BILL ANALYSIS

Senate Research Center

C.S.H.B. 18
By: Slawson et al. (Hughes)
State Affairs
5/16/2023
Committee Report (Substituted)

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

Mounting evidence draws a strong connection between uninhibited access to social media platforms and online content and the harmful consequences of such access—this is especially true for children. There is an epidemic of self-harm, suicide, substance abuse, sexual exploitation, and human trafficking among minors. In tandem, platforms are collecting and processing vast amounts of data from minors. This data raises privacy concerns and feeds algorithms that fuel online addiction. Advertising is increasingly of concern due to its sophistication built on data taken from children and its subtle manipulation. Parents are increasingly powerless to protect their children in the face of these sophisticated companies and the technologies they create.

H.B. 18, the Securing Children Online through Parental Empowerment (SCOPE) Act, seeks to prohibit a digital service provider (DSP) from entering into an agreement with a known minor without the consent of the known minor's parent or guardian and require a DSP to provide in those agreements the ability for the parent or guardian to permanently enable certain settings. The SCOPE Act seeks also to require certain disclosures regarding advertising and provide parents better insight into how algorithms are used to target their children.

(Original Author's/Sponsor's Statement of Intent)

C.S.H.B. 18 amends current law relating to the protection of minors from harmful, deceptive, or unfair trade practices in connection with the use of certain digital services and electronic devices, including the use and transfer of electronic devices to students by a public school.

RULEMAKING AUTHORITY

This bill does not expressly grant any additional rulemaking authority to a state officer, institution, or agency.

SECTION BY SECTION ANALYSIS

ARTICLE 1. SHORT TITLE

SECTION 1.01. Authorizes this Act to be cited as the Securing Children Online through Parental Empowerment (SCOPE) Act.

ARTICLE 2. USE OF DIGITAL SERVICES BY MINORS

SECTION 2.01. Amends Subtitle A, Title 11, Business and Commerce Code, by adding Chapter 509, as follows:

CHAPTER 509. USE OF DIGITAL SERVICES BY MINORS

SUBCHAPTER A. GENERAL PROVISIONS

Sec. 509.001. DEFINITIONS. Defines "digital service," "digital service provider," "harmful material," "known minor," "minor," "personal identifying information," and "verified parent."

Sec. 509.002. APPLICABILITY. (a) Provides that this chapter, except to the extent that Section 509.057 applies to any digital service provider, applies only to a digital service provider who provides a digital service that:

(1) has a primary function of connecting users in a manner that allows users to socially interact with other users on the digital service;

(2) allows a user to create a public or semi-public profile for purposes of signing into and using the digital service; and

(3) allows a user to create or post content that can be viewed by other users of the digital service, including sharing content on:

(A) a message board;

(B) a chat room; or

(C) a landing page or main feed that presents to a user content created and posted by other users.

(b) Provides that this chapter does not apply to:

(1) a state agency or a political subdivision of this state;

(2) a financial institution or data subject to Title V, Gramm-Leach-Bliley Act (15 U.S.C. Section 6801 et seq.);

(3) a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, C.F.R. Parts 160 and 164, established under the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.), and the Health Information Technology for Economic and Clinical Health Act (Division A, Title XIII, and Division B, Title IV, Pub. L. No. 111-5);

(4) a small business as defined by the United States Small Business Administration on September 1, 2024;

(5) an institution of higher education;

(6) a digital service provider who processes or maintains user data in connection with the employment, promotion, reassignment, or retention of the user as an employee or independent contractor, to the extent that the user's data is processed or maintained for that purpose;

(7) an operator or provider regulated by Subchapter D (Student Information), Chapter 32, Education Code, that primarily provides education services to students or educational institutions;

(8) a person subject to the Family Educational Rights and Privacy Act of 1974 (20 U.S.C. Section 1232g) that:

(A) operates a digital service; and

(B) primarily provides education services to students or educational institutions;

(9) a digital service provider who provides a digital service that facilitates e-mail or direct messaging services, if the digital service facilitates only those services; or

(10) a digital service provider who provides a digital service that:

(A) primarily functions to provide a user with access to news, sports, entertainment, commerce, or content selected by the digital service provider; and

(B) allows chat, comment, or other interactive functionality that is incidental to the digital service.

(c) Provides that the Internet service provider, Internet service provider's affiliate or subsidiary, search engine, or cloud service provider, unless an Internet service provider, Internet service provider's affiliate or subsidiary, search engine, or cloud service provider is responsible for the creation of harmful material or other content described by Section 509.053(a), is not considered a digital service provider if the Internet service provider or provider's affiliate or subsidiary, search engine, or cloud service provider solely provides access or connection, including through transmission, download, intermediate storage, access software, or other service, to an Internet website or to other information or content:

(1) on the Internet; or

(2) on a facility, system, or network not under the control of the Internet service provider, provider's affiliate or subsidiary, search engine, or cloud service provider.

