Insights

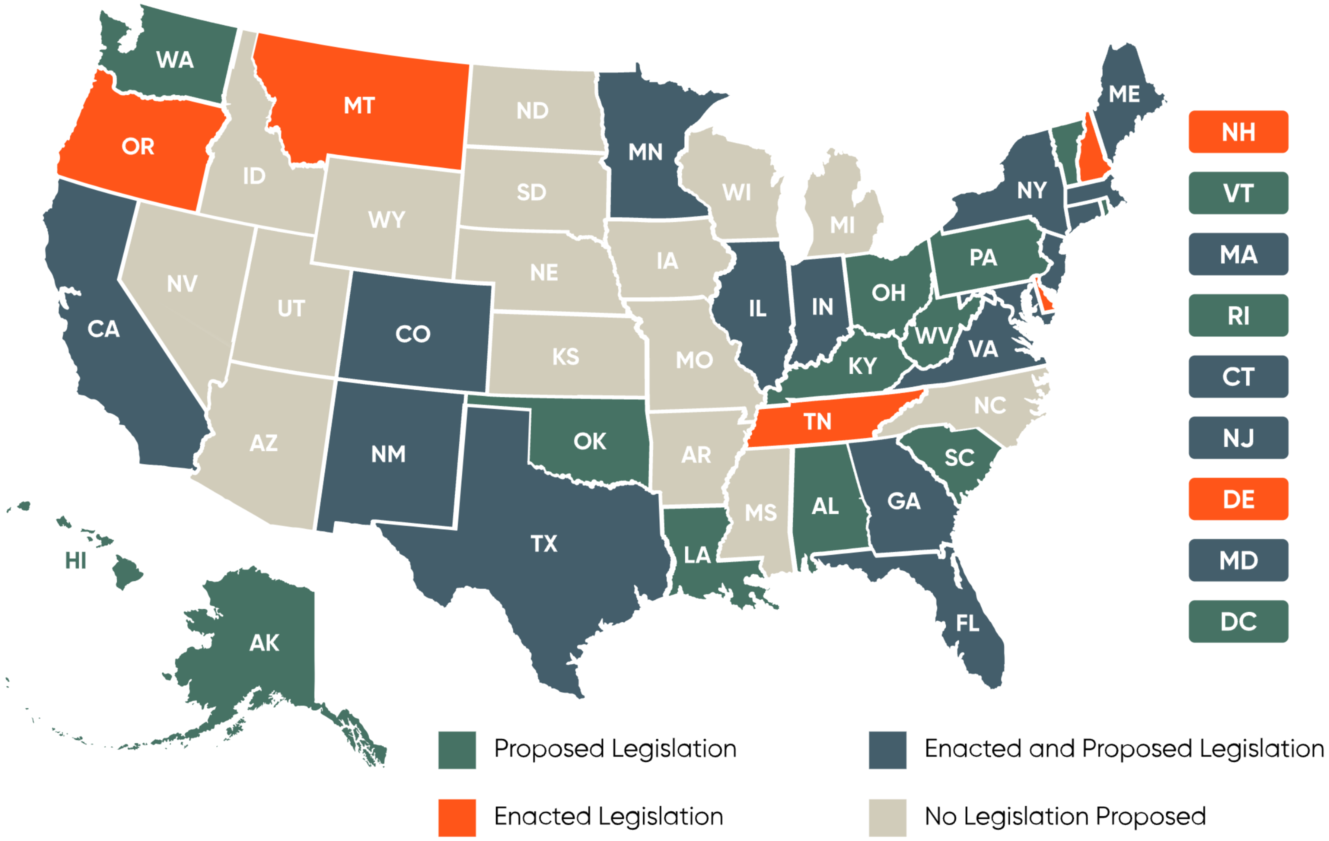
US STATE-BY-STATE AI LEGISLATION SNAPSHOT

SUMMARY

BCLP actively tracks the proposed, failed and enacted AI regulatory bills from across the United States to help our clients stay informed in this rapidly-changing regulatory landscape. The interactive map is current as of June 7, 2024, and will be updated quarterly to include legislation that if passed would directly impact a businesses' development or deployment of AI solutions.[2]

Artificial Intelligence (AI), once limited to the pages of science fiction novels, has now been adopted by more than 1/3 of businesses in the United States, and even more organizations are working to embed AI into current applications and processes.[1] As companies increasingly integrate AI in their products, services, processes, and decision-making, they need to do so in ways that comply with the different state laws that have been passed and proposed to regulate the use of AI.

Click the image below to view detailed state-by-state AI legislation information.



As is the case with most new technologies, the establishment of regulatory and compliance frameworks has lagged behind AI's rise. This is set to change, however, as AI has caught the attention of federal and state regulators and oversight of AI is ramping up.

In the absence of comprehensive federal legislation on AI, there is now a growing patchwork of various current and proposed AI regulatory frameworks at the state and local level. Even with the federal bill uncertain, it is clear that momentum for AI regulation is at an all-time high. Consequently, companies stepping into the AI stream, face an uncertain regulatory environment that must be closely monitored and evaluated to understand its impact on risk and the commercial potential of proposed use cases.

To help companies achieve their business goals while minimizing regulatory risk, BCLP actively tracks the proposed and enacted AI regulatory bills from across the Unites States to enable our clients to stay informed in this rapidly-changing regulatory landscape. The interactive map below is current as of June 7, 2024, and will be updated quarterly to include legislation that if passed would directly impact a business's development or deployment of AI solutions.[1] Click the states to learn more.

We have also created an AI regulation tracker for the UK and EU to keep you informed in this rapidly changing regulatory landscape.

[1]IBM Global AI Adoption Index 2023.

[2]We have also included laws addressing automated decision-making, because AI and automation are increasingly integrated, noting that not all automated decision-making systems involve AI, such businesses will need to understand how their particular systems are designed. We have omitted biometric data, facial recognition, and sector-specific administrative laws.

CALIFORNIA

Enacted

Introduced in 2018 as SB 1001, The Bolstering Online Transparency Act (BOT), went into effect in July 2019. BOT makes it unlawful for a person or entity to use a bot to communicate or interact online with a person in California in order to incentivize a sale or transaction of goods or services or to influence a vote in an election without disclosing that the communication is via a bot. The law defines a “bot” as “an automated online account where all or substantially all of the actions or posts of that account are not the result of a person.” The law applies only to communications with persons in California. In addition, it applies only to public-facing websites, applications, or social networks that have at least 10 million monthly U.S. visitors or users. BOT does not provide a private right of action.

Enacted

The California Consumer Privacy Act, as amended by the California Privacy Rights Act (CCPA) governs profiling and automated decision-making. The CCPA gives consumers opt-out rights with respect to businesses’ use of “automated decision-making technology,” which includes “profiling” consumers based on their “performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.” The CCPA defines “profiling” as “any form of automated processing of personal information, as further defined by regulations pursuant to paragraph (16) of subdivision (a) of Section 1798.185 [of the CCPA], to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements,” leaving the scope relatively undefined. The CCPA also requires businesses to conduct a privacy risk assessment for processing activities that present “significant risk” to consumers’ privacy or security. “Significant risk” is not defined by the CCPA but may be fleshed out by the regulations.

As of the date of publication, regulations addressing automated decision-making have not been published.

Proposed

Introduced on January 31, 2024, AB2013, would require, on or before January 1, 2026, a developer of an artificial intelligence system or service made available to Californians for use, regardless of whether the terms of that use include compensation, to post on the developer's internet website documentation regarding the data used to train the artificial intelligence system or service, as specified.

Proposed

Introduced on January 25, 2024, SB970, this bill would require any person or entity that sells or provides access to any artificial intelligence technology that is designed to create synthetic images, video, or voice to provide a consumer warning that misuse of the technology may result in civil or criminal liability for the user. The bill would require the Department of Consumer Affairs to specify the form and content of the consumer warning and would impose a civil penalty for violations of the requirement. Failure to comply with consumer warning requirement would be punishable by a civil penalty not to exceed twenty-five thousand dollars ($25,000) for each day that the technology is provided to or offered to the public without a consumer warning.

