



www.lsc.ohio.gov

OHIO LEGISLATIVE SERVICE COMMISSION

Office of Research
and Drafting

Legislative Budget
Office

Substitute Bill Comparative Synopsis

Sub. H.B. 226

136th General Assembly

House Judiciary

Austin C. Strohacker, Attorney

This table summarizes how the latest substitute version of the bill differs from the immediately preceding version. It addresses only the topics on which the two versions differ substantively. It does not list topics on which the two bills are substantively the same.

| Previous Version (As Introduced) | Latest Version (I_136_1246-3) |
|---|--|
| Application developers | |
| Requires a developer to determine if an application is likely to be accessed by children and inform the application store of this determination (<i>R.C. 1349.07(B)</i>). | Requires a developer to verify through the application store the user’s age category and, for a minor account, i.e., an account where the primary user is under 18 years of age, whether parental consent has been obtained by minor users (<i>R.C. 1349.072(A)(1)</i>). |
| No provision. | Defines “age category” as one of the following: <ul style="list-style-type: none"> ▪ Child (less than 13 years of age); ▪ Younger teenager (13 to 16 years of age); ▪ Older teenager (16 to 18 years of age); ▪ Adult (18 years of age) (<i>R.C. 1349.07</i>). |
| No provision. | Requires a developer to notify the application store of any significant changes to the developer’s application (<i>R.C. 1349.072(B)(2)</i>). |
| Requires a developer to provide certain parental controls in their applications that allow parents to manage accounts linked to the child, the | Requires a developer use age category data provided by an application store or independently collected by the developer to |

| Previous Version (As Introduced) | Latest Version (I_136_1246-3) |
|--|---|
| delivery of age-appropriate content, and the daily amount of time a child may spend on the application (<i>R.C. 1349.07(F)</i>). | enforce compliance with developer-created age restrictions, ensure compliance with applicable laws, and implement any developer-created safety features, using the lowest age category indicated by such data (<i>R.C. 1349.072(A)(3) and (C)</i>). |
| No provision. | Requires a developer to request age verification data or parental consent when a user downloads an application, when the developer makes a significant change to the application, or as otherwise necessary to comply with applicable laws (<i>R.C. 1349.072(A)(4)</i>). |
| No provision. | Prohibits a developer from requesting age verification data more than every 12 months in order to verify the accuracy of the data or the continued use of the account within the age category but specifies that a developer may request such data more frequently when there is a reasonable suspicion of an account transfer or misuse outside of the verified age category (<i>R.C. 1349.072(B)(1)</i>). |
| No provision. | Prohibits a developer from enforcing a contract against a minor without parental consent, knowingly misrepresenting information in a parental consent disclosure, or sharing age category data with others (<i>R.C. 1349.072(D)</i>). |
| Device and operating system manufacturers | |
| Requires device manufacturers to determine or estimate, upon activation of the device, the age of the device's primary user (<i>R.C. 1349.07(C)(1)</i>). | No provision. |
| Requires that manufacturers of operating systems for devices sold before January 1, 2026, determine or estimate the age of the device's primary user following the first update to the operating system after January 1, 2027 (<i>R.C. 1349.07(C)(2)</i>). | No provision. |

| Previous Version (As Introduced) | Latest Version (I_136_1246-3) |
|--|---|
| Requires device and operating system manufacturers to provide developers with a digital signal via a real-time application programming interface regarding whether the manufacturer knows or estimates the user's age category (<i>R.C. 1349.07(E)</i>). | No provision. |
| Application stores | |
| Requires application stores to provide a mechanism for developers to provide notice that an application is likely to be accessed by children (<i>R.C. 1349.07(D)(1)</i>). | No provision. |
| No provision. | Requires application stores to notify users when developers make significant changes to an application and, for minor users, obtain renewed parental consent (<i>R.C. 1349.071(A)(3)</i>). |
| No provision. | Requires application stores to obtain and verify an individual's age prior to allowing the individual to create an account (<i>R.C. 1349.071(A)(1)</i>). |
| Requires application stores to obtain parental consent prior to allowing minors to download applications likely to be accessed by children (<i>R.C. 1349.07(D)(2) and (3)</i>). | Requires application stores, if the age verification process indicates that the individual is a minor, to require the minor's account to be affiliated with a parent account and obtain parental consent before allowing the individual to download any application (<i>R.C. 1349.071(A)(2)</i>). |
| Requires application stores to provide parents with the option to connect with developers for the purpose of facilitating parental supervision tools (<i>R.C. 1349.07(D)(4)</i>). | No provision. |
| Requires application stores provide developers with a digital signal via a real-time application programming interface regarding whether the application store knows or estimates the user's age category (<i>R.C. 1349.07(E)</i>). | Requires application stores provide developers with age category data and if a parent has given or revoked parental consent (<i>R.C. 1349.071(A)(4) and (5)</i>). |
| No provision. | Requires application stores to protect personal age verification data by doing both of the following: |

