Department of Legislative Services

Maryland General Assembly
2025 Session

FISCAL AND POLICY NOTE
First Reader

Senate Bill 889 (Senator Henson)
Judicial Proceedings

Criminal Law - Distribution of Students' Personal Information - Prohibition

This bill prohibits a person from intentionally distributing the personal identifying information or image of a student enrolled in an institution of secondary education or postsecondary education (1) without the express permission of the student or, if the student is younger than age 18, the parent or guardian of the student and (2) with intent or knowledge or with reckless disregard for the risk that the personal identifying information or image will be used to "harm" the student. Violators are guilty of a misdemeanor and on conviction are subject to imprisonment of up to one year and/or a fine of up to $5,000. The bill may not be construed or applied in a manner that violates an individual's right to free speech under the U.S. Constitution or the Maryland Declaration of Rights.

Fiscal Summary

State Effect: Potential minimal increase in general fund revenues from fines imposed in the District Court. Potential minimal increase in general fund expenditures for incarcerations in Baltimore City. The Judiciary can implement the bill with existing budgeted resources.

Local Effect: Potential minimal increase in revenues from fines imposed in the circuit courts. Potential minimal increase in local incarceration expenditures. The bill is not expected to materially affect circuit court caseloads or workloads.

Small Business Effect: None.

Analysis

Bill Summary: "Distribute" means to give, sell, transfer, disseminate, publish, upload, circulate, broadcast, make available, allow access to, or engage in any other form of transmission, electronic or otherwise.

"Harm" means physical injury, severe emotional distress, or economic damages.

"Institution of postsecondary education" means a school or other institution that offers an educational program in the State for individuals who are at least 16 years old and who have graduated from or left elementary or secondary school. Institution of postsecondary education does not include any adult education, evening high school, or high school equivalence program conducted by a public school system of the State or any apprenticeship or on-the-job training, as specified.

"Institution of secondary education" means a school or any other institution that enrolls students in grades 6 through 12.

"Personal identifying information" includes a person's (1) name; (2) address; (3) telephone number; (4) driver's license number; (5) Social Security number; (6) place of employment or employee identification number; (7) health insurance or medical identification number; (8) mother's maiden name; (9) bank or other financial institution account number; (10) date of birth; (11) personal identification number; (12) unique biometric data, including fingerprint, voiceprint, retina or iris image, or other unique physical representation; (13) digital signature; (14) credit card or other payment device number; and (15) school address.

Current Law:

Identity Fraud – § 8-301 of the Criminal Law Article

The identity fraud statute contains several prohibitions. Among other things, the statute prohibits a person from knowingly, willfully, and with fraudulent intent possessing, obtaining, or helping another to possess or obtain any "personal identifying information" of an individual, without the consent of the individual, in order to use, sell, or transfer the information to get a benefit, credit, good, service, or other thing of value or to access health information or health care.

Violators of this prohibition are subject to the following penalties, based on the value involved:

- at least $100 but less than $1,500 – misdemeanor, imprisonment for up to 1 year and/or a $500 maximum fine;

- at least $1,500 but less than $25,000 – felony, imprisonment for up to 5 years and/or a $10,000 maximum fine;
- at least $25,000 but less than $100,000 – felony, imprisonment for up to 10 years and/or a $15,000 maximum fine; and
- $100,000 or more – felony, imprisonment for up to 20 years and/or a $25,000 maximum fine.

The statute also prohibits a person from maliciously using an "interactive computer service" to disclose or assist another person to disclose the driver's license number, bank or other financial institution account number, credit card number, payment device number, Social Security number, or employee identification number of an individual, without the consent of the individual, in order to annoy, threaten, embarrass, or harass the individual. Violators are guilty of a misdemeanor punishable by imprisonment for up to one year and/or a $500 maximum fine.

"Interactive computer service" means an information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including a system that provides access to the Internet and cellular phones.

"Personal identifying information" includes a name, address, telephone number, driver's license number, Social Security number, place of employment, employee identification number, health insurance identification number, medical identification number, mother's maiden name, bank or other financial institution account number, date of birth, personal identification number, unique biometric data, including fingerprint, voice print, retina or iris image or other unique physical representation, digital signature, credit card number, or other payment device number.

Misuse of Electronic Communication or Interactive Computer Service – § 3-805 of the Criminal Law Article

A person may not maliciously engage in a course of conduct, through the use of electronic communication, that alarms or seriously annoys another (1) with the intent to harass, alarm, or annoy the other; (2) after receiving a reasonable warning or request to stop by or on behalf of the other; and (3) without legal purpose.