Failed

Introduced on January 30, 2023, AB 331, would, among other things, require an entity that uses an automated decision tool (ADT) to make a consequential decision (deployer), and a developer of an ADT, to, on or before January 1, 2025, and annually thereafter, perform an impact assessment for any ADT used that includes, among other things, a statement of the purpose of the ADT and its intended benefits, uses, and deployment contexts. The bill requires a deployer or developer to provide the impact assessment to the Civil Rights Department within 60 days of its completion. Before using an ADT to make a consequential decision deployers must notify any natural person that is the subject of the consequential decision that the depoloyer is using an ADT to make, or be a controlling factor in making, the consequential decision. Deployers are also required to accommodate a natural person’s request to not be subject to the ADT and to be subject to an alternative selection process or accommodation if a consequential decision is made solely based on the output of an ADT, assuming that an alternate process is technically feasible. This bill would also prohibit a deployer from using an ADT in a manner that contributes to algorithmic discrimination. Finally, the bill includes a private right of action which would open the door to significant litigation risk for users of ADT.

COLORADO

Enacted

In 2021, Colorado enacted SB 21-169, Protecting Consumers from Unfair Discrimination in Insurance Practices, a law intended to protect consumers from unfair discrimination in insurance rate-setting mechanisms. The law applies to insurers’ use of external consumer data and information sources (ECDIS), as well as algorithms and predictive models that use ECDIS in "insurance practices," that "unfairly discriminate" based on race, color, national or ethnic origin, religion, sex, sexual orientation, disability, gender identity, or gender expression.

On February 1, 2023, the Colorado Division of Insurance (CDI) released a draft of the first of several regulations to implement the bill.

On February 1, 2023, the Colorado Division of Insurance (CDI) released a draft of the first of several regulations to implement the bill. On September 21, 2023, the CDI adopted Regulation 10-1-1 - Governance and Risk Management Framework Requirements for Life Insurers. The regulation governs the use of algorithms and predictive models that use external consumer data and information sources (ECDIS). Among other things, the regulation requires all Colorado-licensed life insurers to submit a compliance progress report on June 1, 2024, and an annual compliance attestation beginning on December 1, 2024.

Enacted

The Colorado Privacy Act (CPA), which goes into force on July 1, 2023, provides consumers the right to opt-out of the processing of their personal data for purposes of "profiling in furtherance of decisions that produce legal or similarly significant effects." The law defines those decisions as "a decision that results in the provision or denial of financial and lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services, or access to essential goods or services." The CPA further requires that controllers conduct a data protection impact assessment (DPIA) if the processing of personal data creates a heightened risk of harm to a consumer. Processing that presents a heightened risk of harm to a consumer includes profiling if the profiling presents a reasonably foreseeable risk of:

- Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;
- Financial or physical injury to consumers;
- A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers if the intrusion would be offensive to a reasonable person; or
- Other substantial injury to consumers.

All of which means that deployers of automated-decision making (which may or may not use AI) need to ensure that their design and implementation do not create the heightened risks outlined above, and are included in their DPIA. On March 15, 2023, the Colorado Attorney General's Office finalized rules implementing the CPA.

CONNECTICUT

Enacted

The Connecticut Privacy Act (CTPA) which goes into force on July 1, 2023, provides consumers the right to opt-out of profiling if such profiling is in furtherance of automated decision-making that produces legal or other similarly significant effects. Controllers must also perform data risk assessments prior to processing consumer data when such processing presents a "heightened risk of harm." These situations include certain profiling activities that present a reasonably foreseeable risk of unfair or deceptive treatment of or unlawful disparate impact on consumers, financial, physical or reputational injury to consumers, physical or other intrusion into the solitude, seclusion or private affairs or concerns of consumers that would be offensive to a reasonable person, or other substantial injury to consumers.

Proposed

Introduced on January 29, 2024, HB 1147, would create a statutory scheme to regulate the use of deepfakes produced using generative artificial intelligence in communications about candidates for elective office. HB1147 would prohibit the distribution of a communication that includes an undisclosed deepfake with actual malice as to the deceptiveness or falsity of the communication related to a candidate for public office. Violators would be subject to civil penalties. Additionally, a candidate who is the subject of a communication that includes a deepfake and does not comply with the disclosure requirements may bring a civil action for injunction or for general or special damages or both.

DELAWARE

Enacted

The Delaware Personal Data Privacy Act which goes into force on January 1, 2025 provides consumers the right to opt-out of profiling if such profiling is in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer. Controllers must also perform data protection assessments when data processing presents a "heightened risk of harm" including where Controller processes personal data for the purposes of profiling, where such profiling presents a reasonably foreseeable risk of any of the following: (a) unfair or deceptive treatment of, or unlawful disparate impact on, consumers, (b) financial, physical, or reputational injury to consumers, (c) a physical or other intrusion upon the solitude or seclusion, or private affairs or concerns, of consumers, where such intrusion would be offensive to a reasonable person; or (d) other substantial injury to consumers.

DISTRICT OF COLUMBIA

Failed

Introduced on February 2, 2023, B114, Stop Discrimination by Algorithms Act of 2023 (SDAA) would prohibit would prohibit both for-profit and nonprofit organizations from using algorithms that make decisions based on protected personal traits. This bill makes it unlawful for a DC business to make a decision stemming from an algorithm if it is based on a broad range of personal characteristics, including actual or perceived race, color, religion, national origin, sex, gender identity or expression, sexual orientation, familial status, source of income or disability in a manner that makes “important life opportunities” unavailable to that individual or class of individuals. Any covered entity or service provider who violates the act would be liable for a civil penalty of up to $10,000 per violation.

FLORIDA

Proposed

Introduced on January 19, 2024, SB 850, the *Use of Artificial Intelligence in Political Advertising*, would take effect July 1, 2024, if enacted, aims to require political campaigns to disclose through a disclaimer the use of AI in any “mages, video, audio, text, and other digital content used in ads. This bill seeks to address the rising concern of deceptive campaign advertising (deepfakes) by mandating disclaimers on political ads that contain certain content generated through artificial intelligence. Generative artificial intelligence is defined as a “machine based system that can for a given set of human defined objectives emulate the structure and characteristics of input data in order to generate derived synthetic content.” Violators of this proposed legislation could face civil penalties. Anyone can file a complaint with the Florida Elections Commission if they have suspicions of violations. This bill would apply to anyone person or entity releasing a political advertisement, electioneering communication, or other miscellaneous advertisement.

GEORGIA

Proposed

Introduced on January 9, 2024, H4696

"Profiling" means “any form of solely automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.” If passed, the act would take effect immediately.

Proposed

Introduced on January 9, 2024, H4660 would require that “a person, corporation, committee, or other entity shall not, within ninety days of an election at which a candidate for elective office will appear on the ballot, distribute a synthetic media message that the person, corporation, committee, or other entity knows or should have known is a deceptive and fraudulent deepfake of a candidate on the ballot." If passed, the act would take effect immediately.

Proposed

Introduced on January 16, 2024, H4842, the South Carolina Age-Appropriate Design Code Act would apply to any business operating in South Carolina that either: "(i) has annual gross revenues more than twenty-five million dollars, as adjusted every odd-numbered year to reflect the Consumer Price Index; (ii) alone or in combination, annually buys, receives for the covered entity's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal data of fifty thousand or more consumers, households, or devices; or (iii) derives fifty percent or more of its annual revenues from selling consumers' personal data."

Covered entities would be prohibited from "profiling" children under age 18 by default unless both of the following criteria are met: " (a) the covered entity can demonstrate it has appropriate safeguards in place to ensure that profiling is consistent with the best interests of children reasonably likely to access the online service, product, or feature; and (b) either of the following is true: (i) profiling is necessary to provide the online service, product, or feature requested and only with respect to the aspects of the online service, product, or feature with which a child is actively and knowingly engaged; or (ii) the covered entity can demonstrate a compelling reason that profiling is in the best interests of children."

"Profiling" means "any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. 'Profiling' does not include the processing of information that does not result in an assessment or judgment about a natural person."

