Automated Decisionmaking and Profiling (ADM) Requirements in U.S. State Privacy Laws, and Current State of Play in State AI Regulations

May 2024

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

May 14, 2024

CIPL US State Privacy Laws Mapping Project

Discussion Paper

Automated Decisionmaking and Profiling (ADM) Requirements in U.S. State Privacy Laws, and Current State of Play in State AI Regulations

As the number of privacy laws in the US enacted by state legislatures grows rapidly,[1] organizations with limited budgets and resources are seeking ways to synthesize requirements and harmonize compliance measures across jurisdictions. CIPL[2] has initiated a project to identify areas of alignment and divergence between state laws, and to examine the compliance challenges organizations face due to the divergences. Our goal is to help state law and policymakers in the US advance the principles of privacy and data protection in a more consistent and manageable way.

The present paper examines the requirements regarding automated decisionmaking and profiling included in comprehensive state privacy laws as well as notable, state-level artificial intelligence (**"AI"**) regulations. Comprehensive state consumer privacy laws play a crucial role in shaping the use of AI technologies by imposing specific regulations on automated processing and decisionmaking. Most such laws that have been adopted to date provide consumers the right to opt-out of any processing of personal information for the purpose of "profiling" that produces legal or similarly significant effects (see discussion of the definition of profiling below). We also compare these requirements to similar requirements found in the EU General Data Protection Regulation (**"GDPR"**) to benchmark US state law requirements against the currently dominant global standard on this issue.

When examining the rules concerning automated decisionmaking and profiling in state comprehensive privacy laws, it is important to recognize that some state laws incorporate exemptions that exclude specific types of data or entities from their scope. For example, California and the GDPR cover employment-related information and business-to-business ("B2B") data, making the scope of their automated decisionmaking and profiling rules broader compared to other state privacy laws, such as Colorado and Virginia, which exclude employee and B2B data. Furthermore, state comprehensive privacy laws also differ regarding exemptions at the entity-level. For example, while these laws typically apply

[1] As of May 14, 2024, the following states adopted their own comprehensive privacy laws: California ("CPRA" or "the CCPA as amended"), Colorado ("CPA"), Connecticut ("CTDPA"), Delaware ("DOPPA"), Florida ("FDBR"), Indiana ("ICDPA"), Iowa ("ICDPA"), Kentucky ("KCDPA"), Maryland ("MODPA"), Montana ("MCDPA"), Nebraska ("NEDPA"), New Hampshire ("NHCPA"), New Jersey ("NJCPA"), Oregon ("OCPA"), Tennessee ("TIPA"), and Texas ("TDPSA"), Utah ("UCPA"), Virginia ("VCDPA"). We include Florida in our list of comprehensive laws, although some sources do not count it due to its applicability to a limited set of entities. While the Vermont legislature passed its comprehensive privacy law on May 10, 2014, the final text of the bill is not yet available as of May 14, 2024. Therefore, this paper does not include the Vermont privacy law.

[2] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure effective privacy protections and the responsible use of personal information in the modern information age. Please see CIPL's website at www.informationpolicycentre.com. Nothing in this paper should be construed as representing the views of any individual CIPL member company or Hunton Andrews Kurth, nor does anything in this paper constitute legal advice.

only to for-profit entities that meet certain thresholds, Colorado and Oregon extend their applicability to nonprofit organizations. Moreover, certain state privacy laws, such as those in California and Oregon, provide carve-outs for personal data subject to specific laws, such as the Graham-Leach-Bliley Act (GLBA) instead of institutional or entity-level exemptions.

Several US states have enacted (or plan to enact) laws regulating the use of AI technologies, particularly focusing on the public sector, including law enforcement and state agencies.[3] However, **this paper primarily focuses on AI regulations for the private sector**. Nonetheless, we acknowledge that the enforcement and implementation of regulations in the public sector may ultimately influence the use of AI by the private sector, particularly in the context of public procurement.[4]

This report analyzes ADM requirements in state comprehensive privacy laws across five topics:

- scope of opt-out rights for the purposes of automated decisionmaking and profiling;
- notice requirements;
- access rights; and,
- data protection assessments.

Within each topic, features of state laws are grouped into "Most Common Approach" and "Other Approach" categories.

A separate section addresses state laws specific to AI.

[3] For instance, SB 1103 in Connecticut (An Act Concerning Artificial Intelligence, Automated Decisionmaking and Personal Data Privacy) prohibits the executive and judicial branches from implementing any system that uses AI unless they have done an impact assessment to make sure the system will not result in any unlawful discrimination or disparate impact against specified people or groups of people based on actual or perceived characteristics. Another example comes from Maine, which enacted a law (Bill No.1585) prohibiting the use of facial recognition across all levels of state, county, and municipal government except for very limited law enforcement-related exceptions. In Alabama (Code 15-10-11), law enforcement are also prohibit from using facial recognition matches as the sole basis to establish probable cause in a criminal investigation or to make an arrest.

