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 1438
INTRODUCER:	Senator Grall
SUBJECT:	Online Access to Materials Harmful to Minors
DATE:	March 24, 2025 REVISED:

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	McMillan	McKay	CM	**Pre-meeting**
2.			JU	
3.			RC	

I. Summary:

SB 1438 creates ss. 282.803 and 501.1741, F.S., to enhance online protections for minors, and establishes requirements for developers and manufacturers of applications and devices. Developers are required to assess whether their applications are likely to be accessed by minors, and manufacturers must implement age verification measures upon the activation of devices. The bill also requires developers to provide features for parental management of a minor's usage of applications and devices.

The bill amends s. 501.1737, F.S., to require commercial entities to use digital age verification methods to verify that a user accessing harmful materials is 18 years or older. "Digital age verification" means either anonymous age verification, standard age verification, or device-based age verification.

The bill creates a framework for device-based age verification, which requires that covered manufacturers take reasonable steps to determine user age and obtain parental consent for users under 16, and requires a website, application, or online service to block access for minors under 18 years of age. Additionally, the bill requires a website, application, or online service to provide disclaimers before displaying known material harmful to minors.

The Department of Legal Affairs is authorized to adopt rules to enforce the provisions of the bill.

The bill takes effect July 1, 2025.

II. Present Situation:

Addictive Designs and Deceptive Patterns

In general, "addictive designs" or "deceptive patterns," also called "dark patterns," are deceptive user experiences that take advantage of how people habitually use websites, to get them to do things that they may not normally do, such as impulse purchasing, giving away personal information, or spending excessive time on websites.[1]

In 2022, the Federal Trade Commission (FTC) issued a report outlining the ways that companies are increasingly using dark patterns to manipulate consumers into buying products or forfeiting their privacy.[2] Common dark pattern tactics include:

- Disguising ads by designing advertisements to look like independent editorial content.
- Claiming to be neutral, but actually ranking companies in exchange for compensation.
- Using countdown timers designed to make consumers believe they only have a limited time to purchase a product or service, even though the offer is not actually time-limited.
- Making it difficult to cancel subscriptions or charges, which involves tricking someone into paying for goods or services without consent.
- Burying key terms and junk fees, which involves hiding or obscuring material information from consumers that they do not see before making a purchase.
- Tricking consumers into sharing data, which involves falsely giving consumers choices about privacy settings or sharing data, but instead steering them toward the option that gives away the most personal information.[3]

Effects on Children

Social media has become an important aspect of the digital interactions of minors who use social media for entertainment and communication purposes.[4] Adolescents are constantly in touch with their peers via social media accounts. However, social media has the potential to have both positive and negative effects on their health.[5] Some 80 percent of teenagers say social media allows them to feel more connected to their peers, according to a 2022 Pew Research Center survey of U.S. teens ages 13 to 17. Overall, one in three said that social media has had a mostly positive effect on them, while 59 percent said that it had neither a positive nor a negative effect.[6] On the other hand, many teens' use, and overuse, of social media has raised questions about its

---

[1] Brad Bartlett, *Dark Design Patterns: Teach Kids to Recognise Them,* Kidslox, Feb. 7, 2023, available at https://kidslox.com/guide-to/dark-design-patterns/ (last visited Mar. 24, 2025).
[2] Federal Trade Commission (FTC), *FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers,* Sep. 15, 2022, available at https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers (last visited Mar. 24, 2025).
[3] *Id.*
[4] Andrea Irmer & Florian Schmiedek, *Associations between youth's daily social media use and well-being are mediated by upward comparisons,* 1 COMMUN. PSYCHOL. 12 (Aug. 22, 2023), available at https://doi.org/10.1038/s44271-023-00013-0 (last visited Mar. 24, 2025).
[5] Maya Dollarhide, *Social Media: Definition, Effects, and List of Top Apps,* Investopedia.com, Feb. 19, 2025, available at https://www.investopedia.com/terms/s/social-media.asp (last visited Mar. 24, 2025).
[6] Monica Anderson et al., *Connection, Creativity, and Drama: Teen Life on Social Media in 2022,* Pew Research Center, Nov. 16, 2022, available at https://www.pewresearch.org/internet/2022/11/16/connection-creativity-and-drama-teen-life-on-social-media-in-2022/ (last visited Mar. 24, 2025).

effect on their physical and mental health by distracting them, disrupting their sleep, and exposing them to bullying, rumor spreading, unrealistic views of other people's lives, and peer pressure.[7]

In May 2023, U.S. Surgeon General Dr. Vivek Murthy released an advisory to call attention to the effects of social media on youth mental health. The advisory noted that at crucial periods of adolescent brain development, social media use is predictive of decreases in life satisfaction, as well as additional concerns around body image, sleep issues, and much more.[8] He also concluded that 13 years old is "too early" for children to use social media, despite most social media companies allowing 13-year-olds to use their platforms, because in early adolescence, kids are still "developing their identity, their sense of self."[9]