SUBCHAPTER B. DIGITAL SERVICE PROVIDER DUTIES AND PROHIBITIONS

Sec. 509.051. DIGITAL SERVICE PROVIDER DUTY TO REGISTER AGE OF USER. (a) Prohibits a digital service provider from entering into an agreement with a person for access to a digital service unless the person has registered the person's age with the digital service provider.

(b) Provides that a person who registers the person's age as younger than 18 years of age is considered to be a known minor to the digital service provider until after the person's 18th birthday.

(c) Prohibits a digital service provider from allowing a person who registers the person's age to alter the person's registered age, unless the alteration process involves a commercially reasonable review process.

(d) Provides that a minor is considered to be a known minor to a digital service provider if:

(1) the minor registers the minor's age under Section 509.051 as younger than 18 years of age; or

(2) the minor's parent or guardian, including a verified parent:

(A) notifies a digital service provider that the minor is younger than 18 years of age;

(B) successfully disputes the registered age of the minor; or

(C) performs another function of a parent or guardian under this chapter.

(e) Provides that a digital service provider, if a minor is a known minor, or if the minor's parent or guardian, including a verified parent, takes an action under Subsection (a):

(1) is considered to have actual knowledge that the minor is younger than 18 years of age; and

(2) is required to treat the minor as a known minor under this chapter.

Sec. 509.052. DIGITAL SERVICE PROVIDER DUTIES RELATING TO AGREEMENT WITH MINOR. Provides that a digital service provider that enters into an agreement with a known minor for access to a digital service, unless a verified parent provides otherwise under Section 509.102:

(1) is required to:

(A) limit collection of the known minor's personal identifying information to information reasonably necessary to provide the digital service; and

(B) limit use of the known minor's personal identifying information to the purpose for which the information was collected; and

(2) is prohibited from:

(A) allowing the known minor to make purchases or engage in other financial transactions through the digital service;

(B) sharing, disclosing, or selling the known minor's personal identifying information;

(C) using the digital service to collect the known minor's precise geolocation data; or

(D) using the digital service to display targeted advertising to the known minor.

Sec. 509.053. DIGITAL SERVICE PROVIDER DUTY TO PREVENT HARM TO KNOWN MINORS. (a) Requires a digital service provider, in relation to a known minor's use of a digital service, to develop and implement a strategy to prevent the known minor's exposure to harmful material and other content that promotes, glorifies, or facilitates:

(1) suicide, self-harm, or eating disorders;

(2) substance abuse;

(3) stalking, bullying, or harassment; or

(4) grooming, trafficking, child pornography, or other sexual exploitation or abuse.

(b) Authorizes a strategy developed under Subsection (a) to include:

(1) creating and maintaining a comprehensive list of harmful material or other content described by Subsection (a) to block from display to a known minor;

(2) using filtering technology and other protocols to enforce the blocking of material or content on the list under Subdivision (1) uniformly across all platforms on which the digital service operates;

(3) using hash-sharing technology and other protocols to identify recurring harmful material or other content described by Subsection (a);

(4) creating and maintaining a database of keywords used for filter evasion, such as identifiable misspellings, hash-tags, or identifiable homoglyphs;

(5) performing standard human-performed monitoring reviews to ensure efficacy of filtering technology;

(6) making available to users a comprehensive description of the categories of harmful material or other content described by Subsection (a) that will be filtered;

(7) engaging a third party to rigorously review the digital service provider's content filtering technology;

(8) except as provided by Section 509.058, making available the digital service provider's algorithm code to independent security researchers;

(9) participating in industry-specific partnerships to share best practices in preventing access to harmful material or other content described by Subsection (a); or

(10) conducting periodic independent audits to ensure:

(A) continued compliance with the digital service provider's strategy; and

(B) efficacy of filtering technology and protocols used by the digital service provider.

Sec. 509.054. DIGITAL SERVICE PROVIDER DUTY TO CREATE PARENTAL TOOLS. (a) Requires a digital service provider to create and provide to a verified parent parental tools to allow the verified parent to supervise the verified parent's known minor's use of a digital service.

(b) Requires that the parental tools under this section allow a verified parent to:

(1) control the known minor's privacy and account settings;

(2) alter the duties of a digital service provider under Section 509.052 with regard to the verified parent's known minor;

(3) if the verified parent alters the duty of a digital service provider under Section 509.052(2)(A), restrict the ability of the verified parent's known minor to make purchases or engage in financial transactions; and

(4) monitor the amount of time the verified parent's known minor spends using the digital service.

