F.S., do not apply.

Jurisdiction

For purposes of bringing an action pursuant to the provisions in the bill, any person who meets the definition of an app store provider or developer which operates or develops an app store or app likely to be accessed by minors and accessible by minors located in Florida is considered to be both engaged in substantial and not isolated activities within Florida and operating, conducting, engaging in, or carrying on a business and doing business in Florida, and is therefore subject to the jurisdiction of the courts of Florida.

Rules

The DLA is given rulemaking authority.

Safe Harbor

A developer is not liable for a violation of the provisions in the bill if the developer demonstrates that the developer:
- Relied in good faith on applicable age category data received through an app store's data-sharing methods;
- Relied in good faith on notification from an app store provider that verifiable parental consent was obtained if the account holder was a minor; and
- Complied with the requirements in the bill applicable to developers.

In determining an app's age rating and content description for purposes of this bill, a developer is not liable for a violation of the bill if the developer uses widely adopted industry standards to determine the app's age category and content description and applies those standards consistently and in good faith.

This "safe harbor" for developers only applies to actions brought under the provisions in this bill and does not limit a developer's or app store provider's liability under any other applicable law. Additionally, the provisions in the bill does not displace any other available rights or remedies authorized under federal or Florida law.

Construction

The provisions in the bill may not be construed to do any of the following:
- Prevent an app store provider or developer from taking reasonable measures to block, detect, or prevent distribution to minors of unlawful material, obscene material, or other harmful material; block or filter spam; prevent criminal activity; or protect app store or app security.
- Require an app store provider to disclose user information to a developer beyond age category data or status of parental consent.

- Allow an app store provider or developer to implement measures required by the bill in a manner that is arbitrary, capricious, anticompetitive, or unlawful.
- Require an app store provider or developer to obtain verifiable parental consent for an app that:
  - Provides direct access to emergency services, including 911, crisis hotlines, or emergency assistance services, legally available to minors;
  - Limits data collection to information necessary to provide emergency services in compliance with the Children's Online Privacy Protection Act, 15 U.S.C. s. 6501 et seq.;
  - Provides access without requiring account creation or collection of unnecessary personal information; and
  - Is operated by or in partnership with a governmental entity, a nonprofit organization, or an authorized emergency service provider.
- Require a developer to collect, retain, reidentify, or link any information beyond what is necessary to verify age category data as required by this bill, and what is collected, retained, reidentified, or linked in the developer's ordinary course of business.
- Require an app store provider or developer to block access to an application that an account holder has downloaded or installed onto a mobile device before July 1, 2027, except to the extent that a parent account revokes verifiable consent for an affiliated minor account or there has been a significant change to the application.

If any provision of this bill or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this bill which can be given effect without the invalid provision or application, and to this end the provisions of this bill are severable.

Effective Date

The bill takes effect on July 1, 2027.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

The First Amendment to the U.S. Constitution guarantees that "Congress shall make no law ... abridging the freedom of speech."[41] Generally, "government has no power to restrict expression because of its message, its ideas, its subject matter, or its content."[42] The rights guaranteed by the First Amendment apply with equal force to state governments through the due process clause of the Fourteenth Amendment.[43]

In most circumstances, these protections "are no less applicable when government seeks to control the flow of information to minors"[44] as states do not possess "a free-floating power to restrict the ideas to which children may be exposed."[45]

Many of the questions regarding the constitutionality of age verification laws may concern whether such laws are sufficiently narrow to avoid inhibiting more speech than necessary. The degree of tailoring required may vary depending on whether a given law is content-based or content-neutral. In both circumstances, a law's constitutionality depends on several factors, including the:

- Strength of the government's interest.
- Amount of protected speech that the law directly or indirectly restricts.
- Availability of less speech-restrictive alternatives.[46]

Content-neutral regulations on free speech are legitimate if they advance important governmental interests that are not related to suppression of free speech, do so in a way that is substantially related to those interests, and do not substantially burden more speech than necessary to further those interests.[47]

The U.S. Supreme Court regards content-based laws, which limit communication because of the message it conveys, as presumptively unconstitutional.[48] Such a law may be justified only if the government shows that the law is required to promote a compelling state interest and that the least restrictive means have been chosen to further that articulated interest.[49]

In general, the U.S. Supreme Court has held that requiring adults to prove their age to access certain content is an unconstitutional, content-based limit on free speech, when

---

[41] U.S. CONST. amend. I.
[42] *Police Dept. of City of Chicago v. Mosley,* 408 U.S. 92, 95 (1972).
[43] U.S. CONST. amend. XIV; *see also* FLA. CONST., art. I.
[44] *Erznoznik v. City of Jacksonville,* 422 U.S. 205, 214 (1975).
[45] *Brown v. Ent. Merchants Ass'n,* 564 U.S. 786, 794 (2011).
[46] Eric N. Holmes, Congressional Research Service, *Online Age Verification (Part III): Select Constitutional Issues* (CRS Report No. LSB11022, August 17, 2023), available at https://crsreports.congress.gov/product/pdf/LSB/LSB11022.
[47] *Turner Broadcasting System, Inc. v. F.C.C.,* 520 U.S. 180,189 (U.S. 1997).
[48] *Reed v. Town of Gilbert,* 576 U.S. 155, 163 (2015).
[49] *Sable Commc's of California, Inc. vs. F.C.C.,* 492 U.S. 115, 126 (1989).