Other experts, such as David Greenfield, a psychologist, agree and assert the platforms lure users with powerful tactics. One such tactic is "intermittent reinforcement," which refers to a reward scheme in which the user receives rewards inconsistently and unpredictably. While adults are susceptible, young people are particularly at risk because the brain regions that are involved in resisting temptation and reward are not nearly as developed in children and teenagers as in adults.[10]

Based on their preparation and review of studies and other scientific research, many experts have called for the regulation of social media, and specifically, regulation of the use of social media by children. Dr. Mary Alvord, a member of the American Psychological Association social media advisory panel, has stated that just because social media is here to stay, it does not mean the dangers have to be accepted. "Just as we decide when kids are old enough to drive, and we teach them to be good drivers, we can establish guidelines and teach children to use social media safely." [11]

Safety Measures and Parental Controls

Providing children with information regarding how to more safely use social media could reduce or eliminate harms. Having conversations with them about social media, its benefits, and its risks, could promote positive social media usage.[12] Parental controls can also protect children

---

[7] Mayo Clinic, *Tween and teen health*, available at https://www.mayoclinic.org/healthy-lifestyle/tween-and-teen-health/in-depth/teens-and-social-media-use/art-20474437 (last visited Mar. 24, 2025).
[8] U.S. Department of Health and Human Services, Office of the Surgeon General, *Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory* (2023), available at https://www.ncbi.nlm.nih.gov/books/NBK594761/ (last visited Mar. 24, 2025).
[9] Lauraine Langreo, *Surgeon General: Kids Under 14 Should Not Use Social Media,* EducationWeek, Feb. 2, 2023, available at https://www.edweek.org/leadership/surgeon-general-kids-under-14-should-not-use-social-media/2023/02 (last visited Mar. 24, 2025).
[10] Matt Richtel, *Is Social Media Addictive? Here's What the Science Says.*, The New York Times, Oct. 25, 2023, available at https://www.nytimes.com/2023/10/25/health/social-media-addiction.html (last visited Mar. 24, 2025).
[11] Kirsten Weir, *Social media brings benefits and risks to teens. Here's how psychology can help identify a path forward,* American Psychological Association, Sept. 1, 2023, available at https://www.apa.org/monitor/2023/09/protecting-teens-on-social-media (last visited Mar. 24, 2025).
[12] WebMD Editorial Contributors, *How to Talk to Your Kids About Social Media,* WebMD.com, available at https://www.webmd.com/parenting/how-to-talk-to-kids-about-social-media (last visited Mar. 24, 2025).

from inappropriate content, cyberbullying, and other online safety issues.[13] Examples of parental controls include blocking websites, filtering content, imposing limits on screen time, allowing parents to monitor online activity, using location tracking, and disabling Wi-Fi.[14]

However, two 2018 studies found that parental control apps may actually be counterproductive because they harm the trust between a parent and child and reduce the child's ability to respond to online threats. In one of the studies, children believed that the apps were overly restrictive and prevented them from doing everyday tasks, such as homework assignments. Additionally, a researcher stated that "parental involvement and direct supervision were both associated with fewer peer problems and less online victimization for teens, but neither of these factors correlated with the use of parental control apps."[15]

Child-Focused Online Privacy Laws

Federal Children's Online Privacy Protection Act (COPPA)

COPPA,[16] and its related rules,[17] regulate websites' collection and use of children's information. The operator of a website or online service that is directed to children, or that has actual knowledge that it collects children's personal information (covered entities), must comply with requirements regarding data collection and use, privacy policy notifications, and data security.[18]

For purposes of COPPA, children are individuals under the age of 13.[19] A covered entity may not collect personal information from a child under the age of 13 without the prior, verifiable consent of his or her parent.[20]

COPPA defines personal information as individually identifiable information about an individual that is collected online, including:[21]

- First and last name.
- A home or other physical address including street name and name of a city or town.
- An email address.
- A telephone number.
- A social security number.
- Any other identifier that the FTC determines permits the physical or online contacting of a specific individual; or

---

[13] Internetmatters.org, *Parental Controls*, available at https://www.internetmatters.org/parental-controls/ (last visited Mar. 24, 2025).
[14] Caroline Knorr, *Parents' Ultimate Guide to Parental Controls,* Commonsensemedia.org, Mar. 9, 2021, available at https://www.commonsensemedia.org/articles/parents-ultimate-guide-to-parental-controls (last visited Mar. 24, 2025).
[15] Barbara Abney & Zenaida Kotala, *Apps to Keep Children Safe Online May be Counterproductive*, UCF Today, Apr. 2, 2018, available at https://www.ucf.edu/news/apps-keep-children-safe-online-may-counterproductive/ (last visited Mar. 24, 2025).
[16] 15 U.S.C. ss. 6501-6505.
[17] 16 C.F.R. pt. 312.
[18] Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions*, available at https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions (last visited Mar. 24, 2025).
[19] *Id.*
[20] 15 U.S.C. §§ 6502(a)-(b).
[21] *Id.*