Sec. 509.055. DIGITAL SERVICE PROVIDER DUTIES REGARDING ADVERTISING AND MARKETING. Requires a digital service provider to make a commercially reasonable effort to prevent advertisers on the digital service provider's digital service from targeting a known minor with advertisements that facilitate, promote, or offer a product, service, or activity that is unlawful for a minor in this state to use or engage in.

Sec. 509.056. USE OF ALGORITHMS. Requires a digital service provider that uses algorithms to automate the suggestion, promotion, or ranking of information to known minors on the digital service to:

(1) make a commercially reasonable effort to ensure that the algorithm does not interfere with the digital service provider's duties under Section 509.053; and

(2) disclose in the digital service provider's terms of service, privacy policy, or similar document, in a clear and accessible manner, an overview of:

(A) the manner in which the digital service uses algorithms to provide information or content;

(B) the manner in which algorithms promote, rank, or filter information or content; and

(C) the personal identifying information used as inputs to provide information or content.

Sec. 509.057. DIGITAL SERVICE PROVIDER DUTY AS TO HARMFUL MATERIAL. (a) Requires a digital service provider as defined by Section 509.001 that knowingly publishes or distributes material, more than one-third of which is harmful material or obscene as defined by Section 43.21 (Definitions), Penal Code, to use a commercially reasonable age verification method to verify that any person seeking to access content on or through the provider's digital service is 18 years of age or older.

(b) Prohibits the digital service provider, if a person seeking to access content on or through the provider's digital service is not 18 years of age or older, from entering into an agreement with the person for access to the digital service.

Sec. 509.058. PROTECTION OF TRADE SECRETS. Prohibits anything in this subchapter from being construed to require a digital service provider to disclose a trade secret.

Sec. 509.059. USE OF KNOWN MINOR'S PERSONAL IDENTIFYING INFORMATION FOR CERTAIN PURPOSES. Prohibits anything in this subchapter from being construed to prevent a digital service provider from collecting, processing, or sharing a known minor's personal identifying information in a manner necessary to comply with:

(1) a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a governmental entity; or

(2) a law enforcement investigation.

SUBCHAPTER C. VERIFIED PARENTS

Sec. 509.101. VERIFICATION OF PARENT OR GUARDIAN. (a) Requires a digital service provider to verify, using a commercially reasonable method and for each person seeking to perform an action on a digital service as a minor's parent or guardian:

(1) the person's identity; and

(2) the relationship of the person to the known minor.

(b) Requires a digital service provider to provide a process by which a person who has been verified under Subsection (a) as the parent or guardian of a known minor

is authorized to participate in the digital service as the known minor's verified parent as provided by this chapter.

Sec. 509.102. POWERS OF VERIFIED PARENT. (a) Provides that a verified parent is entitled to alter the duties of a digital service provider under Section 509.052 with regard to the verified parent's known minor.

(b) Provides that a verified parent is entitled to supervise the verified parent's known minor's use of a digital service using tools provided by a digital service provider under Section 509.054.

Sec. 509.103. ACCESS TO KNOWN MINOR'S PERSONAL IDENTIFYING INFORMATION. (a) Authorizes a known minor's verified parent to submit a request to a digital service provider to:

(1) review and download any personal identifying information associated with the minor in the possession of the digital service provider; and

(2) delete any personal identifying information associated with the minor collected or processed by the digital service provider.

(b) Requires a digital service provider to establish and make available on the digital service provider's digital service a method by which a known minor's parent or guardian is authorized to make a request for access under this section.

Sec. 509.104. MINOR IN CONSERVATORSHIP OF DEPARTMENT OF FAMILY AND PROTECTIVE SERVICES. Authorizes the Department of Family and Protective Services (DFPS), if a minor is in the conservatorship of DFPS, to designate the minor's caregiver or a member of DFPS's staff to perform the functions of the minor's parent or guardian under this chapter.

SUBCHAPTER D. ENFORCEMENT

Sec. 509.151. DECEPTIVE TRADE PRACTICE; ENFORCEMENT BY ATTORNEY GENERAL. Provides that a violation of this chapter is a deceptive act or practice actionable under Subchapter E (Deceptive Trade Practices and Consumer Protection), Chapter 17, solely as an enforcement action by the consumer protection division of the attorney general's office.

Sec. 509.152. PRIVATE CAUSE OF ACTION. (a) Prohibits this chapter, except as provided by Subsection (b), from being construed as providing a basis for, or being subject to, a private right of action for a violation of this chapter.

(b) Authorizes the parent or guardian of a known minor affected by that violation, if a digital service provider violates this chapter, to bring a cause of action seeking:

(1) a declaratory judgment under Chapter 37 (Declaratory Judgments), Civil Practice and Remedies Code; or

(2) an injunction against the digital service provider.

