ARTIFICIAL INTELLIGENCE

Overview

In May, **Colorado** enacted SB 205/Chapter 198, the most sweeping artificial intelligence (AI) law in the country. Effective upon enactment, it provides consumer protections for artificial intelligence and requires developers of high-risk systems to use reasonable care to avoid algorithmic discrimination in the high-risk system. The law also includes provisions that will:

- Require AI developers and those who use AI systems for lending approval or denial decisions, to make, and regularly update, disclosures to the Colorado attorney general;
- Require developers to notify the attorney general if they determine their AI systems have caused "algorithmic discrimination" in their consumer lending and finance decisions;
- Require AI deployers to notify consumers when they use an AI system to make consumer lending and finance decisions, give the consumer the right to opt out of the AI system review, and provide the consumer with an opportunity to appeal the AI system's decision.

A wide range of organizations from industries like financial services, tech, and healthcare advocated against the law because of the risk it poses to businesses. In a joint comment letter to Democratic Governor Jared Polis, these groups argued that AI is providing opportunities for companies to innovate and solve problems for their customers and that the new law would put these innovations at risk.[1] SB 205/Chapter 198 also gives the attorney general broad rulemaking authority, which creates even more uncertainty for businesses. In addition, the comment letter makes the case that Colorado's employment and labor, anti-discrimination, and character defamation laws already provide robust protections for consumers that are not dependent on whether a specific technology is utilized.

Governor Polis signed the bill "with reservations," as mentioned in his signing statement, and noted that the long timeline for implementation gave "guardrails." Governor Polis also encouraged the legislature to "work closely with stakeholders to craft future legislation . . . that will amend this bill[.]"

A similar bill in **Connecticut**, SB 2, died when the legislature adjourned on May 8. Just before this, Connecticut Democratic Governor Ned Lamont urged caution against the passage of SB 2, saying "…you don't begin to know what the potential is for AI, so it's pretty tough to regulate

[1] AFSA, *Colorado SB 205 re: Artificial Intelligence*, at https://afsaonline.org/afsa_resource/colorado-sb-205-re-artificial-intelligence/ (May 24, 2024).

something that you're just beginning to get some feel for… you shouldn't have one state doing it. You should have us do this as a collective."[2]

The first government body to focus on regulating privacy concerns was the European Union (EU). The General Data Protection Regulation (GDPR)[3] was introduced in 2016 and included measures regulating AI.[4] Adopted on April 2016 and implemented in May 2018, this regulation became the model for laws around the world, including the California Consumer Privacy Act (CCPA) that was adopted in June 2018. In 2022, the EU proposed the AI Act, the first AI law that could be passed by a major regulator. This proposal separates AI algorithms into three risk areas: risk of unacceptable menace, which would be prohibited; risk that is high but would be allowable with strict constraints; and risk that is low and would be allowed with perceptible limits.[5] This act could provide a template for AI regulation in the same way that the GDPR paved the way for data protection in the U.S.

AI and Financial Services

AI and algorithms are transforming industries, including financial services. They are already being used within the industry to improve operations and benefit consumers. As the technology has developed, AI and machine learning have affected payment systems in many beneficial ways, including:[6]

- Improved and more sophisticated fraud detection;
- Increased accuracy and efficiency of underwriting;
- Higher quality assessment of data collected to better know customers;
- Automated customer service interactions.

In the credit underwriting process, algorithms can be used to eliminate some of the human error and bias that inherently exists in human interaction. This can make credit decisions more accurate, fair, faster and more affordable by judging applicants on their credit worthiness.[7] Automation can help at all steps of the credit approval process: collecting financial data and other mandatory information from customers, assisting in financial spreading, and even making the final decision to approve or deny the loan. An overarching benefit to all this automation is the

---

[2] The Register Citizen, *Proposed bill on artificial intelligence regulation in CT dies after Gov. Ned Lamont threatens veto* at https://www.registercitizen.com/politics/article/if-bill-ai-survives-ct-house-vote-lamont-19444053.php (May 7, 2024).
[3] EUR-Lex, *General Data Protection Regulation*, at https://eur-lex.europa.eu/eli/reg/2016/679, (2016).
[4] GDPR.EU, *What is the GDPR, the EU's new data protection law?*, at https://gdpr.eu/what-is-gdpr/ (Accessed June 21, 2024).
[5] Future of Life Institute, EU Artificial Intelligence Act, at https://artificialintelligenceact.eu/ai-act-explorer/ (Accessed June 27, 2024).
[6] Barclays, *AI Payments Revolution*, at https://www.barclayscorporate.com/insights/innovation/aipaymentsrevolution/#aiandkyc, (April 26, 2019).
[7] AFSA, *District of Columbia B24-0558 Joint Comment Letter*, at https://afsaonline.org/wpcontent/uploads/2022/10/Joint-comment-letter-DC-B24-0558-Algorithms-1.pdf (October 6, 2022).

time saved for credit analysts to focus on other things.[8] Importantly, an algorithm allows for processing of more pieces of information than possible through human interaction, which further limits the impact of any single variable on the final decision. Fraud detection and prevention is another area where artificial intelligence can improve over human performance. Detecting fraudulent patterns typically consists of processing large multi-country data sets, as fraudsters will use similar methods from one country to another and then attempt to take them globally. Artificial intelligence can process this information faster than humans and is able to identify more complex patterns. A machine learning system could analyze more data and react to new, suspicious behaviors faster.[9] For example, a payment services provider in Europe found its fraud monitoring and prevention model immediately reduced fraud by 25 percent and could reduce it by an estimated 40 percent as the model continues to learn.[10]