Failed

Introduced on January 18, 2023, SB404, would prohibit any operator of a website, an online service, or an online or mobile application, including any social media platform, to utilize an automated decision system (ADS) for content placement, including feeds, posts, advertisements, or product offerings, for a user under the age of eighteen. In addition, an operator that utilizes an ADS for content placement for residents of South Carolina who are eighteen years or older shall perform an age verification through an independent, third-party age-verification service, unless the operator employs the bill's prescribed protections to ensure age verification. The bill includes a private right of action.

HAWAII

Proposed

Introduced on January 20, 2023, SB974, the Hawaii Consumer Data Protection Act, would establish a framework to regulate controllers and processors' access to personal consumer data and introduces penalties, as well as a new consumer privacy special fund.

The bill also provides consumers the option to opt-out of the processing of their personal data for the purposes of “profiling in furtherance of decisions made by the controller that results in the provision or denial by the controller of financial and lending services, housing, insurance; education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities, including food and water.” "Profiling" is defined as any-form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation; health, personal preferences, interests, reliability, behavior, location, or movements.

The bill further requires covered entities to conduct a data protection assessment when they process personal data for purposes of profiling and the profiling presents “a reasonably foreseeable risk of: (A) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (B) Financial, physical, or reputational injury to consumers; (C) A physical intrusion or other intrusion upon the solitude or seclusion, or the private affairs or concerns; of consumers, where the intrusion would be offensive to a reasonable person; or (D) Other substantial injury to consumers[.]” The law goes into effect July 1, 2050, as currently drafted. The bill stalled in 2023 but was picked back up and carried over to the 2024 regular legislative session.

Proposed

Introduced on January 20, 2023, SB1110, an alternate version of the Hawaii Consumer Data Protection Act, would create materially similar obligations with respect to “profiling” as SB974. The bill stalled in 2023 but was picked back up and carried over to the 2024 regular legislative session.

ILLINOIS

Enacted

In 2019, Illinois became the first state to enact restrictions with respect to the use of AI in hiring. The Illinois AI Video Interview Act was amended in 2021 and went into effect in 2022, and now requires employers using AI-enabled assessments to:

- Notify applicants of AI use;
- Explain how the AI works and the “general types of characteristics” it uses to evaluate applicants;
- Obtain their consent;

- Share any applicant videos only with service providers engaged in evaluating the applicant;
- Upon an applicant's request, destroy all copies of the applicant's videos and instruct service providers to do so as well; and
- Report annually, after use of AI, a demographic breakdown of the applicants they offered an interview, those they did not, and the ones they hired.

Failed

Introduced December 19, 2022, HB 1002, would amend the University of Illinois Hospital Act and the Hospital Licensing Act, to require that before using any diagnostic algorithm to diagnose a patient, a hospital must first confirm that the diagnostic algorithm has been certified by the Department of Public Health and the Department of Innovation and Technology, has been shown to achieve as or more accurate diagnostic results than other diagnostic means, and is not the only method of diagnosis available to a patient.

Failed

Introduced February 17, 2023, HB 3773, would amend the Human Rights Act, and provide that an employer that uses predictive data analytics in its employment decisions may not consider the applicant's race or ZIP code when used as a proxy for race to reject an applicant in the context of recruiting, hiring, promotion, renewal of employment, selection for training or apprenticeship, discharge, discipline, tenure or terms, privileges, or conditions of employment.>

Failed

Introduced February 17, 2023, HB 3943, would create the Social Media Content Moderation Act, and require that a social media company post terms of service for each social media platform owned or operated by the company in a manner reasonably designed to inform all users of the social media platform of the existence and contents of the terms of service and submit a terms of service report to the Attorney General on a semi-annual bases that includes a detailed description of content moderation systems, information on content that was flagged and how that content was flagged, including if the content was flagged and actioned by AI software.

Failed

Introduced on February 17, 2023, HB 3385, would create the Illinois Data Privacy and Protection Act, to regulate, among other data uses, the collection and processing of personal information and the use of "covered algorithms." The bill defines "covered algorithm," broadly as "a computational process that uses machine learning, natural language processing, artificial intelligence techniques, or other computational processing techniques of similar or greater complexity and that makes a decision or facilitates human decision-making with respect to covered data, including to determine the provision of products or services or to rank, order, promote, recommend, amplify, or similarly determine the delivery or display of information to an individual." "Covered algorithm" is defined but not used further in the bill.

Failed

Introduced February 17, 2023, HB 3880, would create the Children's Privacy Protection and Parental Empowerment Act, and require a business that provides an online service to children shall not profile a child by default unless the profiling is necessary to provide the online service and only with respect to the aspect of the online service with which the child is actively and knowingly engaged and the business can demonstrate a compelling reason that profiling is in the best interest of children. Profiling is defined as any form of automated processing of personal information that uses personal information to evaluate certain aspects relating to a natural person, including analysing or predicting aspects concerning a natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.

INDIANA

Enacted

Introduced on January 9, 2023, SB5, would create an omnibus consumer privacy law along the lines of the Virginia Consumer Data Privacy Act and the Colorado Privacy Act, to regulate, among other data uses, the collection and processing of personal information. In particular, the bill sets out rules for profiling and automated decision-making. Specifically, the bill enables individuals to opt-out of "profiling in furtherance of decisions that produce legal or similarly significant effects" concerning the consumer. Profiling is defined as "any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements[.]" Controllers must also perform a data protection impact assessment for high-risk profiling activities. Enchanted as Public Law 94 May 01, 2023.

Failed

Introduced on January 29, 2023, HB1554, is similar to SB5 with respect to its regulation of "profiling."

MAINE

Proposed

Introduced March 02, 2023, HP 569, An Act To Protect Workers From Employer Surveillance, would require an employer to provide upon an employee request whether employee data interacts with an automated decisions system. Amended by H-173 and H-575.

Proposed

Introduced May 18, 2023, LD 1973, would enact the Maine Consumer Privacy Act aimed at protecting consumer data. Section 9603 would require a consumer to opt-in to processing if the controller processes consumer data for the purpose of profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer unless the consumer opts-in to the processing. Section 9607 requires a controller to conduct a DPA if processing personal data for the purpose of profiling if the profiling presents a reasonably foreseeable risk to the consumer. Profiling is not defined.

Proposed

Introduced on May 23, 2023, the Data Privacy and Protection Act, HP 1270, is a comprehensive bill aimed at protecting consumer data. The Act includes retention limits, use restrictions, and reporting requirements. Section 9615 specifically governs the use of algorithms. The Act provides that covered entities using covered algorithms (broadly defined, including machine learning, AI, and natural language processing tools) to collect, process, or transfer data “in a manner that poses a consequential risk of harm” complete an impact assessment of the algorithm. The impact assessment must be submitted to the Attorney General’s office within 30 days of finishing it. The assessment must include a publicly available and easily accessible summary.

In addition to an impact assessment, the Act requires covered entities to create a design evaluation prior to deploying a covered algorithm. The design evaluation must include the design, structure, and inputs of the covered algorithm.

This bill includes a private right of action and allows for the recovery of punitive damages. It is currently pending in the Maine Senate. If enacted, the first assessment will be due two years from the day the bill is enacted.

MARYLAND

Enacted

Maryland law, HB 1202, prohibits an employer from using a facial recognition service for the purpose of creating a facial template during an applicant’s pre-employment interview, unless the applicant consents by signing a specified waiver. This workplace AI law went into force on October 1, 2020.

MASSACHUSETTS

Proposed

Introduced on January 18 and 19, 2023, the Massachusetts Data Privacy Protection Act (MDPPA) was filed in both the Senate SD 745, and in the House HD 2281. The bill is based on the federal American Data Privacy Protection Act with additional provisions relating to workplace surveillance. The MDPPA would require companies to conduct impact assessments if they use a “covered algorithm” in a way that poses a consequential risk of harm to individuals. “Covered algorithm,” is defined as “a computational process that uses machine learning, natural language processing, artificial intelligence techniques, or other computational processing techniques of similar or greater complexity and that makes a decision or facilitates human decision-making with respect to covered data, including determining the provision of products or services or to rank, order, promote, recommend, amplify, or similarly determine the delivery or display of information to an individual.”

