BRYAN CAVE LEIGHTON PAISNER BCLP

2023 STATE-BY-STATE ARTIFICIAL INTELLIGENCE LEGISLATION SNAPSHOT

Artificial Intelligence (AI), once limited to the pages of science fiction novels, has now been adopted by more than 1/4 of businesses in the United States, and nearly half of all organizations are working to embed AI into current applications and processes.[1] As companies increasingly integrate artificial intelligence 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.

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 as AI has caught the attention of federal and state regulators and oversight of AI is ramping up.

At the federal level the proposed privacy bill - the American Data Protection and Privacy Act (ADPPA) - sets out rules for AI, including risk assessment obligations that would directly impact companies developing and utilizing AI technologies. However, the ADPPA stalled during the past Congressional session, and it remains to be seen whether its framework will advance in the new Congress. In the absence of comprehensive federal legislation on AI there is now a patchwork of various current and proposed AI regulatory frameworks at the state and local level. What is clear is that momentum for AI regulation is at an all-time high, which makes the development and implementation of AI solutions challenging in the face of an uncertain regulatory environment.

BCLP actively tracks the proposed 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 March 22, 2023, and will be updated quarterly to include legislation that if passed would directly impact a businesses' development or deployment of AI solutions.[2]

---

[1] IBM Global AI Adoption Index 2022.

[2] We have 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 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.

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.

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. At the time of publication, the regulations were still in the proposal stage.

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.

DISTRICT OF COLUMBIA

Proposed

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.

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[.]"

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.

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.

Proposed

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.

INDIANA

Proposed

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.

Proposed

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

MARYLAND

Existing

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 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."

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), and 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 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.

Proposed

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

Proposed

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.

MONTANA

Proposed

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

Proposed

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.

NEW JERSEY

Proposed

Introduced on December 5, 2022, Bill 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.

Proposed

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.

Proposed

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 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 went into effect on January 1, 2023, and 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.

At the time of publication, rulemaking by the NYC Department of Consumer and Worker Protection is still underway. We are continuing to monitor the law and proposed rules for further updates.

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.

Proposed

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.

Proposed

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.

Proposed

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.

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.

OREGON

Proposed

Introduced on January 9, 2023, SB619, *relating to protections for the personal data of consumers*, 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 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.

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' 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."

RHODE ISLAND

Proposed

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.

Proposed

Introduced on March 30, 2023, HB62236, 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[.]"

SOUTH CAROLINA

Proposed

Introduced on January 28, 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

Proposed

Introduced on January 4, 2023, SB73, and companion bill HB1181, introduced on January 31, 2023, the *Tennessee Information Protection Act,* would establish 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 bill gives the Tennessee Attorney General’s Office authority to impose civil penalties on companies who violate the law.

TEXAS

Proposed

Introduced on February 3, 2023, HB1844, the *Texas Data Privacy and Security Act*, is based on the Virginia Consumer Data Protection Act. If passed, the bill would 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.

Proposed

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.

VERMONT

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.

VIRGINIA

Proposed

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.

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[.]"

RELATED LINKS

- Data Privacy & Security

MEET THE TEAM

Goli Mahdavi

Counsel, San Francisco

goli.mahdavi@bclplaw.com

+1 415 675 3448

Amy de La Lama

Chair - Global Data Privacy and Security, Boulder

amy.delalama@bclplaw.com

+1 303 417 8535