[4] *See*, for instance, SB 1103 in Connecticut, which requires the executive and judicial branches to annually do an inventory of all their systems that employ artificial intelligence, and make policies and procedures on developing, procuring, using, and assessing systems that use AI.

1. Scope of Opt-out Rights in the Context of Automated Decisionmaking and Profiling

Most Common Approach: Profiling Producing a Legal or Similarly Significant Effect – State comprehensive privacy laws often grant consumers the right to opt-out of processing personal information for the purposes of profiling in furtherance of automated decisions that produce legal or similarly significant effects concerning the consumer.[5] The majority of these states[6] define profiling as "*any form of automated processing of personal data to evaluate, analyze, or predict personal aspects concerning an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements*." Delaware goes further by also including "demographic characteristics" in its profiling definition (but it does not further define the term). Importantly, at the time of drafting this paper, no US state privacy law requires covered entities to provide opt-out preferences transmitted through a universal opt-out mechanism (**"UOOM"**) for the purpose of profiling activities.[7]

The "legal or similarly significant effects" standard benefits businesses' compliance efforts because it is interoperable with identical or similar standards in other domestic and global frameworks, such as the EU

[5] Section 7221(a) in conjunction with Section 7200(a)(2) of California Risk Assessment and Automated Decisionmaking Regulations (March 2024), Section 6-1-1306 1(a)(I)(c) Colorado Privacy Act and Rule 9.02 of Colorado Privacy Act Rules, Section 4(a)(5)(c) Connecticut Data Privacy Act, Section 12D-104(a)(6)(c) Delaware Personal Data Privacy Act, Section 501.705(2)(e)(3) Florida Digital Bill of Rights, Chapter 3 Section 1(b)(5)(c) Indiana Consumer Privacy Act, Section 3(2)(e) Kentucky Consumer Data Protection Act, Section 14-4605(b)(7)(III) Maryland Online Data Privacy Act, Section 5(1)(e)(3) Montana Consumer Data Privacy Act, Section 7(2)(e)(iii) Nebraska Data Privacy Act, Section 507-H:4(1)(e) New Hampshire Data Privacy Act, Section 7(a)(5)(c) New Jersey Data Privacy Act, Section 3(1)(d)(c) Oregon Consumer Privacy Act, Section 47-18-3203(A)(2)(e)(iii) Tennessee Information Protection Act, Section 541.051(b)(5)(c) Texas Data Privacy and Security Act, Section 59.1-573(a)(5)(iii) Virginia Consumer Data Protection Act. Please note that the Connecticut Privacy Act Amendments (Bill No.3 – aka "CT Online Privacy Act") also specifically prescribe that no controller that offers online service, product, or feature to consumers whom such controller has actual knowledge, or willfully disregards, are minors can process any minor's personal data for the purposes of profiling in furtherance of any automated decision that produces legal or similarly significant effect concerning the minor, unless the controller obtains the minor's consent or, if the minor is younger than 13 years old, the consent of such minor's parent or legal guardian. *See* Section 9(b)(1) of the CT Online Privacy Act.

[6] Section 7001 of California Risk Assessment and Automated Decisionmaking Regulations (March 2024), Section 6-1-1301(20) Colorado Privacy Act, Section 1(22) Connecticut Data Privacy Act, Section 12D-102(25) Delaware Personal Data Privacy Act, Section 1(23) Kentucky Consumer Data Protection Act, Section 2(19) Montana Consumer Data Privacy Act, Section 507-H:1(XXIII) New Hampshire Data Privacy Act, Section 1 New Jersey Data Privacy Act, Section 1(16) Oregon Consumer Privacy Act, Section 47-18-3201(21) Tennessee Information Protection Act, Section 59.1-571 Virginia Consumer Data Protection Act.

[7] UOOMs are a diverse set of desktop and mobile tools designed to give consumers the ability to configure their devices to automatically opt-out of certain processing activities, such as sales or sharing, with online entities with whom they have interactions. While certain US state privacy laws (i.e., California, Colorado, Connecticut, Delaware, Montana, New Jersey, Oregon, Texas) require covered entities to honor opt-out preferences transmitted through UOOMs, the requirement applies only to opting out of targeted advertising and sale of personal data and do not apply to processing for the purpose of profiling. In the initial draft of the New Jersey Consumer Privacy Act, consumers were originally given the right to opt-out of profiling in furtherance of decisions that produce legal or similarly significant effects through the use of a UOOM. However, this provision was removed from the final version of the act during the legislative process. For more details, refer to Section 8(b) and the Explanation remarks on page 2 of the New Jersey Consumer Privacy Act [Sixth Reprint].