Proposed

Introduced on January 20, 2023, in both the Senate SD 1971 (assigned SB227), and in the House HD 3263, the Massachusetts Information Privacy and Security Act (MIPSA) creates various rights for individuals regarding the processing of their personal information, including the right to a privacy notice at or before the point of collection of an individual's personal information, the right to opt out of the processing of an individual's personal information for the purposes of sale and targeted advertising, rights to access and transport, delete, and correct personal information, and the right to revoke consent. Additionally, large data holders are required to perform risk assessments where the processing is based in whole or in part on an algorithmic computational process. A “large data holder”, is a controller that, in a calendar year: (1) has annual global gross revenues in excess of $1,000,000,000; and (2) determines the purposes and means of processing of the personal information of not less than 200,000 individuals, excluding personal information processed solely for the purpose of completing a payment-only credit, check or cash transaction where no personal information is retained about the individual entering into the transaction.

Proposed

Introduced on January 11, 2024, HD. 4788, the Artificial Intelligence Disclosure Act would require that any generative artificial intelligence system used to create audio, video, text or print AI-generated content within Massachusetts include on or within such content a clean and conspicuous disclosure that meets the following criteria: (i) a clear and conspicuous notice, as appropriate for the medium of the content, that identifies the content as AI-generated content, which is to the extent technically feasible, permanent or uneasily removed by subsequent users; and (ii) metadata information that includes an identification of the content as being AI-generated content, the identity of the system, tool or platform used to create the content, and the date and time the content was created.

Proposed

Introduced on February 16, 2023, H. 83, would create an omnibus consumer privacy law called the Massachusetts Data Privacy Protection Act to regulate, among other data uses, the collection and processing of personal information. In particular, the bill sets out rules for the use of automated decision making technologies that would require that a covered entity using automated decision making technologies (Covered Algorithms) to conduct an impact assessment and evaluate any training data used to develop the Covered Algorithm to reduce the risk of any potential harms from the use of such technologies.

Failed

Introduced on February 16, 2023, HB1974, would regulate the use of artificial intelligence (AI) in providing mental health services. In particular, the bill provides that the use of AI by any licensed mental health professional in the provision of mental health services must satisfy the following conditions: (1) pre-approval from the relevant professional licensing board; (2) any AI system used must be designed to prioritize safety and must be continuously monitored by the mental health professional to ensure its safety and effectiveness; (3) patients must be informed of the use of AI in their treatment and be afforded the option to receive treatment from a licensed mental health professional; and (4) patients must provide their informed consent to receiving mental health services through the use of AI. AI is defined as "any technology that can simulate human intelligence, including but not limited to, natural language processing, training language models, reinforcement learning from human feedback and machine learning systems."

Failed

Introduced on February 16, 2023, H1873, An Act Preventing A Dystopian Work Environment, would require that employers provide employees and independent contractors (collectively, "workers) with a particularized notice prior to the use of an Automated Decision System (ADS) and the right to request information, including, among other things, whether their data is being used as an input for the ADS, and what ADS output is generated based on that data. "Automated Decision System (ADS)" or "algorithm," is defined as "a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes or assists an employment-related decision." The bill further requires that employers review and adjust as appropriate any employment-related decisions or ADS outputs that were partially or solely based on the inaccurate data, and inform the worker of the adjustment. Employers and vendors acting on behalf of an employer must maintain an updated list of all ADS currently in use, and must submit this list to the department of labor on or before January 31 of each year. The bill also prohibits the use of ADSs in certain circumstances and requires the performance of algorithmic impact assessments.

Failed

Introduced on February 16, 2023, SB31, An Act drafted with the help of ChatGPT to regulate generative artificial intelligence models like ChatGPT, would require any company operating a large-scale generative artificial intelligence model to adhere to certain operating standards such as reasonable security measures to protect the data of individuals used to train the model, informed consent from individuals before collecting, using, or disclosing their data, and performance of regular risk assessments. A “large-scale generative artificial intelligence model” is defined to mean “a machine learning model with a capacity of at least one billion parameters that generates text or other forms of output, such as ChatGPT.” The bill further requires any company operating a large-scale generative artificial intelligence model to register with the Attorney General and provide certain enumerated information regarding the model.

MINNESOTA

Failed

Introduced on March 1, 2023, HF2309, would create an omnibus consumer privacy law based on the Colorado Privacy Act and Connecticut Data Privacy Act, to regulate, among other data uses, the collection and processing of personal information. In particular, the bill sets out rules for profiling and automated decision-making. Specifically, the bill enables individuals to opt-out of “profiling in furtherance of decisions that produce legal or similarly significant effects” concerning the consumer. Profiling is defined as “any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.” Controllers must also perform a data privacy and protection assessment for high-risk profiling activities.

Failed

Introduced on March 15, 2023, SF2915, establishes consumer rights regarding personal data. Consumers would have the right to access their personal data gathered by controllers and correct inaccurate information. They would have the right to delete personal data, opt out of data used for targeted advertising or profiling. Profiling includes any form of automated processing of personal data to evaluate or predict personal aspects. If passed, this act will be effective beginning July 31, 2024.

MONTANA

Enacted

Introduced on February 16, 2023, SB384, An act establishing the Consumer Data Privacy Act, would create an omnibus consumer privacy law, to regulate, among other data uses, the collection and processing of personal information, and profiling and automated decision-making. Specifically, the bill creates certain transparency requirements around profiling and enable individuals to opt-out of “profiling in furtherance of automated decisions that produce legal or similarly significant effects” concerning the consumer. Profiling is defined as “any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.” Controllers must also perform a data protection assessment for high-risk profiling activities.

NEW HAMPSHIRE

Enacted

Introduced on January 19, 2023, SB 255, would create an omnibus consumer privacy law based on a composite of the Colorado Privacy Act, Connecticut Data Privacy Act, and Virginia Consumer Data Protection Act. In particular, the bill sets out rules for profiling and automated decision-making. Specifically, the bill enables individuals to opt-out of “in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.” Profiling is defined as “any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.” Controllers must also perform a data protection assessment for high-risk profiling activities. The bill was reintroduced and passed by the legislature on January 18, 2024.

NEW JERSEY

Enacted

Initially introduced on January 11, 2022, S332 (the “Act”), creates an omnibus consumer privacy law along the lines of the Washington Privacy Act. Among other things, the Act requires companies to conduct data protection assessments of “processing that presents a heightened risk of harm to a consumer” before conducting such processing. Such “heightened risk” results from activities such as profiling. “Profiling” means any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual’s economic situation, health, personal preferences, interests, reliability, behavior, location or movements. Consumers are also afforded the right to opt-out of profiling in furtherance of decisions that produce legal or similarly significant effects.

The bill was signed into law on January 16, 2024. The law will go into effect January 15, 2025.

Failed

Introduced on December 5, 2022, A4909, would regulate the “use of automated tools in hiring decisions to minimize discrimination in employment.” The bill imposes limitations on the sale of automated employment decision tools (AEDTs), including mandated bias audits, and requires that candidates be notified that an AEDT was used in connection with an application for employment within 30 days of the use of the tool.

Failed

Introduced on January 1, 2022, A537, would require an automobile insurer using an automated or predictive underwriting system to annually provide documentation and analysis to the Department of Banking and Insurance to demonstrate that there is no discriminatory outcome in the pricing on the basis of race, ethnicity, sexual orientation, or religion, that is determined by the use of the insurer's automated or predictive underwriting system. Under this bill, "automated or predictive underwriting system" is defined to mean a computer-generated process that is used to evaluate the risk of a policyholder and to determine an insurance rate. An automated or predictive underwriting system may include, but is not limited to, the use of robotic process automation, artificial intelligence, or other specialized technology in its underwriting process.