| Previous Version (As Introduced) | Latest Version (I_136_1246-3) |
|--|---|
| No provision. | <ul style="list-style-type: none"> ▪ Limiting collection and processing to data that is necessary to verify a user’s age, obtain parental consent, and maintain compliance records; ▪ Transmitting personal age verification data using industry standard encryption protocols that ensure data integrity and confidentiality (<i>R.C. 1349.071(A)(6)</i>). <p>Prohibits an application store from enforcing a contract or terms of service against a minor unless the application store obtains parental consent (<i>R.C. 1349.071(B)(1)</i>).</p> |
| No provision. | Prohibits an application store from knowingly misrepresenting information in a parental consent disclosure (<i>R.C. 1349.071(B)(2)</i>). |
| No provision. | Prohibits an application store from sharing personal age verification data except to a developer, as required by the bill, or as otherwise required by law (<i>R.C. 1349.071(B)(3)</i>). |
| No provision. | Requires the Director of Commerce to adopt rules establishing processes and means by which an application store may verify whether an account holder is a minor (<i>R.C. 1349.071(C)</i>). |
| Enforcement | |
| No provision. | States that developer or application store that knowingly misrepresents information in a parental consent disclosure commits an unfair or deceptive act or practice under the Consumer Sales Practices Act (CSPA) (<i>R.C. 1349.073</i>). |
| Authorizes the Attorney General to bring a civil action for up to \$2,500 per violation of the bill’s provisions if the violator fails to timely cure the violation (<i>R.C. 1349.07(I)(1), (2), and (3)</i>). | No provision. |
| Specifies that no private cause of action is created by the bill (<i>R.C. 1349.07(I)(7)</i>). | Provides that a minor or the parent of a minor harmed by an application store or developer failing to comply with the bill has a cause of action against that party. A prevailing minor or |

| Previous Version (As Introduced) | Latest Version (I_136_1246-3) |
|---|---|
| | parent is entitled to actual damages, or \$1,000 per violation, whichever is greater, reasonable attorney's fees, and litigation costs <i>(R.C. 1349.073(B) and (C)).</i> |
| Safe harbor | |
| Provides that a developer is not liable if the developer reasonably relied on a signal from a manufacturer regarding a user's age or parental consent status <i>(R.C. 1349.07(I)(5)).</i> | Provides that a developer is not liable for a violation of the bill if they, in good faith, relied on age verification data or parental consent notification from an application store <i>(R.C. 1349.074(A)).</i> |
| Provides that taking commercially reasonable and technically feasible steps to comply with the bill's provisions is an affirmative defense to an alleged violation <i>(R.C. 1349.07(I)(6)).</i> | No provision. |
| No provision. | Specifies that a developer is not liable for misrepresenting information in a parental consent disclosure if the developer uses widely adopted industry standards to determine the age category of the application and the content description disclosure and applies those standards consistently and in good faith <i>(R.C. 1349.0741(B)).</i> |
| No provision. | Specifies that the bill's safe harbor provisions and civil remedies do not limit or displace any other remedies available under state or federal law <i>(R.C. 1349.074(C) and (D)).</i> |
| Specifies that the bill does not require application developers or manufacturers of devices, operating systems, or application stores to access, retain, re-identify, or link information outside the developer's or manufacturer's ordinary course of business, except as absolutely necessary to comply with the bill <i>(R.C. 1349.07(G)(1)).</i> | Same as the As Introduced version <i>(R.C. 1349.075(E)).</i> |
| Specifies that application developers or manufacturers of devices, operating systems, or application stores are not required to implement new account controls or safety settings if existing | No provision. |

| Previous Version (As Introduced) | Latest Version (I_136_1246-3) |
|---|--|
| <p>controls and settings are sufficient to comply with the bill (<i>R.C. 1349.07(G)(2)</i>).</p> <p>No provision.</p> <p>No provision.</p> | <p>Specifies that the bill does not prevent an application store or developer from taking reasonable measures to do any of the following:</p> <ul style="list-style-type: none"> ▪ Block, detect, or prevent distribution to minors of unlawful, obscene, or harmful material; ▪ Block or filter spam; ▪ Prevent criminal activity; ▪ Protect application store or application security (<i>R.C. 1349.075(A)</i>). <p>Specifies that the bill does not require an application store provider to disclose information to a developer other than age category and verification of parental consent status (<i>R.C. 1349.075(B)</i>).</p> |
| Competition | |
| <p>Specifies that the bill does not modify, impair, or supersede the operation of any federal or state antitrust law (<i>R.C. 1349.07(H)</i>).</p> <p>Requires application stores to comply with the bill in a nondiscriminatory way by imposing the same restrictions on their own applications as they do on third-party applications, by not using data collected from third parties to compete against the third parties, or by otherwise acting in a manner adverse to competition (<i>R.C. 1349.07(H)</i>).</p> | <p>No provision.</p> <p>Specifies that the bill does not allow an application store or provider to implement measures required by the bill in a manner that is arbitrary, capricious, adverse to competition, or unlawful (<i>R.C. 1349.075(C)</i>).</p> |
| Effective date and name | |
| <p>Delays the bill’s requirements from going into effect until January 1, 2026 (<i>R.C. 1349.07(B), (C), (D), (E), and (F)</i>).</p> <p>No provision.</p> | <p>No provision.</p> <p>Names the bill “The App Store Accountability Act” (<i>Section 2</i>).</p> |

SUHB0226-136/ts