Legislative Analysis

During the 2021-2022 legislative session, the **District of Columbia** Council introduced an omnibus bill B24-0558 that would have affected algorithm use across industries if it had been enacted. Titled the "Stop Discrimination by Algorithm Act of 2021," the bill was introduced on December 9, 2021, accompanied by a letter of support from Democrat Attorney General Karl Racine. The bill was last considered at a hearing held on September 22, 2022. AFSA testified during the September 22 hearing[11] and submitted a joint trade letter[12] for the record expressing numerous concerns with the legislation. The bill died at the end of the legislative session but an identical version with a new title was reintroduced during the current session as B25-0114. It was referred to the Business and Economic Development Committee and the Judiciary and Public Safety Committee on February 7.

This bill would prohibit the use of algorithmic decision-making to discriminate in any manner; inadvertently banning many beneficial uses of AI algorithms and other automated decision-making tools through other requirements. The bill would require multiple disclosures to individuals whose personal information was collected and separate notices to individuals subject to any adverse action resulting from an algorithm. This bill would also require extensive auditing and annual reporting to the attorney general. Either the attorney general's office or a private citizen could enforce violations through a civil right of action.

Although few are as sweeping as the bills in **Colorado** or the District of Columbia, other states have begun introducing legislation addressing artificial intelligence:

---

[8] Moody's Analytics, *Maximize Efficiency: How Automation Can Improve Your Loan Origination Process*, at https://www.moodysanalytics.com/articles/2018/maximize-efficiency-how-automation-can-improve-your-loanorigination-process (November 2018).
[9] Deloitte, *Automation is the future of fraud risk management*, at https://www2.deloitte.com/in/en/pages/finance/topics/forensic/automation-is-the-future-of-fraud-riskmanagement.html (Accessed April 20, 2023).
[10] KPMG*, Fighting Fraud with a Model of Models*, at https://assets.kpmg.com/content/dam/kpmg/dk/pdf/dk2020/04/Nets-KPMG-Fighting-Fraud-with-a-Model-of-Models-whitepaper-2020.pdf (April, 21, 2020).
[11] American Financial Services Association, *Testimony - DC-B24-0558*, at https://afsaonline.org/?s=Testimony+-+DC-B24-0558, (September 22, 2022).
[12] American Financial Services Association, *Comment Letter - DC-B24-0558*, at https://afsaonline.org/?s=Comment+Letter+-+DC-B24-0558, (October 6, 2022).

California AB 2930 is scheduled to be heard before the Senate Judiciary Committee on July 2. This bill would require agencies using automated decision tools to make consequential decisions, such as determining the cost or terms of financial services provided by a mortgage company, to perform an impact assessment for any automated decision tool the deployer uses that includes, among other things, a statement of the purpose of the automated decision tool and its intended benefit, uses, and deployment context. The bill would also:

- Prohibit a deployer from using an automated tool that results in algorithmic discrimination;
- Require deployers to notify natural people if they are the subject of a consequential decision that an automated tool is being used to make;
- Authorize civil actions being brought against a deployer for violations. Violations involving algorithmic discrimination would equal $25,000 per violation.

The bill does include a 45 day right to cure provision.

New Jersey AB 1902 was introduced and referred to the Assembly Science, Innovation and Technology Committee on January 9 and awaits further action. In instances in which a legal entity would process and use personally identifiable information, this bill would make it so that no consumer would be bound to a decision from the legal entity that is determined solely by an automated decision-making process.

Companion bill SB 2052 was introduced and referred to the Senate Commerce Committee and awaits further action.

Rhode Island HB 7521 was held for further study in the House Innovation, Internet and Technology Committee on February 15 and awaits further action. This bill would require any corporation using an automated decision tool to make a consequential decision, including decisions related to financial services, to notify any person impacted by the decision about the use of an automated tool. Additionally, this bill would instruct the user of the automated decision tool to conduct an annual impact assessment of the tool regarding specific information related to its use. The bill would also require the developer of the automated decision tool or the corporation using the tool to provide safeguards against algorithmic discrimination. If enacted, this bill would take effect immediately.

Rhode Island SB 2888 was held for further study in the Senate Judiciary Committee on April 11 and awaits further action. This bill would require any entity or corporation using any system that utilizes artificial intelligence with the intended purpose of determining consequential decisions to perform, implement and maintain a risk management program to identify risks of using the program and, if applicable, the steps used to retrain the system and notify individuals impacted. This bill would demand that an impact assessment be conducted prior to deployment of the program and annually thereafter. If enacted, this bill would take effect on January 1, 2026.

Utah SB 149 was signed into law by Republican Governor Spencer Cox on March 13. Effective on May 1, this law created the "Artificial Intelligence Policy Act" and established liability for

use of AI that violates consumer protection laws if not properly disclosed. It also created the Office of AI Policy and a regulatory AI policy program, as well as including a few other provisions.

Conclusion

AFSA members are committed to ensuring that state AI regulation is reasonable and does not add duplicative layers on top of existing law that provides the same protection. AFSA will continue to work with stakeholders to discuss concerns on AI and develop solutions.