there are less restrictive means to curb access to minors, such as filters and parental controls.[50]

According to Justice O'Connor's *Reno* dissent, because technology was insufficient for ensuring that minors could be excluded while still providing adults full access to protected content, the age verification provision was viewed as ultimately unconstitutional; however, she contemplated the possibility that future technological advances may allow for a constitutionally sound age verification law.[51]

In June of 2025, the U.S. Supreme Court upheld a Texas law that requires commercial pornography websites to verify the age of their users.[52] The court applied intermediate scrutiny and upheld the law as constitutional because it merely imposes an incidental burden on adults' protected speech while serving the state's important interest in shielding children from harmful content.[53]

Experts assert that age verification systems have progressed considerably from a generation ago when the U.S. Supreme Court held that age verification methods often failed and were too burdensome for law-abiding adults.[54] Currently, there are numerous minimally invasive verification techniques that do not require sharing any age verification information at all with social media platforms.[55]

Additionally, in determining whether laws requiring age verification to access social media platforms unconstitutionally restrict free speech, courts have found that even if "the state has the power to enforce parental prohibitions it does not follow that the state has the power to prevent children from hearing or saying anything without their parents' prior consent."[56] Moreover:

> [A]ge-verification requirements are more restrictive than policies enabling or encouraging users (or their parents) to control their own access to information, whether through user-installed devices and filters or affirmative requests to third-party companies. "Filters impose selective restrictions on speech at the receiving end, not universal restrictions at the source." And "[u]nder a filtering regime, adults ... may gain access to speech

[50] *Reno v. Am. C. L. Union,* 521 U.S. 844, 874 (1997); *Ashcroft v. American Civil Liberties Union,* 542 U.S. 656, 666 (2004); Ronald Kahn, *Reno v. American Civil Liberties Union (1997),* Free Speech Center at Middle Tennessee State University, Dec. 15, 2023, https://firstamendment.mtsu.edu/article/reno-v-american-civil-liberties-union/.
[51] *Reno,* 521 U.S. at 886-91 (O'Connor concurring in part and dissenting in part). The court also considered overbreadth and vagueness arguments, and determined that the Communications Decency Act of 1996 was too broad and vague. *Id.* at 883-84.
[52] *Free Speech Coalition, Inc. v. Paxton*, 606 U.S. 461 (2025).
[53] *Id. See also Computer & Communications Industry Association v. Uthmeier*, 95 F.4th 1022 (11th Cir. 2025), where the U.S. Court of Appeals for the Eleventh Circuit stayed the district court's preliminary injunction, and thus Florida's law that prohibits minors under 14 from having social media accounts and requires parental consent for 14- and 15-year-olds can be enforced while the appeal proceeds.
[54] Broadband Breakfast, *Improved Age Verification Allows States to Consider Restricting Social Media,* Nov. 20, 2023, https://broadbandbreakfast.com/2023/11/improved-age-verification-allows-states-to-consider-restricting-social-media/; *Reno,* 521 U.S. at 886 (1997); *Ashcroft,* 542 U.S. at 666.
[55] The Federalist Society, *Age Verification for Social Media: A Constitutional and Reasonable Regulation,* Aug. 7, 2023, https://fedsoc.org/commentary/fedsoc-blog/age-verification-for-social-media-a-constitutional-and-reasonable-regulation.
[56] *NetChoice, LLC v. Yost,* 2024 WL 104336, *8 (S.D. Ohio Jan. 9, 2024) (internal citations and quotations omitted).

> they have a right to see without having to identify themselves[.]" Similarly, the State could always "act to encourage the use of filters ... by parents" to protect minors.[57]

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

App store providers and developers will be required to adhere to the provisions in the bill.

C. Government Sector Impact:

The DLA will be required to establish rules to implement and enforce the provisions in the bill.

VI. Technical Deficiencies:

None.

VII. Related Issues:

If in enforcing the bill's provisions, the Department of Legal Affairs might come into possession of information that should be exempt from a public records request, a separate bill creating the exemption would be needed.

VIII. Statutes Affected:

This bill creates section 501.1733 of the Florida Statutes.

IX. Additional Information:

A. Committee Substitute – Statement of Changes:
(Summarizing differences between the Committee Substitute and the prior version of the bill.)

None.

B. Amendments:

None.

[57] *NetChoice, LLC v. Griffin,* 2023 WL 5660155, *21 (W.D. Ark. Aug. 31, 2023) (internal citations omitted).