- Information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier.[22]

Operators covered by the rule must:[23]

- Provide notice of what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information.
- Obtain verifiable parental consent for the collection, use, or disclosure of personal information from children.[24]
- Upon request of a parent whose child has provided personal information to a website or online service, upon proper identification of that parent, to such parent, a description of the specific types of personal information collected from the child by that operator.
- Upon request of a parent whose child has provided personal information to a website or online service, upon proper identification of that parent, to such parent, the opportunity at any time to refuse to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that child.
- Upon request of a parent whose child has provided personal information to a website or online service, upon proper identification of that parent, a means that is reasonable under the circumstances for the parent to obtain any personal information collected from that child.
- Prohibit conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity.
- Require the operator of a website or online service to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.[25]

Violations of COPPA are deemed an unfair or deceptive act or practice and are therefore prosecuted by the Federal Trade Commission.[26] While there is no criminal prosecution or private right of action under COPPA, the act authorizes state attorneys general to enforce violations that affect residents of their states.[27]

In 2019, Google and its subsidiary YouTube agreed to pay a $170 million settlement for lawsuits brought by the commission and the state of New York for violations of COPPA for collecting personal information from children without consent. Specifically, it was alleged that YouTube tracked cookies[28] from viewers of child-directed channels, without first notifying parents and

---

[22] *Id.*
[23] *Id.*
[24] The FTC's finalized updates to the COPPA include the requirements that operators obtain separate verifiable parental consent for disclosures to third parties, parents will have to provide consent for disclosures to third parties such as ad networks. *See* Federal Trade Commission, *Children's Online Privacy Protection Rule*, available at https://www.ftc.gov/system/files/ftc_gov/pdf/coppa_sbp_1.16_0.pdf (last visited Mar. 24, 2025).
[25] *Id.*
[26] *See id.; see also* 15 U.S.C. s. 6502(c); 16 C.F.R. s. 312.9.
[27] *See* Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions*, available at https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions (last visited Mar. 24, 2025).
[28] Cookies are bits of data that are sent to and from a user's browser to identify the user. When the user opens a website, the user's browser sends a piece of data to the web server hosting that website. This data usually appears as strings of numbers and letters in a text file. Every time the user accesses a website, a cookie is created and placed in a temporary folder on the user's device. From here, cookies try to match the user's preferences for what the user wants to read, see, or purchase.

obtaining their consent. YouTube earned millions of dollars by using the identifiers to deliver targeted ads to viewers of these channels.[29]

On January 16, 2025, the FTC finalized updates to the COPPA to set new requirements around the collection, use, and disclosure of children's personal information and give parents new tools and protections to help them control what data is provided to third parties about their children.[30]

Age Verification Mechanisms

Many industries are currently required to use online age verification methods, including:
- Alcohol and tobacco.[31]
- Gambling.
- Adult websites.
- Firearms.[32]

Adult websites in the U.S. generally use checkboxes for users to confirm that they are at least 18 years of age. Recently, however, numerous states and the United Kingdom have enacted laws requiring adult websites to use age verification measures to block adult content from being accessed by minors.[33]

Additionally, some social media platforms ask for age-identifying information to create new accounts, but such information is not always verified. For example, Facebook requires new users to self-report a birthdate to confirm that they are at least 13 years old. Meta is currently testing new ways to verify age, including through the use of biometrics and online interviews.[34]

Microsoft, *Everything you need to know about Internet cookies,* Apr. 25, 2023, available at https://www.microsoft.com/en-us/edge/learning-center/what-are-cookies?form=MA13I2 (last visited Mar. 24, 2025).

[29] Federal Trade Commission, *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law,* Sep. 4, 2019, available at https://www.ftc.gov/news-events/news/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations-childrens-privacy-law (last visited Mar. 24, 2025).

[30] Federal Trade Commission, *FTC Finalizes Changes to Children's Privacy Rule Limiting Companies' Ability to Monetize Kids' Data*, available at https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data#:~:text=The%20Federal%20Trade%20Commission%20finalized,was%20last%20updated%20in%202013 (last visited Mar. 24, 2025).

[31] The U.S. Food and Drug Administration (FDA) recommends using independent, third -party age- and identity-verification services that compare customer information against third-party data sources for online sellers of tobacco. FDA, *Enforcement Priorities for Electronic Nicotine Delivery Systems (ENDS) and Other Deemed Products on the Market Without Premarket Authorization (Revised)* (April 2020), at 7, available at https://www.fda.gov/media/133880/download (last visited Mar. 24, 2025).