Failed

Introduced on February 10, 2022, S1402, provides that it is unlawful discrimination and a violation of the law against discrimination for an automated decision system (ADS) to discriminate against any person or group of persons who is a member of a protected class in: (1) the granting, withholding, extending, modifying, renewing, or purchasing, or in the fixing of the rates, terms, conditions or provisions of any loan, extension of credit or financial assistance; (2) refusing to insure or continuing to insure, limiting the amount, extent or kind of insurance coverage, or charging a different rate for the same insurance coverage provided to persons who are not members of the protected class; or (3) the provision of health care services. Under the bill, ADS means a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes a decision or facilitates human decision making.

An ADS is discriminatory if the system selects individuals who are members of a protected class for participation or eligibility for services at a rate that is disproportionate to the rate at which the system selects individuals who are not members of the protected class. If passed, the law would take effect on the first day of the third month next following enactment.

NEW MEXICO

Proposed

Introduced on January 17, 2024, SB 68, the Age-Appropriate Design Code Act applies to “a sole proprietorship, partnership, limited liability company, corporation, association, affiliate or other legal entity that is organized or operated for the profit or financial benefit of the entity's shareholders or other owners and that offers online products, services or features to individuals in New Mexico and processes children's personal data.”

The Act would prohibit a covered entity from “profiling” a child under 18 unless:

1. the covered entity can demonstrate that the covered entity has appropriate safeguards in place to ensure that profiling is consistent with the best interest of children reasonably likely to access the online product, service or feature; and

2. profiling is necessary to provide the online product, service or feature requested, and only with respect to the aspects of the online product, service or feature with which the child is actively and knowingly engaged; or

3. the covered entity can demonstrate a compelling reason that profiling is in the best interest of children. "Profiling" means automated processing of personal data that uses personal data to evaluate certain aspects relating to a natural person, including analyzing or predicting aspects concerning a natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements; "profiling" does not include the processing of data that does not result in an assessment or judgment about a natural person.

For the most part, SB 68 is the same as SB 319, which was introduced on February 2, 2023, and failed to pass.

NEW YORK

Enacted

In December 2021, New York City passed the first law (Local Law 144), in the United States requiring employers to conduct bias audits of AI-enabled tools used for employment decisions. The law imposes notice and reporting obligations.

Specifically, employers who utilize automated employment decision tools (AEDTs) must:

1. Subject AEDTs to a bias audit, conducted by an independent auditor, within one year of their use;

2. Ensure that the date of the most recent bias audit and a “summary of the results”, along with the distribution date of the AEDT, are publicly available on the career or jobs section of the employer’s or employee agency’s website;

3. Provide each resident of NYC who has applied for a position (internal or external) with a notice that discloses that their application will be subject to an automated tool, identifies the specific job qualifications and characteristics that the tool will use in making its assessment, and informs candidates of their right to request an alternative selection process or accommodation (the notice shall be issued on an individual basis at least 10 business days before the use of a tool); and

4. Allow candidates or employees to request alternative evaluation processes as an accommodation.

While enforcement of the law has been delayed multiple times pending finalization of the law's implementing rules, on April 6, 2023 the Department of Consumer and Worker Protection (DCWP) published the law's Final Rule. The law is now in effect, and enforcement began on July 5, 2023.

Proposed

Introduced on November 3, 2023, S7735 (assembly version A7906), provides that it shall be unlawful for a landlord to implement or use an automated decision tool, unless it: (1) no less than annually, conducts a disparate impact analysis to assess the actual impact of any automated decision tool and publicly files the assessment; and (2) notifies all applicants than an automated decision tool will be used and provides the applicant with certain disclosures related to the automated decision tool. If passed, the law will go into immediate effect.

Proposed

Introduced on July 7, 2023, S7592 (assembly version A7904), would amend election law to require that any political communication, that uses an image or video footage that was generated in whole or in part with the use of artificial intelligence, disclose that artificial intelligence was used in such communication.

Proposed

Introduced on October 13, 2023, A8126 (senate version S8209), would create the New York Artificial Intelligence Bill of Rights. Where a New York resident is affected by any system making decisions without human intervention, under the AI Bill of Rights they would be afforded the following rights and protections: (i) the right to safe and effective systems; (ii) protections against algorithmic discrimination; (iii) protections against abusive data practices; (iv) the right to have agency over one's data; (v) the right to know when an automated system is being used; (vi) the right to understand how and why an automated system contributed to outcomes that impact one; (vii) the right to opt out of an automated system; and (viii) the right to work with a human in the place of an automated system.

Proposed

Introduced on September 29, 2023, A8098, requires publishers of books created wholly or partially with the use of generative artificial intelligence to disclose such use of generative artificial intelligence before the completion of such sale; applies to all printed and digital books consisting of text, pictures, audio, puzzles, games or any combination thereof.

Proposed

Introduced on October 16, 2023, A8158 (senate version S7847), requires that every newspaper, magazine or other publication printed or electronically published in this state, which contains the use of generative artificial intelligence or other information communication technology, identify that certain parts of such newspaper, magazine, or publication were composed through the use of artificial intelligence or other information communication technology.

Proposed

Introduced on January 12, 2024, S8214, requires the registration with the Department of State of certain companies whose (i) primary business purpose is related to artificial intelligence as evidenced by their North American Industry Classification System (NAICS) Code of 541512, 334220, or 511210, and (ii) who reside in New York or sell their products or services in New York. The fee for registration is $200. Failure to register can result in a fine of up to ten thousand dollars. Companies that knowingly fail to register may be barred from operating or selling their AI products or services in the state for a period of up to ten years.

Proposed

Introduced on October 27, 2023, A8195, the Advanced Artificial Intelligence Licensing Act, requires the registration and licensing of high-risk advanced artificial intelligence systems, establishes the advanced artificial intelligence ethical code of conduct, and prohibits the development and operation of certain artificial intelligence systems.

Proposed

Introduced on January 12, 2024, S8206 (assembly version A8105), requires that every operator of a generative or surveillance advanced artificial intelligence system that is accessible to residents of the state require a user to create an account prior to utilizing such service. Prior to each user creating an account, such operator must present the user with a conspicuous digital or physical document that the user must affirm under penalty of perjury prior to the creation or continued use of such account. Such document shall state the following:

"I, ________ RESIDING AT ________, DO AFFIRM UNDER PENALTY OF PERJURY THAT I HAVE NOT USED, AM NOT USING, DO NOT INTEND TO USE, AND WILL NOT USE THE SERVICES PROVIDED BY THIS ADVANCED ARTIFICIAL INTELLIGENCE SYSTEM IN A MANNER THAT VIOLATED OR VIOLATES ANY OF THE FOLLOWING AFFIRMATIONS:

- 1. I WILL NOT USE THE PLATFORM TO CREATE OR DISSEMINATE CONTENT THAT CAN FORESEEABLY CAUSE INJURY TO ANOTHER IN VIOLATION OF APPLICABLE LAWS;
- 2. I WILL NOT USE THE PLATFORM TO AID, ENCOURAGE, OR IN ANY WAY PROMOTE ANY FORM OF ILLEGAL ACTIVITY IN VIOLATION OF APPLICABLE LAWS;
- 3. I WILL NOT USE THE PLATFORM TO DISSEMINATE CONTENT THAT IS DEFAMATORY, OFFENSIVE, HARASSING, VIOLENT, DISCRIMINATORY, OR OTHERWISE HARMFUL IN VIOLATION OF APPLICABLE LAWS;
- 4. I WILL NOT USE THE PLATFORM TO CREATE AND DISSEMINATE CONTENT RELATED TO AN INDIVIDUAL, GROUP OF INDIVIDUALS, ORGANIZATION, OR CURRENT, PAST, OR FUTURE EVENTS THAT ARE OF THE PUBLIC INTEREST WHICH I KNOW TO BE FALSE AND WHICH I INTEND TO USE FOR THE PURPOSE OF MISLEADING THE PUBLIC OR CAUSING PANIC."

Proposed

Introduced on August 4, 2023, SO7623, would impose statewide requirements regulating tools that incorporate artificial intelligence to assist in employee monitoring and the employment decision-making process. In particular, the bill (1) defines a narrow set of allowable purposes for the use of electronic monitoring tools (EMTs), (2) requires that the EMT be “strictly necessary” and the “least invasive means” of accomplishing those goals, and (3) requires that the EMT collect as little data as possible on as few employees as possible to accomplish the goal. The bill also requires that employers exercise “meaningful human oversight” of the decisions of automated tools, and conduct and publically post the results of an independent bias audit, and provide notification requirements to candidates that a tool is in use.