A person may not use an interactive computer service to maliciously engage in a course of conduct that inflicts serious emotional distress on a minor or places a minor in reasonable fear of death or serious bodily injury with the intent (1) to kill, injure, harass, or cause serious emotional distress to the minor or (2) to place the minor in reasonable fear of death or serious bodily injury.

A person may not maliciously engage in an electronic communication if (1) the electronic communication is part of a series of communications and has the effect of intimidating or harassing a minor and causing physical injury or serious emotional distress to a minor and (2) the person engaging in the electronic communication intends to intimidate or harass the minor and cause physical injury or serious emotional distress to the minor.

A person may not maliciously engage in a single significant act or course of conduct using an electronic communication if:

- the person's conduct, when considered in its entirety, has the effect of intimidating or harassing a minor and causing physical injury or serious emotional distress to a minor;
- the person intends to intimidate or harass the minor and cause physical injury or serious emotional distress to the minor; and
- in the case of a single significant act, the communication (1) is made after receiving a reasonable warning or request to stop; (2) is sent with a reasonable expectation that the recipient would share the communication with a third party; or (3) shocks the conscience.

A person may not maliciously engage in electronic conduct if (1) the act of electronic conduct has the effect of intimidating or harassing a minor and causing physical injury or serious emotional distress to a minor and (2) the person intends to intimidate or harass the minor and cause physical injury or serious emotional distress to the minor.

The above prohibitions do not apply to a peaceable activity intended to express a political view or provide information to others or conducted for a lawful purpose.

A person convicted of violating one of the aforementioned crimes is guilty of a misdemeanor and subject to imprisonment of up to three years and/or a maximum fine of $10,000.

A person may not violate these provisions with the intent to induce a minor to commit suicide. Such violators are guilty of a misdemeanor and subject to maximum penalties of 10 years' imprisonment and/or a $10,000 fine.

Under these provisions, "electronic communication" means the act of transmitting any information, data, writing, image, or communication by the use of a computer or any other electronic means, including a communication that involves the use of email, an instant messaging service, an Internet website, a social media application, a network call, a facsimile machine, or any other Internet-based communication tool.

Family Educational Rights and Privacy Act

At the federal level, the Family Educational Rights and Privacy Act (FERPA) of 1974 governs the privacy of student data. FERPA generally prohibits the disclosure by schools that receive federal education funding of personally identifiable information from a student's education record unless the educational institution has obtained signed and dated written consent from a parent or eligible student or one of FERPA's exceptions applies. An education record includes a range of information about a student.

FERPA's exceptions are not always well understood, which leads to some believing that no information about a student may be disclosed without facing a lawsuit, even in the face of health or safety concerns. However, federal regulations (34 CFR 99.36) specifically address these circumstances so that an institution may disclose personally identifiable information from an education record to appropriate parties, including parents of an eligible student, in connection with an emergency if knowledge of the information is necessary to protect the health or safety of the student or other individuals.

However, federal regulations (34 CFR 99.3 and 99.37) may allow a school to disclose a student's "directory information" to a third party without the student's or student's parent's consent if the school has given public notice of (1) the information designated as "directory information;" (2) the student's or parent's right to restrict disclosure of such information; and (3) the time period within which a student or parent may notify the school that they would like to restrict any or all of the information from the designation of "directory information." "Directory information" often includes the student's name, address, telephone number, date and place of birth, participation in officially recognized activities and sports, and dates of attendance.

In addition, not all information that comes into the hands of an educator, administrator, or other school staff is an "education record" subject to FERPA restrictions. Two particular sources of information are outside FERPA's definition of "education record": (1) information an educator learns through personal observation, peer reports, or social media; and (2) records of school security personnel, which are governed under a specific exception to FERPA. Therefore, this information may be disclosed outside of FERPA.

Penalties for violations of FERPA include loss of federal funding.

Additional Information

Recent Prior Introductions: Similar legislation has not been introduced within the last three years.

Designated Cross File: None.

Information Source(s): Anne Arundel, Frederick, and Montgomery counties; Maryland State Commission on Criminal Sentencing Policy; Judiciary (Administrative Office of the Courts); Office of the Public Defender; Maryland State Department of Education; University System of Maryland; U.S. Department of Education; Department of Legislative Services

Fiscal Note History: First Reader - February 25, 2025
rh/aad

Analysis by: Amanda L. Douglas

Direct Inquiries to:
(410) 946-5510
(301) 970-5510