Department of Legislative Services

Maryland General Assembly
2024 Session

FISCAL AND POLICY NOTE
First Reader

Senate Bill 1089 (Senator M. Washington)
Education, Energy, and the Environment

Education - Student and School Employee Data Privacy - Protections

This bill applies the same data privacy protections afforded to students under the Student Data Privacy Act to school employees, as well. The bill also requires the protections to apply for students and employees of a virtual school and clarifies that the protections apply to a website, service, or an application that uses artificial intelligence (AI).

Fiscal Summary

State Effect: None. The bill is directed at operators of specified websites, online services, online applications, and mobile applications.

Local Effect: No material effect on local finances. Local school systems may need to adjust their procurement and contract management practices to ensure that digital vendors comply with the bill's requirements, and/or limit the websites, online services, online applications, and mobile applications that they use.

Small Business Effect: Potential meaningful.

Analysis

Bill Summary/Current Law: The Student Data Privacy Act requires an operator of specified websites, online services, online applications, and mobile applications to:

- protect covered information, which includes specified personal information about a student such as name, address, phone number, socioeconomic status, food purchases, and photos, from unauthorized access, destruction, use, modification or disclosure;

- implement and maintain reasonable security procedures and practices to protect covered information; and
- if covered information is under the authority of a public school or local school system in accordance with a contract or an agreement, delete within a reasonable time the covered information if the public school or local school system requests deletion of the covered information.

The Act includes specifications for the types of websites, services, and applications to which the Act applies; certain activities that an operator is explicitly prohibited from undertaking; how and when an operator is authorized to use and/or disclose a student's covered information, including to law enforcement agencies under specified circumstances; the transfer of responsibility when an operator is merged with or acquired by another entity; the rights of an operator in following the Act's requirements; and the limitations of the Act.

The *bill* applies each of the specifications for students under the Act to also apply to school employees and, as a result, an operator of specified websites, online services, online applications, and mobile applications must protect student and school employee data and personal information in the same manner.

For information on the status of AI in the nation and State, please see the **Appendix – Artificial Intelligence**.

Small Business Effect: Small business operators of websites, online services, online applications, and mobile applications may need to change their business practices or they will not be able to conduct business with local school systems, public schools, or public school teachers.

Additional Information

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

Designated Cross File: None.

Information Source(s): Maryland Longitudinal Data System Center; Office of the Attorney General (Consumer Protection Division); Maryland State Department of Education; Baltimore City Public Schools; Baltimore County Public Schools; Montgomery County Public Schools; Department of Legislative Services

Fiscal Note History: First Reader - February 21, 2024
km/mcr

Analysis by: Richard L. Duncan

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

Appendix – Artificial Intelligence

Artificial Intelligence – Generally

Artificial intelligence (AI) is a broad field of computer science that deals with the creation of "intelligent" systems that can reason, learn, and act autonomously. There are many different branches of AI, each with its own focus and set of techniques, such as machine learning, neural networks, robotics, expert systems, fuzzy logic, and natural language processing. AI research has been successful in developing algorithms for solving a wide range of problems, from game playing to conversation simulation.

Though a variety of forms of AI are now in use, experts have not established an agreed-upon definition for the technology. An early definition in 1955 branded AI as "making a machine behave in ways that would be called intelligent if a human were so behaving." A more recent and expansive consensus definition of AI emerging in academic circles as cited by Stuart Russell and Peter Norvig in their computer science textbook *Artificial Intelligence: A Modern Approach*, defines it as "the designing and building of intelligent agents that receive percepts from the environment and take actions that affect that environment."

In Executive Order 01.01.2024.02, which is discussed in more detail below, for State regulatory purposes, AI means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.

History of Artificial Intelligence

Though the general public's awareness of AI may be relatively recent, AI has existed conceptually for nearly 70 years. In 1950, Alan Turing, the English mathematician and computer scientist, wrote Computing Machinery and Intelligence, one of the first papers that posed the question of whether machines can think. The phrase "artificial intelligence" was first coined in 1956 at an academic conference on the subject. From 1964 to 2017, numerous developments were made in the field, including the Massachusetts Institute of Technology's "ELIZA," a chatbot that simulates conversation; IBM's Watson, a cognitive computing platform that uses AI to help businesses and individuals make decisions; and Apple's Siri, a voice assistant for consumers that uses speech recognition.