Proposed

Introduced on March 10, 2023, SB 5641, would amend labor law to establish criteria for the use of automated employment decision tools (AEDTs). The proposed bills mirrors NYC’s Local Law 144 in many ways. In particular, employers who utilize AEDTs must: (1) obtain from the seller of the AEDT a disparate impact analysis, not less than annually; (2) ensure that the date of the most recent disparate impact analysis and a summary of the results, along with the distribution date of the AEDT, are publicly available on the employer’s or employee agency’s website prior to the implementation or use of such tool; and (3) annually provide the labor department a summary of the most recent disparate impact analysis.

Failed

Introduced on January 4, 2023, SB 365, the New York Privacy Act, would be the state’s first comprehensive privacy law. The law would require companies to disclose their use of automated decision-making that could have a “materially detrimental effect” on consumers, such as a denial of financial services, housing, public accommodation, health care services, insurance, or access to basic necessities; or could produce legal or similarly significant effects. Companies must provide a mechanism for a consumer to formally contest a negative automated decision and obtain a human review of the decision, and must conduct an annual impact assessment of their automated decision-making practices to avoid bias, discrimination, unfairness or inaccuracies.

The law would also permit consumers to opt-out of "profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer." Profiling is defined as any type of automated processing performed on personal data to evaluate, analyze, or predict personal aspects" such as "economic situation, health, personal preferences, interests, reliability, behavior, location, or movements." Finally, the law would mandate that companies conduct a data protection assessment on their profiling activities, since profiling would be considered a processing activity with a heightened risk of harm to the consumer.

Failed

Introduced on January 4, 2023, A216, would require advertisements to disclose the use of synthetic media. Synthetic media is defined as "a computer-generated voice, photograph, image, or likeness created or modified through the use of artificial intelligence and intended to produce or reproduce a human voice, photograph, image, or likeness, or a video created or modified through an artificial intelligence algorithm that is created to produce or reproduce a human likeness." Violators would be subject to a $1,000 civil penalty for a first violation and a $5,000 penalty for any subsequent violation.

Failed

Introduced on March 7, 2023, A5309, would amend state finance law to require that where state units purchase a product or service that is or contains an algorithmic decision system, that such product or service adheres to responsible artificial intelligence standards. The bill requires the commissioner of taxation and finance to adopt regulations in support of the law.

Failed

Introduced on May 3, 2023 and May 10, 2023, S6638 and A7106, the Political Artificial Intelligence Disclaimer (PAID) Act, would amend election and legislative law in relation to the use and disclosure of synthetic media. The act would add a subdivision to the election law that requires any political communication which was produced by synthetic media to be disclosed via printed or digital communications. The disclosure must read "This political communication was created with the assistance of artificial intelligence." If passed, the act would take effect on January 1, 2024.

Failed

S7422, introduced on May 24, 2023 and A7634, introduced on May 25, 2023, would prohibit film production companies who apply for Empire State film production credit from using synthetic media in any component of production that would displace a natural person from that role. This includes any form of media, such as text, image, video, or sound that is created or modified by use of artificial intelligence. Compliance with this act would be a condition for granting of the credit. If passed, the act would take effect immediately.

OHIO

Proposed

Introduced on January 24, 2024, SB 217 would require AI-generated products have a watermark, prohibit removing such a watermark, prohibit simulated child pornography, and prohibit identity fraud using a replica of a person. Provides for injunctive relief and, for unauthorized removal of an AI watermark, a civil penalty of up to $10,000.

OKLAHOMA

Proposed

Introduced on February 5, 2024, HB 3453, the Oklahoma Artificial Intelligence Bill of Rights would give Oklahoma residents the following rights:

1. The right to know when they are interacting with an artificial intelligence engine rather than a real person;

2. The right to know when their data is being used in an artificial intelligence model and the right to opt-out;

3. The right to know when contracts and other documents that they are relying on were generated by an artificial intelligence engine rather than a real person;

4. The right to know when they are consuming images or text that were generated entirely by an artificial intelligence engine and not reviewed by a human;

5. The right to be able to rely on a watermark or some other form of content credentials to verify the authenticity of creative product they generate or consume. Specifically, it shall not be permissible for any websites, social media platforms, search engines, and the like, to remove a watermark or content credential without inserting an updated credential that indicates that the original was removed or altered.

6. The right to know that any company which includes any of their data in an artificial intelligence model has implemented industry best practice security measures for data privacy, and conducts at least annual risk assessments to assess design, operational and discrimination harm.
7. The right to approve any derivative media that is generated by an artificial intelligence engine and uses audio recordings of their voice or images of them to recreate their likeness.
8. The right to not be subject to algorithmic or model bias which discriminates based on age, race, national origin, sex, disability, pregnancy, religious beliefs, veteran status, or any other legally protected classification.

If passed, the act would take effect November 1, 2024.

Proposed

Introduced on February 5, 2024, HB 3577, the Artificial Intelligence Utilization Review Act would:

- Require health insurers to disclose the use of AI algorithms;
- Require health insurers to submit AI systems to Oklahoma Department of Insurance for review;

A violation shall be deemed to be an unfair method of competition and an unfair or deceptive act or practice. Civil penalties between $5,000 and $10,000.

If passed, the act would take effect November 1, 2024.

Proposed

Introduced on February 5, 2024, HB 3835, the Ethical Artificial Intelligence Act would:

- direct deployers of automated decision tools to complete and document certain impact assessments
- direct developers of automated decision tools to complete and document certain impact assessment;
- direct deployers and developers to make impact assessment of certain updates;
- mandate that developers and deployers provide certain impact assessment to the office of the attorney general;
- require developer provide certain documentation to deployer;
- require developer make certain information publicly available;
- prohibit deployers from algorithmic discrimination.

The act would be enforced by the attorney general. A violation of the act would be an unfair or deceptive act in trade or commerce for the purpose of applying the Oklahoma Consumer Protection Act. Harmed parties may bring a civil action.

If passed, the act would take effect November 1, 2024.

OREGON

Enacted

On August 1, 2023, Oregon passed SB619, the state's first omnibus consumer privacy law. The bill generally follows the Virginia Consumer Data Protection Act and sets out rules for profiling and automated decision-making. Specifically, the bill enables individuals to opt-out of processing for the purpose of "profiling the consumer to support decisions that produce legal effects or effects of similar significant significance." Profiling is defined as "an automated processing of personal data for the purpose of evaluating, analyzing or predicting an identified or identifiable consumer's economic circumstances, health, personal preferences, interests, reliability, behavior, location or movements." Controllers must also perform a data protection assessment for high-risk profiling activities. The law goes into effect on July 1, 2024.

PENNSYLVANIA

Proposed

Introduced on March 7, 2023, HB49, would direct the Department of State to establish a registry of businesses operating artificial intelligence systems in the State. The registry would include (1) The name of the business operating artificial intelligence systems; (2) The IP address of the business; (3) The type of code the business is utilizing for artificial intelligence; (4) The intent of the software being utilized; (5) The personal information and first and last name of a contact person at the business; (6) The address, electronic email address and ten-digit telephone number of the contact person; and (7) A signed statement indicating that the business operating an artificial intelligence system has agreed for the Department of State to store the business's information on the registry.

Proposed

Introduced on March 27, 2023, HB708, would establish an omnibus consumer privacy law along the lines of those enacted in states like Virginia. Among its requirements, the bill provides consumers with the right to opt-out of the processing of their personal data for purposes of "profiling in furtherance of in furtherance of decisions that produce legal or similarly significant effects concerning the consumer." Profiling is defined as a "form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location or movements.” The bill also mandates the performance of data protection assessments in connection with “profiling” where the profiling presents “a reasonably foreseeable risk of: (i) discriminatory, unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (ii) financial, physical or reputational injury to consumers; (iii) a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where the intrusion would be offensive to a reasonable person; or (iv) other substantial injury to consumers.”