[32] Jan Stepnov, *What Is an Age Verification System and Why Incorporate It Into Your Business,* Regula, Apr. 21, 2023, available at https://regulaforensics.com/blog/age-verification-system/ (last visited Mar. 24, 2025).

[33] Masha Borak, *UK introduces Online Safety Bill mandating age verification,* Oct. 27, 2023, available at https://www.biometricupdate.com/202310/uk-introduces-online-safety-bill-mandating-age-verification (last visited Mar. 24, 2025); Dmytro Sashchuk, *Age verification regulations in the United States of America*, Veriff, Oct. 30, 2024, available at https://www.veriff.com/fraud/learn/age-verification-legalization-in-the-united-states-of-america (last visited Mar. 24, 2025).

[34] Meta, *Introducing New Ways to Verify Age on Instagram*, Jun. 23, 2022, available at https://about.fb.com/news/2022/06/new-ways-to-verify-age-on-instagram/ (last visited Mar. 24, 2025).

There are several ways that Internet companies can verify, or attempt to verify, age. Options include using:[35]

- Government identity documents, which generally require users to submit government documents to a third-party company for review.
- Phone records, which generally check users' phones for parental controls.
- Credit score databases, which generally require the user to enter identifying information that is subsequently confirmed through a credit check agency.
- Biometric age estimation, which generally requires a facial analysis to estimate age.
- Credit cards, which generally requires users to supply credit card information for validation.
- Open banking, which generally requires users to log into their own online banking system and give approval for date of birth information to be supplied to a bank-approved, third-party age verification provider.
- Algorithmic profiling, which generally assesses the likely ages of users based on their online behavior.
- Self-declaration, which generally requires users to check a box or enter a birthdate.
- Zero knowledge proofs, which generally enables users to upload identity documents to privacy servers and securely share encrypted, anonymous "proofs" of age to a company, through a process called "hashing," without actually transmitting the identity documents to the company.

When verifying age online, people usually share personal information, including:

- Full name and location.
- Email or phone number (when using two-factor authorization).
- Home address.

Identity theft is a potential risk when users reveal this information, and websites can collect information revealed through age verification processes, and combine it with other data for targeted advertisements or data-sharing with third parties.[36]

Florida's Laws

In 2024, the Legislature enacted laws to require age verification for online access to materials that are harmful to minors.[37]

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.[38]

---

[35] The Age Verification Providers Association, *How do you check age online?*, available at https://avpassociation.com/avmethods/ (last visited Mar. 24, 2025).
[36] John Reynolds, *Don't risk identity fraud just to play that video game – do this instead,* Aleo, Dec. 28, 2023, available at https://aleo.org/post/dont-risk-identity-fraud-to-play-that-video-game/ (last visited Mar. 24, 2025).
[37] Ch. 2024-42, Laws of Fla.
[38] Section 501.1737, F.S.

"Standard age verification" means any commercially reasonable method of age verification approved by the commercial entity.[39]

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.[40] 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.[41]

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.[42]

A third party conducting anonymous age verification:

- 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.[43]

Other States

At least 17 states require websites with adult content to verify the age of users.[44] Many of these laws are facing challenges on free speech grounds, and the Supreme Court is considering a case from the United States Court of Appeals for the Fifth Circuit, *Free Speech Coalition, Inc. v. Paxton*, which challenges a Texas law that requires websites with adult content to implement age verification mechanisms.[45] The court applied rational basis review and held that the age-

[39] 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.
[40] *Id.*
[41] *Id.*
[42] Section 501.1738, F.S.
[43] *Id.*
[44] Technology and Privacy, *States with Age Verification Laws* available at https://www.multistate.us/insider/2025/2/5/supreme-court-ruling-could-impact-state-age-verification-laws (last visited Mar. 24, 2025).
[45] *Free Speech Coalition, Inc. v. Paxton* 95 F.4th 263 (5th Cir. 2024). *See also* "Constitutional Issues" of this bill analysis.

verification requirement did not violate the First Amendment because the state has an interest in protecting the welfare of children and to see that they are safeguarded from abuses.[46]

Social Media Laws for Children

State Requirements for Social Media and Phones in Schools

Florida law requires students in grades 6 through 12 to receive instruction on the social, emotional, and physical effects of social media. The instructional materials must be available online, and district school boards must notify parents of the material's availability.[47]

Florida law also prohibits students from using wireless communication devices at school during instructional time, except when expressly directed by a teacher solely for educational purposes, and requires a teacher to designate an area for wireless communications devices during instructional time.[48]

State Protection of Children in Online Spaces

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.[49]

In 2024, the Legislature enacted a law to prohibit children under the age of 14 from creating a social media account.[50] 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

[46] *Id*.
[47] Section 1003.42(2)(o)5., F.S.
[48] Sections 1006.07(2)(f) and 1003.32(1)(a), F.S.
[49] Section 501.1735, F.S.
[50] Ch. 2024-42, Laws of Fla.