ARTICLE 3. USE AND TRANSFER OF ELECTRONIC DEVICES BY STUDENTS

SECTION 3.01. Amends the heading to Subchapter C, Chapter 32, Education Code, to read as follows:

SUBCHAPTER C. TRANSFER OF DATA PROCESSING EQUIPMENT AND ELECTRONIC DEVICES TO STUDENTS

SECTION 3.02. Amends Section 32.101, Education Code, as follows:

Sec. 32.101. DEFINITIONS. Defines "data processing," "electronic device," and "Internet filter."

SECTION 3.03. Amends Subchapter C, Chapter 32, Education Code, by adding Section 32.1021, as follows:

Sec. 32.1021. STANDARDS. Requires the Texas Education Agency (TEA) to adopt standards for permissible electronic devices and software applications used by a school district or open-enrollment charter school. Requires TEA, in adopting the standards, to:

(1) minimize data collection conducted on students through electronic devices and software applications;

(2) ensure direct and informed parental consent is required for a student's use of a software application necessary for the administration of:

(A) an assessment instrument under Subchapter B (Assessment of Academic Skills), Chapter 39; or

(B) an assessment relating to college, career, or military readiness for which student performance is considered in evaluating a school district's performance under Section 39.054 (Methods and Standards for Evaluating Performance);

(3) ensure software applications do not conduct mental health assessments or other assessments unrelated to educational curricula that are intended to collect information about students without direct and informed parental consent;

(4) ensure that parents are provided the resources necessary to understand cybersecurity risks and online safety regarding their child's use of electronic devices before the child uses an electronic device at the child's school;

(5) specify periods of time during which an electronic device transferred to a student is required to be deactivated in the interest of student safety;

(6) consider necessary adjustments by age level to the use of electronic devices in the classroom to foster development of students' abilities regarding spending school time and completing assignments without the use of an electronic device;

(7) consider appropriate restrictions on student access to social media websites or applications with an electronic device transferred to a student by a district or school;

(8) require a district or school, before using a social media application for an educational purpose, to determine that an alternative application that is more secure and provides the same educational functionality as the social media application is unavailable for that educational purpose;

(9) consider the required use of an Internet filter capable of notifying appropriate school administrators, who are then required to notify the student's parent, if a student accesses inappropriate or concerning content or words, including content related to:

(A) self-harm;

(B) suicide;

(C) violence to others; or

(D) illicit drugs;

(10) assign to the appropriate officer of a district or school the duty to receive complaints or concerns regarding student use of electronic devices, including cybersecurity and online safety concerns, from district or school staff, other students, or parents; and

(11) provide methods by which a district or school is authorized to ensure an operator, as that term is defined by Section 32.151 (Definitions), that contracts with the district or school to provide software applications complies with Subchapter D.

SECTION 3.04. Amends Section 32.104, Education Code, as follows:

Sec. 32.104. REQUIREMENTS FOR TRANSFER. Requires a school district or open-enrollment charter school, before transferring data processing equipment or an electronic device to a student, to:

(1) makes no changes to this subdivision;

(2)-(3) makes nonsubstantive changes to these subdivisions;

(4) adopt rules establishing programs promoting parents as partners in cybersecurity and online safety that involve parents in students' use of transferred equipment or electronic devices; and

(5) for the transfer of an electronic device to be used for an educational purpose, install an Internet filter that blocks and prohibits pornographic or obscene materials or applications, including from unsolicited pop-ups, installations, and downloads.

ARTICLE 4. STUDY OF EFFECTS OF MEDIA ON MINORS

SECTION 4.01. (a) Requires a joint committee of the legislature to conduct a study on the effects of media on minors.

(b) Requires the joint committee to consist of:

(1) members of the house of representatives appointed by the speaker of the house of representatives; and

(2) members of the senate appointed by the lieutenant governor.

(c) Requires members of the joint committee, in conducting the study, to confer with experts on the subject.

(d) Requires the members of the joint committee to examine:

(1) the health and developmental effects of media on minors; and

(2) the effects of exposure by a minor to various forms of media, including:

(A) social media platforms;

(B) software applications;

(C) Internet websites;

(D) television programming;

(E) motion pictures and film;

(F) artificial intelligence;

(G) mobile devices;

(H) computers;

(I) video games;

(J) virtual and augmented reality; and

(K) other media formats the joint committee considers necessary.

ARTICLE 5. TRANSITION AND EFFECTIVE DATE

SECTION 5.01. Severability Clause.

SECTION 5.02. Provides that Article 3 of this Act applies beginning with the 2023–2024 school year.

SECTION 5.03. (a) Effective date, except as provided by Subsection (b) of this section: September 1, 2024.

(b) Effective date, Article 3: upon passage or September 1, 2023.