If passed, the act would go into effect in 18 months.

Proposed

Introduced on December 13, 2023, HB1201 appears similar to HB 708 (above) in that it would establish an omnibus consumer privacy law. It provides consumers with the right to “Opt out of the processing of the consumer's personal data for the purpose of any of the following: (i) Targeted advertising; (ii) The sale of personal data, except as provided under section 5(b); and (iii) Profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.” “Profiling” is defined as “Any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements.” The bill would mandate data protection impact assessments where “the profiling presents a reasonably foreseeable risk of any of the following: (i) Unfair or deceptive treatment of, or an unlawful disparate impact on, a consumer. (ii) Financial, physical or reputational injury to a consumer. (iii) A physical or other intrusion upon the solitude or seclusion of a consumer or the private affairs or concerns of a consumer where the intrusion would be offensive to a reasonable person. (iv) Any other substantial injury to a consumer.”

If passed, the act will take effect in 6 months.

Proposed

Introduced on September 7, 2023, HB1663 would require disclosure by health insurers of the use of artificial intelligence-based algorithms in the utilization review process. Requirements would include:

- Disclose to clinicians, subscribers, and the public that claims evaluations use AI algorithms
- Define ‘Algorithms used in claims review’ as clinical review criteria and therefore ensure they are subject to existing laws and regulations that such criteria be grounded in clinical evidence
- Require specialized health care professionals who review claims for health insurance companies and rely on initial AI algorithms for such reviews to individually open each clinical record or clinical data, examine this information, and document both their own review and

reason for denial before any decision to deny a claim is conveyed to a subscriber or health care provider.

- Require health insurance companies to submit their AI-based algorithms and training datasets to the Pennsylvania Department of Insurance for transparency and require the Department of Insurance to certify that said algorithms and training data sets have minimized the risk of bias based on categories outlined in the Human Relations Act and other anti-discrimination statutes as applicable to health insurance in Pennsylvania and adhere to evidence-based clinical guidelines.

If passed, the act will take effect in 60 days.

Proposed

Introduced on August 7, 2023, HB1598 would amend the Unfair Trade Practices and Consumer Protection Law to expand the definition of an unfair trade practice to include “creating, distributing or publishing any content generated by artificial intelligence without clear and conspicuous disclosure, including written text, images, audio and video content and other forms of media. A disclosure under this subclause must state that the content was generated using artificial intelligence and must be presented in a manner reasonably understandable and readily noticeable to the consumer.

If passed, the act will take effect in 60 days.

RHODE ISLAND

Failed

Introduced on February 1, 2023, SB146, would prohibit certain uses of automated decision systems and algorithmic operations in connection with video-lottery terminals and sports betting applications. The law would take effect upon passage. The law was not accepted prior to the end of the legislative session in June 2023.

Failed

Introduced on March 30, 2023, HB6236, the Rhode Island Data Transparency And Privacy Protection Act, would establish an omnibus consumer privacy law along the lines of those enacted in states like Virginia. Among its requirements, the bill provides consumers with the right to opt-out of the processing of their personal data for purposes of “profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the customer.” Profiling is defined as “any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements.” The bill also mandates the performance of data protection assessments in connection with “profiling” where the profiling presents “a reasonably foreseeable risk of unfair or deceptive treatment of, or unlawful disparate impact on, customers, financial, physical or reputational injury to customers, a physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of customers, where such intrusion would be offensive to a reasonable person, or other substantial injury to customers[.]” The law was not accepted prior to the end of the legislative session in June 2023.

Failed

Introduced on April 19, 2023, H6286, would regulate companies’ uses of generative artificial intelligence models. Any company using large-scale generative AI may not use AI for discriminatory practices. The AI model must be programmed to generate text with a distinctive watermark to prevent plagiarism. The company must implement reasonable security measures to protect the data of individuals used to train the model, and the company must obtain informed consent from these individuals before using their data. The company must also conduct regular risk assessments of potential risks and harms related to their services. Within 90 days of the effective date of this act, any company using large-scale generative AI must register the name of the company, description of the AI model, and information on the company’s data gathering practices with the attorney general.

SOUTH CAROLINA

Proposed

Introduced on January 9, 2024, H4696

"Profiling" means “any form of solely automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.” If passed, the act would take effect immediately.

Proposed

Introduced on January 9, 2024, H4660 would require that “a person, corporation, committee, or other entity shall not, within ninety days of an election at which a candidate for elective office will appear on the ballot, distribute a synthetic media message that the person, corporation, committee, or other entity knows or should have known is a deceptive and fraudulent deepfake of a candidate on the ballot.” If passed, the act would take effect immediately.

Proposed

Introduced on January 16, 2024, H4842, the South Carolina Age-Appropriate Design Code Act would apply to any business operating in South Carolina that either: “(i) has annual gross revenues more than twenty-five million dollars, as adjusted every odd-numbered year to reflect the Consumer Price

Index; (ii) alone or in combination, annually buys, receives for the covered entity's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal data of fifty thousand or more consumers, households, or devices; or (iii) derives fifty percent or more of its annual revenues from selling consumers' personal data.”

Covered entities would be prohibited from “profiling” children under age 18 by default unless both of the following criteria are met: “ (a) the covered entity can demonstrate it has appropriate safeguards in place to ensure that profiling is consistent with the best interests of children reasonably likely to access the online service, product, or feature; and (b) either of the following is true: (i) profiling is necessary to provide the online service, product, or feature requested and only with respect to the aspects of the online service, product, or feature with which a child is actively and knowingly engaged; or (ii) the covered entity can demonstrate a compelling reason that profiling is in the best interests of children.”

“Profiling” means “any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable natural person’s economic situation, health, personal preferences, interests, reliability, behavior, location, or movements. ‘Profiling’ does not include the processing of information that does not result in an assessment or judgment about a natural person.”

Failed

Introduced on January 18, 2023, SB404, would prohibit any operator of a website, an online service, or an online or mobile application, including any social media platform, to utilize an automated decision system (ADS) for content placement, including feeds, posts, advertisements, or product offerings, for a user under the age of eighteen. In addition, an operator that utilizes an ADS for content placement for residents of South Carolina who are eighteen years or older shall perform an age verification through an independent, third-party age-verification service, unless the operator employs the bill’s prescribed protections to ensure age verification. The bill includes a private right of action.

TENNESSEE

Enacted

Effective July 1, 2024, HB1181, the Tennessee Information Protection Act, establishes an omnibus consumer privacy law along the lines of those enacted in states like Virginia. Among its requirements, the bill mandates the performance of data protection assessments in connection with “profiling” where the profiling presents a reasonably foreseeable risk of: (A) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers; (B) Financial, physical, or reputational injury to consumers; (C) A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, where the intrusion would be offensive to a reasonable person; or

(D) Other substantial injury to consumers. "Profiling" is defined as “a form of automated processing performed on personal information to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements[.]” The law gives the Tennessee Attorney General’s Office authority to impose civil penalties on companies who violate the law.

TEXAS

Enacted

Introduced on February 16, 2023, HB4, the Texas Data Privacy and Security Act, is based on the Virginia Consumer Data Protection Act. Once effective, the law will create similar requirements enabling individuals to opt-out of “profiling” that produces a legal or similarly significant effect concerning the individual. Controllers must also perform a data protection assessment for high-risk profiling activities.

Failed

Introduced on March 10, 2023, HB4695, would prohibit the use of artificial intelligence technology to provide counseling, therapy, or other mental health services unless (1) the artificial intelligence technology application through which the services are provided is an application approved by the commission; and (2) the person providing the services is a licensed mental health professional or a person that makes a licensed mental health professional available at all times to each person who receives services through the artificial intelligence technology. The artificial intelligence technology must undergo testing and approval by the, Texas Health and Human Services Commission, the results of which will be made publicly available. If passed, the law would take effect September 1, 2023.