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.[51]

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.[52]

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.[53]

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.[54] 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.[55] 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.[56]

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

[51] Section 501.1736, F.S.
[52] *Id.*
[53] 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.
[54] Section 501.1736, F.S.
[55] *Id*.
[56] *Id*.

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.[57]

In October 2024, two internet-industry groups filed a federal lawsuit challenging the constitutionality of Florida's law limiting minors' access to social media platforms. The Computer & Communications Industry Association and NetChoice, whose members include tech giants such as Google and Meta Platforms, alleged that the law violated their First Amendment rights and that parents have control of their children's social-media use.[58]

In March 2025, the motion for preliminary injunction was denied. The order did not include a ruling on the First Amendment issue. The order was instead based on the decision that the plaintiffs did not "show a substantial likelihood demonstrating standing" that at least one of the group members "will suffer irreparable injury" without an injunction. The effective date of the law was supposed to be January 1, 2025; however, in November the State agreed not to enforce it until the ruling occurred.[59]

Florida Deceptive and Unfair Trade Practices Act (FDUTPA)

The FDUTPA is a consumer and business protection measure that prohibits unfair methods of competition, and unconscionable, deceptive, or unfair acts or practices in the conduct of trade or commerce.[60] The FDUTPA was modeled after the Federal Trade Commission Act.[61]

The Department of Legal Affairs or the state attorney's office in the judicial circuit affected or where the violation occurs may bring actions on behalf of consumers or governmental entities when it serves the public interest.[62] The state attorney's office may enforce violations of the FDUTPA if the violations take place within its jurisdiction. The department has enforcement authority when: the violation is multi-jurisdictional; the state attorney defers to the department in writing; or the state attorney fails to act within 90 days after a written complaint is filed.[63] In certain circumstances, consumers may also file suit through private actions.[64]

The department and the state attorney's office have powers to investigate the FDUTPA claims, which include:[65]

---

[57] *Id*.
[58] Computer & Communications Industry Association and NetChoice v. Uthmeier, Case No.: 4:24-cv-00438-MW-MAF. The case is in the US District Court, Northern District of Florida.
[59] *Id*.
[60] Section 501.202, F.S.
[61] *See* 15 U.S.C. s. 45; *see also* D. Matthew Allen, et. al., *The Federal Character of Florida's Deceptive and Unfair Trade Practices Act*, 65 U. MIAMI L. REV. 1083 (Summer 2011).
[62] Sections 501.203(2) and 501.207(1)(c) and (2), F.S.; *see also* David J. Federbush, *FDUTPA for Civil Antitrust Additional Conduct, Party, and Geographic Coverage; State Actions for Consumer Restitution*, 76 FLA. BAR J. 52 (Dec. 2002), available at https://www.floridabar.org/the-florida-bar-journal/fdutpa-for-civil-antitrust-additional-conduct-party-and-geographic-coverage-state-actions-for-consumer-restitution/ (analyzing the merits of FDUPTA and the potential for deterrence of anticompetitive conduct in Florida) (last visited Mar. 24, 2025).
[63] Section 501.203(2), F.S.
[64] Section 501.211, F.S.
[65] Section 501.206(1), F.S.

- Administering oaths and affirmations.
- Subpoenaing witnesses or matter.
- Collecting evidence.

The department and the state attorney's office may seek the following remedies:[66]
- 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.

The FDUTPA may not be applied to certain entities in certain circumstances, including:[67]
- Any person or activity regulated under laws administered by the Office of Insurance Regulation or the Department of Financial Services.
- Banks, credit unions, and savings and loan associations regulated by the Office of Financial Regulation or federal agencies.

III. Effect of Proposed Changes:

Online Application Stores

Definitions

Section 1 of the bill creates s. 282.803, F.S., which provides the following definitions:
- "Application store" means a publicly available website, software application, or online service that distributes third party platform software applications to a computer, a mobile device, or any other general purpose computing device.
- "Child" means an individual consumer under 18 years of age.
- "Covered application" means a software application, website, or other online service that is likely to be accessed by children and that is intended to be run or directed by a user on a computer, mobile device, or any other general purpose computing device. The term does not include a broadband Internet access service as defined in 47 C.F.R. s. 8.1(b); a telecommunications service as defined in 47 U.S.C. s. 153; or the delivery or use of a physical product unconnected to the Internet.
- "Covered entity" means a covered manufacturer or developer of a covered application.
- "Covered manufacturer" means a manufacturer of a device, an operating system for a device, or an application store.
- "Developer" means any person, entity, or organization that creates, owns, or controls an application and is responsible for the design, development, maintenance, and distribution of the application to users through an application store.
- "Device" means a device or a portion of a device that is designed for and capable of communicating across a computer network with other computers or devices for the purpose of transmitting, receiving, or storing data, including, but not limited to, a desktop, a laptop, a

[66] Sections 501.207(1), 501.208, and 501.2075, F.S. Civil Penalties are deposited into general revenue. Enforcing authorities may also request attorney fees and costs of investigation or litigation. Section 501.2105, F.S.
[67] Section 501.212(4), F.S.

cellular telephone, a tablet, or any other device designed for and capable of communicating with or across a computer network and that is used for such purpose. The term does not include cable, fiber, or wireless modems, and home routers whether standalone or combined with the aforementioned modems; managed set-top boxes; and any physical object that only supports communications within a closed user group or private network available to a limited set of users.