More recently, in November 2022, OpenAI's ChatGPT (Chat Generative Pre-Trained Transformer) was released for public beta testing and by January 2023 had become one of the fastest growing consumer software applications in history, gaining more than 100 million users in that time. As users interact with the software, the software learns from the conversations and improves its capabilities. The continued development of this and other generative AI software systems is drawing the attention of policymakers to better understand the technology, regulate it to protect individuals from potential risks, and promote the development of safe applications of the technology.

Major Risks – Data Privacy, Bias, and Academic Integrity

Although data privacy has been a matter of concern since the advent of the Internet, the complexity of the algorithms that power AI has prompted interest in government regulation of the technology to prevent the improper or unethical use of personal data. However, regulation of this aspect of AI is sometimes challenging due to intellectual property claims and resistance by the private owners of these technologies to allow exploration of the internal workings of their systems.

As AI algorithms and neural networks are trained by humans, existing societal discriminations can be incorporated into the internal and inherent biases of the data sets that AI systems use and can affect the way an AI model functions. One set of AI functions that has been identified as potentially having some bias is the use of facial recognition software in security or policing contexts. In use by various law enforcement agencies throughout the nation, this software has been shown to be prone to error and unable to accurately recognize people of color, women, and young people. Similarly, some AI software designed to screen resumes for employment consideration has been found to be biased against minorities, women, and older individuals.

Academic institutions, including secondary and postsecondary institutions, have also raised concerns about AI's potential to compromise academic integrity. Generative AI systems can produce written works in response to prompts that can be presented by students as their work product. These institutions have struggled to develop policies and practices to limit the potential for such adverse uses of AI.

Federal Initiatives

The National Artificial Intelligence Initiative Act of 2020 became law on January 1, 2021. The aim of the Act is to promote U.S. leadership in AI research and development with the goal of accelerating the nation's economic prosperity and national security through the development and use of trustworthy AI in the public and private sectors and preparation of the workforce for the inevitable integration of AI systems. This multi-agency initiative has included work by the U.S. Department of Energy, in consultation with the National

Institute of Standards and Technology, to develop the AI Risk Management Playbook as a reference guide to support responsible and trustworthy AI use and development. Though not a binding document, the playbook addresses common AI risks and steps that AI leaders, practitioners, and procurement teams can take to manage data privacy and bias risks.

In addition, the White House introduced its Blueprint for an AI Bill of Rights, a set of five principles and associated practices (safe and effective systems; algorithmic discrimination protections; data privacy; notice and explanation; and human alternatives, consideration, and fallback) to help guide the design and deployment of automated systems to protect the rights and opportunities of the public, as well as public access to critical resources and services, and to serve as a guide for how new AI resources are developed. The blueprint is designed to apply to speech-related systems, surveillance and criminal justice algorithms, voting-related systems, and any other systems that could lead to potential algorithmic discrimination.

In October 2023, the White House issued an executive order to establish new standards for AI safety and security and direct actions that aim to protect privacy of Americans, advance equity and civil rights, protect consumers and workers, and promote innovation and competition.

Maryland Law

Maryland has certain statutes in effect that govern AI directly or indirectly. The Department of Information Technology and the Secretary of Information Technology are statutorily responsible for annually evaluating the feasibility of units of State government providing public services using AI, machine learning, commercial cloud computer services, device-as-a-service procurement models, and other emerging technologies.

Indirectly, Chapter 446 of 2020 prohibits employers from using facial recognition services to create facial templates of job applicants without their consent, and Chapter 41 of 2022 requires courts to consider the results of algorithmic tools before detaining juveniles. Additionally, Maryland's broader consumer protection and data privacy laws, such as the Consumer Protection Act and the Maryland Personal Information Protection Act (MPIPA), offer certain protections against AI-related risks. For example, MPIPA requires businesses that collect, maintain, or license personal information to implement reasonable security measures.

Regulatory Framework by Executive Order

In January 2024, the Governor issued Executive Order 01.01.2024.02 to direct, guide, and regulate the use of AI by State agencies. Primarily, the executive order establishes an AI subcabinet to, among other things, (1) promote the foundational principles that State

agencies must adhere to when using AI (*i.e.*, fairness, equity, privacy, safety, validity, and transparency); (2) provide advice and recommendations to the Governor on the use of AI; (3) facilitate statewide coordination on the responsible, ethical, and productive use of AI; (4) develop an AI action plan to operationalize the AI principles; (5) find, evaluate, and offer training programs for state workers on the use of AI; and (6) study and make recommendations to the Governor and General Assembly on how AI affects the State workforce, economic development, and security.