UTAH

Proposed

Introduced on January 24, 2024, SB 149 would require covered businesses to “clearly and conspicuously disclose to a consumer that they are interacting with “generative artificial intelligence and not a human.” As relevant here, “generative artificial intelligence” refers to “an artificial system that: i) is trained on data; ii) interacts with a person using text, audio, or visual communication; and iii) generates non-scripted outputs similar to outputs created by a human, with limited or no human oversight.” Failure to comply with the bill would result in a civil penalty of no more than $5,000 per violation.

VERMONT

Proposed

Introduced on January 9, 2024, H710 would put in place certain obligations for both developers and deployers of "high-risk artificial intelligence system." For developers, these obligations would include, among others, using reasonable care to avoid any risk of algorithmic discrimination that is a reasonably foreseeable consequence of developing or modifying a high-risk system to make consequential decisions. Developers would also be required to provide disclosures relating to the system, such as disclosures about the known limitations of the system and foreseeable risks of algorithmic discrimination, a summary of the type of data to be processed, the purpose of processing, mitigation measures put in place to limit identified risks, and other similar information necessary to conduct a risk assessment. Similar obligations would apply to developers of generative artificial intelligence.

Deployers would be required to use reasonably care to avoid any risk of algorithmic discrimination that is a reasonably foreseeable consequence of deploying or using a high-risk artificial intelligence system. High-risk systems may only be used to the extent that the deployer has already implemented a risk management policy that is at least as stringent as the Artificial Intelligence Risk Management Framework published through NIST and the deployer has conducted a risk assessment for the system.

Search engines and social media platforms knowingly using, or which reasonably believes that it is using, synthetic digital content would also be required to provide consumers with a signal indicating that the content was produced, or is reasonably believed to have been produced, by generative artificial intelligence.

Failure to comply with the Act would be treated as an unfair and deceptive act in trade and commerce in violation of 9 VSA 2453. The Attorney General may provide a cure period at its discretion. The Act would take effect on July 1, 2024.

Proposed

Introduced on January 9, 2024, H711 would create an oversight and enforcement agency to collect and review risk assessments taken in connection with the use of high-risk artificial intelligence systems. The Act would require each deployer of "inherently dangerous artificial intelligence systems" to submit a risk assessment prior to deploying such a system and every two years thereafter, as well as submit a new risk assessment in case material and substantial changes are made to the system. Deployers would also be required to submit a 1-, 6-, and 12-month testing results to the Division of Artificial Intelligence showing the reliability of the results generated by the systems, as well as variances and mitigation measures put in place to limit risks posed by the use of such systems.

The Act would also create a duty for deployers and developers to meet a certain standard of care for the use of any inherently dangerous artificial intelligence systems that “could be reasonably expected to impact consumers.” The Act would also prohibit the deployment of inherently dangerous artificial intelligence systems that pose disproportionate risks unless those risks are evaluated and validated against the Artificial Intelligence Risk Management Framework published by NIST.

Violations of the Act would be treated as an unfair practice in commerce. The Act would also create a private right of action for consumers harmed by a violation of the chapter. The Act would take effect July 1, 2024.

Proposed

Introduced on January 25, 2023, H114, would restrict the use of electronic monitoring of employees and the use of automated decision systems (ADSs) for employment-related decisions. Electronic monitoring of employees may only be conducted when, for example, the monitoring is used to ensure compliance with applicable employment or labor laws or to protect employee safety, and certain notice is given to employees 15 days prior to commencement of the monitoring. ADSs must also meet a number of requirements, including corroboration of system outputs by human oversight of the employee and creation of a written impact assessment prior to using the ADS. The law was not accepted prior to the end of the legislative session in May 2023.

VIRGINIA

Enacted

The Virginia Consumer Data Protection Act (VCDPA), which went into force on January 1, 2023, sets out rules for profiling and automated decision-making. Specifically, the VCDPA enables individuals to opt-out of “profiling in furtherance of decisions that produce legal or similarly significant effects” concerning the consumer, which is generally defined as “the denial and/or provision of financial and lending services, housing, insurance, education enrollment or opportunities, criminal justice, employment opportunities, healthcare services, or access to basic necessities.” Controllers must also perform a data protection impact assessment for high-risk profiling activities.

Proposed

Introduced on January 10, 2024, HB 747 , the Artificial Intelligence Developer Act, would prohibit developers of “high-risk artificial intelligence systems” from offering, selling, leasing, giving, or otherwise providing to a third party to deploy any artificial intelligence unless they provide the developers with sufficient information to perform a risk assessment on the use of the system, such as through a document detailing the potential risks and benefits of using the system, as well as a description of the intended uses of that system. Similar obligations would apply to developers of generative artificial intelligence.

The Act would also require deployers of artificial intelligence to take reasonable care to avoid any risk of reasonably foreseeable "algorithmic discrimination" and may only use the high-risk artificial intelligence system to make "consequential decisions" if the deployer has designed and implemented a risk management policy for the use of that program. The Act also specifies the elements that must be included in a risk assessment, which includes, among other considerations, the purpose of processing, a description of transparency measures taken concerning the system, a description of the data used to train the algorithm, and other information.

Failure to comply with the Act would result in civil penalties not to exceed $1,000 plus reasonable attorney fees, expenses, court costs, and willful violations may result in civil penalties between $1,000 and $10,000. The law would take effect July 1, 2026.

WASHINGTON

Proposed

Introduced on January 31, 2023, SB5643 and its companion HB1616, the People's Privacy Act, would prohibit a covered entity or Washington governmental entity from operating, installing, or commissioning the operation or installation of equipment incorporating "artificial intelligence-enabled profiling" in any place of public resort, accommodation, assemblage, or amusement, or to use artificial intelligence-enabled profiling to make decisions that produce legal effects (e.g., denial or degradation of consequential services or support, such as financial or lending services, housing, insurance, educational enrollment, criminal justice, employment opportunities, health care services, and access to basic necessities, such as food and water) or similarly significant effects concerning individuals. "Artificial intelligence-enabled profiling" is defined as the "automated or semiautomated process by which the external or internal characteristics of an individual are analyzed to determine, infer, or characterize an individual's state of mind, character, propensities, protected class status, political affiliation, religious beliefs or religious affiliation, immigration status, or employability." The bill also ban the use of "face recognition" in any place of public resort, accommodation, assemblage, or amusement. "Face recognition" is defined as "i) An automated or semiautomated process by which an individual is identified or attempted to be identified based on the characteristics of the individual's face; or (ii) an automated or semiautomated process by which the characteristics of an individual's face are analyzed to determine the individual's sentiment, state of mind, or other propensities including, but not limited to, the person's level of dangerousness[.]"

Proposed

Introduced on January 24, 2024, SB6299, would make it unlawful for any employer to utilize artificial intelligence or generative artificial intelligence to evaluate or otherwise make employment decisions regarding current employees without written disclosure of the employer's use of such technology at the time of the employee's initial hire, or within 30 calendar days of the employer starting to use such technology for such purpose.

Proposed

Introduced on December 14, 2023, HB1951, provides that by January 1, 2025, and annually thereafter, a developers and deployers of automated decision tools must complete and document an impact assessment for any automated decision tool the deployer uses, or the developer develops, as specified. "Automated decision tool" means a system or service that uses artificial intelligence and has been specifically developed and marketed to, or specifically modified to, make, or be a controlling factor in making, consequential decisions. Upon the request of the office of the attorney general, a developer or deployer must provide any impact assessment that it performed pursuant to this section to the office of the attorney general. The bill requires certain other public disclosures. The bill also prohibits the use of an automated decision tool that results in algorithmic discrimination.

WEST VIRGINIA

Failed

Introduced on February 14, 2023, HB3498, the *Consumer Data Protection Act*, would create an omnibus consumer privacy law. The bill generally follows the Virginia Consumer Data Protection Act and sets out rules for profiling and automated decision-making. Specifically, the bill enables individuals to opt-out of the processing of their personal data for the purpose of “profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer.” Profiling is defined as “any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.” Controllers must also perform a data protection assessment for high-risk profiling activities.

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Goli Mahdavi

San Francisco

goli.mahdavi@bclplaw.com
+1 415 675 3448

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.