- "Likely to be accessed by children" means it is reasonable to expect that an application would be accessed by children, based on satisfying any of the following criteria:
  - The application is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by children; or
  - Internal research findings determine that the application is routinely accessed by children.
- "Parent" means a biological, foster, or adoptive parent; a stepparent; or a legal guardian.
- "User" means an individual consumer of covered applications.

Developers of Covered Applications

Beginning January 1, 2026, the bill requires a developer of a covered application to:

- Determine whether an application the developer provides is likely to be accessed by children and, if the application is provided for distribution via an application store, provide notice to such application store that the application is likely to be accessed by children.
- To the extent applicable and technically feasible, provide readily available features for parents to protect a user that is a child as appropriate to the risks that arise from the child's use of the developer's covered application. This includes providing features to help manage which accounts are affirmatively linked to the user under the age of 18, to help manage the delivery of age appropriate content, and to limit the amount of time that the user under the age of 18 spends daily on the developer's covered application.

The bill authorizes developers of covered applications to rely on age signals and parental consent for purposes of complying with the aforementioned requirements.

Covered Manufacturers

The bill requires a covered manufacturer to take commercially reasonable and technically feasible steps to:

- Upon initial activation of a device, determine or estimate the age of the device's primary user.
- If the covered manufacturer is an application store:
  - Provide a mechanism for a developer to provide notice that an application is likely to be accessed by children;
  - Obtain parental consent before permitting a known child under 16 years of age to download a covered application from the application store;
  - Provide developers of covered applications in the application store a signal regarding whether a parent has provided consent; and
  - Provide the parent with the option to connect the developer of such a covered application with the approving parent for the purpose of facilitating parental supervision tools.
- Provide developers of covered applications with a digital signal via a real time application programming interface regarding whether a user is:
  - Under 13 years of age;

- At least 13 years of age and under 16 years of age;
- At least 16 years of age and under 18 years of age; or
- At least 18 years of age.[68]

Exceptions

Except when a covered manufacturer is an application store, section 1 of the bill does not:

- Require a covered entity to access, collect, retain, reidentify, or link information, that in the ordinary course of business, would not otherwise be accessed, collected, retained, reidentified, or linked;
- Require a covered entity to implement new account controls or safety settings if it is not necessary to comply with this bill; and
- Modify, impair, or supersede the operation of any antitrust law.

Applications Stores

The bill requires an application store to comply with the requirements in section 1 of the bill in a nondiscriminatory manner, including:

- Imposing at least the same restrictions and obligations on its own applications and application distribution as it does on those from third-party applications or application distributors.
- Not using data collected from third parties, or consent mechanisms deployed for third parties, in the course of compliance, for any of the following:
  - To compete against those third parties;
  - To give the application store's services preference relative to those of third parties; and
  - To otherwise use the data or consent mechanism in an anticompetitive manner.

Enforcement

The bill requires the Attorney General to provide the covered entity with at least 45 days written notice before the date on which the Attorney General initiates an enforcement action against a covered entity. The notice must identify each alleged violation and an explanation of the basis for each allegation.

The Attorney General may not initiate an action if the covered entity cures the violation or violations described in the notice within 45 days after the notice is sent and provides the Attorney General with a written statement indicating that the violation is cured and that no further violations will occur. If the violation is not cured, the Attorney General may bring a civil action and seek damages for up to $2,500 per violation not to exceed $50,000. The bill does not provide a private right of action; the Attorney General has exclusive authority to enforce these provisions.

The bill provides an affirmative defense if the developer acted in reasonable reliance on the application store's determination or estimate that the user is not a child. Additionally, a covered manufacturer is not subject to liability for failure to comply with section 1 of the bill if that

[68] For devices sold before January 1, 2026, the bill requires covered manufacturers to ensure that the requirements are included in its operating system and app store versions and updates by default after January 1, 2027.

covered manufacturer has taken commercially reasonable and technically feasible steps to determine or estimate the age of the user of the relevant device.

Age Verification for Online Access to Materials Harmful to Minors

Definitions

Section 2 of the bill amends s. 501.1737, F.S., and provides the following definitions as used in ss. 501.1737 and 501.1741, F.S.:

- "Application store" means a publicly available website, software application, or online service that distributes third party platforms' software applications to a computer, a mobile device, or any other general-purpose computing device.
- "Covered manufacturer" means a manufacturer of a device, an operating system for a device, or an application store.
- "Device" means equipment or a portion of equipment that is designed for and capable of communicating across a computer network with other computers or devices for the purpose of transmitting, receiving, or storing data, including, but not limited to, a desktop, a laptop, a cellular telephone, a tablet, or any other device designed for and capable of communicating with or across a computer network and that is used for such purpose.
- "Digital age verification" means anonymous age verification, standard age verification, or device-based age verification.
- "Operating system provider" means an entity that develops, distributes, or maintains the operating system of, and provides common services for, a device. The term includes the design, programming, and supply of operating systems for various devices such as smartphones, tablets, and other digital equipment.

Guidelines

The bill provides that 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, must use digital age verification.[69]

The bill requires a commercial entity to ensure that the requirements of s. 501.1738, F.S., which provides the framework for "anonymous age verification," are met unless the commercial entity is relying on device-based age verification.[70]

Penalties

The bill provides that a "covered manufacturer" must follow the requirements provided in section 3 of the bill, which establishes the framework for "device-based age verification." If a covered manufacturer violates any of those requirements, it is deemed an unfair and deceptive trade practice under s. 501.1737(5)(a), F.S.

[69] The bill defines "digital age verification" as either anonymous age verification, standard age verification, or device-based age verification. The bill requires a commercial entity to offer anonymous age verification and standard age verification, and a person attempting to access the material may select which method will be used to verify his or her age unless the commercial entity is relying on device-based age verification.

[70] The bill creates the framework for "device-based age verification" in s. 501.1741, F.S.

The bill removes the provision in s. 501.1737, F.S., that provides a private cause of action to a minor.

The bill removes the provision in s. 501.1737, F.S., that requires all information held by the Department of Legal Affairs pursuant to a notification of a violation or an investigation of a violation to be confidential and exempt from s. 119.07(1), F.S., and s. 24(a), Art. I of the State Constitution.[71]

Device-based Age Verification

Section 3 of the bill creates s. 501.1741, F.S., which establishes the framework for device-based age verification.

Upon activation of a device, a covered manufacturer must take commercially reasonable and technically feasible steps to do the following:

- Determine or estimate the age of the user of the device.
- Provide websites, applications, application stores, and online services with a digital signal and a real-time application programming interface to verify that a person is:
  - Younger than 13 years of age;
  - At least 13 years of age but younger than 16 years of age;
  - At least 16 years of age but younger than 18 years of age; and
  - Eighteen years of age or older.
- If the covered manufacturer is an application store, obtain parental or guardian consent before permitting a person younger than 16 years of age to download an application from the application store and provide the parent or guardian with the option to connect the developer of the application with the approving parent or guardian for the purpose of facilitating parental supervision tools.
- Beginning July 1, 2026, ensure that the requirements of this section of the bill are included by default in all operating systems and application store versions and updates for devices sold after July 1, 2026.

The bill requires a website, an application, or an online service that makes material harmful to minors available to minors to recognize and allow for the receipt of digital age signals.

The bill requires a website, an application, or an online service that makes available a substantial portion of material harmful to minors to do the following:

- Block access to the website, application, or online service if an age signal is received indicating that the person using such website, application, or online service is under 18 years of age;
- Provide a disclaimer to the user or visitors that the website, application, or online service contains material harmful to minors; and
- Label itself as restricted to adults.

[71] Section 119.07(1), F.S., and s. 24(a), Art. I of the State Constitution, guarantees every person the right to inspect or copy public records made or received in connection with the official business of any public body, officer, or employee of the state, with certain exceptions.

The bill requires a website, an application, or an online service that knowingly makes available less than a substantial portion of material harmful to minors to do the following:

- Block access to known material harmful to minors if an age signal is received indicating that the person using such website, application, or online service is under 18 years of age; and
- Provide a disclaimer to users or visitors before displaying known material harmful to minors.

The bill requires a website, an application, or an online service with actual knowledge, through receipt of a signal regarding a user's age or otherwise, that a user is under 18 years of age, to the extent commercially reasonable and technically feasible, provide readily available features for parents or guardians to support a minor with respect to the minor's use of the service, including features to help manage which persons or accounts are affirmatively linked to the minor, to help manage the delivery of age appropriate content, and to limit the amount of time that the minor spends daily on the website, application, or online service.

The bill requires a covered manufacturer to comply with the device-based age verification requirements in a nondiscriminatory manner, specifically including, but not limited to, imposing at least the same restrictions and obligations on its own websites, applications, and online services as it does on those from third parties.

A covered manufacturer is prohibited from taking the following actions:

- Using data collected from third parties, or consent mechanisms deployed for third parties, in the course of compliance with the device-based age verification requirements to compete against such third parties;
- Giving the covered manufacturer's services preference relative to those of third parties; or
- Otherwise use data collected from third parties or consent mechanisms deployed by third parties in an anticompetitive manner.

The bill gives the Department of Legal Affairs rule making authority to implement the device-based age verification requirements.

The bill provides that any state law, regulation, or policy or any ordinance, regulation, or policy adopted by a county, a municipality, an administrative agency, or other political subdivision of Florida which is in conflict with this section of the bill is superseded and is deemed null and void to the extent of the conflict.

Effective Date

The bill takes effect July 1, 2025.

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:

First Amendment Right to Freedom of Speech

The First Amendment to the U.S. Constitution guarantees that "Congress shall make no law ... abridging the freedom of speech."[72] Generally, "government has no power to restrict expression because of its message, its ideas, its subject matter, or its content."[73] The rights guaranteed by the First Amendment apply with equal force to state governments through the due process clause of the Fourteenth Amendment.[74]

In most circumstances, these protections "are no less applicable when government seeks to control the flow of information to minors"[75] as states do not possess "a free-floating power to restrict the ideas to which children may be exposed."[76]

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.[77]

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.[78]

[72] U.S. CONST. amend. I.
[73] *Police Dept. of City of Chicago v. Mosley*, 408 U.S. 92, 95 (1972).
[74] U.S. CONST. amend. XIV; *see also* FLA. CONST., art. I.
[75] *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 214 (1975).
[76] *Brown v. Ent. Merchants Ass'n*, 564 U.S. 786, 794 (2011).
[77] 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 (last visited Mar. 24, 2025).
[78] *Turner Broadcasting System, Inc. v. F.C.C.*, 520 U.S. 180,189 (U.S. 1997).

The U.S. Supreme Court regards content-based laws, which limit communication because of the message it conveys, as presumptively unconstitutional.[79] 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.[80]

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 there are less restrictive means to curb access to minors, such as filters and parental controls.[81]

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.[82]

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."[83] 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 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.[84]

State Authority to Regulate to Protect Minors

The U.S. Supreme Court has determined that the state has a "compelling interest in protecting the physical and psychological well-being of minors," which "extends to

---

[79] *Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015).
[80] *Sable Commc's of California, Inc. vs. F.C.C.*, 492 U.S. 115, 126 (1989).
[81] *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, available at https://firstamendment.mtsu.edu/article/reno-v-american-civil-liberties-union/ (last visited Mar. 24, 2025).
[82] *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.
[83] *NetChoice, LLC v. Yost*, 2024 WL 104336, *8 (S.D. Ohio Jan. 9, 2024) (internal citations and quotations omitted).
[84] *NetChoice, LLC v. Griffin*, 2023 WL 5660155, *21 (W.D. Ark. Aug. 31, 2023) (internal citations omitted).

shielding minors from the influence of literature that is not obscene by adult standards."[85] In doing so, however, the means must be narrowly tailored to achieve that end so as not to unnecessarily deny adults access to material which is constitutionally protected indecent material.[86]

Supremacy Clause

Article VI, Paragraph 2 of the U.S. Constitution, commonly referred to as the Supremacy Clause, establishes that the federal constitution, and federal law generally, take precedence over state laws and constitutions. The Supremacy Clause also prohibits states from interfering with the federal government's exercise of its constitutional powers and from assuming any functions that are exclusively entrusted to the federal government. It does not, however, allow the federal government to review or veto state laws before they take effect.[87]

Section 230 of the federal Communications Decency Act, in part, specifies that "[n]o provider ... of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider"[88] and specifically prohibits all inconsistent causes of action and liability imposed under any state or local law.[89]

V. Fiscal Impact Statement:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

The bill requires covered manufacturers and developers of covered applications to take certain steps, provide certain features, and provide certain notices or disclaimers to assist in protecting minors, which will likely increase costs for such entities.

C. Government Sector Impact:

The Department of Legal Affairs will be required to adopt rules to implement the provisions in this bill.

VI. Technical Deficiencies:

None.

---

[85] *Sable Commc's of California, Inc.*, 492 U.S. at 126.
[86] *Ashcroft,* 542 U.S. at 666; *Cashatt v. State,* 873 So. 2d 430, 434 (Fla. 1st DCA 2004); *but see Erznoznik,* 422 U.S. at 213 (determining that the city's regulation was overly broad).
[87] Cornell Law School, Legal Information Institute, *Supremacy Clause*, available at https://www.law.cornell.edu/wex/supremacy_clause (last visited Mar. 24, 2025).
[88] 47 U.S.C. s. 230(c)(1).
[89] 47 U.S.C. s. 230(e)(3).

VII. Related Issues:

None.

VIII. Statutes Affected:

This bill substantially amends section 501.1737 of the Florida Statutes.

This bill creates the following sections of the Florida Statutes: 282.803 and 501.1741.

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.