GDPR,[8] UK GDPR[9] (and the proposed UK Data Protection and Digital Information Bill),[10] and Brazil's LGPD.[11] The standard also has the benefit of capturing high(er)-risk use cases (e.g., denial of financial or lending services or access to essential goods or services) while providing greater leeway for automated decisions that do not rise to the level of having legal or similar effects on consumers (e.g., decisions ensuring network security and preventing cyber-attacks).

All states in this group define "legal or similarly significant effects" as "*decisions made by the covered entity that result in the provision or denial by the covered entity of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, healthcare services or access to essential goods or services such as food and water.*"[12] The California Draft Risk Assessment and Automated Decisionmaking Regulations introduce the concept of a "significant decision," defined similarly to the legal or similarly significant effect standard employed by other states.[13]

Most Common Approach: Excluding Publicly Available Information – In contrast to the EU GDPR, which does not exclude information collected and processed through publicly available means from its scope of covered personal data,[14] all comprehensive privacy laws in the US define personal information in a way that excludes publicly available information.[15] The concept of "publicly available information" is defined as "*information that is lawfully made available from federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public through widely distributed media, by the consumer, or by a person to whom the consumer has disclosed the information, unless the consumer has restricted the information to a specific audience*."[16] In addition to exempting publicly available information from any opt-out requirements for profiling, this

[8] Article 22 GDPR.
[9] Article 22 UK GDPR.
[10] Data Protection and Digital information (No 2) Bill, Article 22A-D, available here.
[11] Article 20 of the Brazilian Data Protection Law (LGPD) Law No 13853/2019, available here.
[12] Section 6-1-1301(10) Colorado Privacy Act, Section 1(12) Connecticut Data Privacy Act, Section 12D-102(13) Delaware Personal Data Privacy Act, Section 1(10) Kentucky Consumer Data Protection Act, Section 2(10) Montana Consumer Data Privacy Act, Section 507-H:1(XIII), Section 2(11) Nebraska Data Privacy Act, New Hampshire Data Privacy Act, Section 1 New Jersey Data Privacy Act, Section 1(10) Oregon Consumer Privacy Act, Section 47-18-3201(10) Tennessee Information Protection Act, Section 59.1-571 Virginia Consumer Data Protection Act. Please note that the California Risk Assessment
[13] Section 7200(a)(1)(A) of California Risk Assessment and Automated Decisionmaking Regulations (March 2024),
[14] Article 4(1) read in conjunction with Article 14 of the EU GDPR.
[15] Section 1798.140(v)(2) CCPA Section 6-1-1303(17)(b) of Colorado Privacy Act, Section 1(18) Connecticut Privacy Act, Section 12D0102(21) of Delaware Personal Data Privacy and Consumer Protection Act, Section 501.702(19) of Florida Privacy Act, Section 19(b) and Section 26 of Indiana Privacy Act, Section 715D.1(18 & (24) of the Iowa Privacy Act, Section 1(19) Kentucky Consumer Data Protection Act, Section 14-4601(W)(2)(II) Maryland Online Data Privacy Act, Section 2(15)(b) & (22) of Montana Privacy Act, Section 2(20)(b) & (28) Nebraska Data Privacy Act, Section 507-H:1(19)&(26) New Hampshire Privacy Act, Section 1 NJ Privacy Act, Section 1(13)(b)(B) of Oregon Privacy Act, Section 47-18-3201(17)(B)&(24) of Tennessee Privacy Act, Section 541.001(19) & (27) of Texas Privacy Act, Section 13-61-10124(b) Utah Privacy Act, Section 59.1-571 of Virginia Privacy Act.
[16] *Ibid.*

exclusion also is generally useful for some developers of large language models, as they may rely on publicly available data sources to help train those models.[17]

Other Approach: Limited Form of Automated Processing – Florida, Indiana, Maryland, Nebraska, and Texas limit their definitions of profiling to any form of *solely* automated processing, excluding, for example, profiling activities involving partial human involvement.[18] As a result, consumers cannot exercise the right to opt out regarding profiling activities that include human involvement.

Other Approach: No Regulation on Profiling Activities in Utah and Iowa – Utah and Iowa do not address the concept of profiling in their comprehensive state privacy laws, and, thus, also do not include the right to opt out of profiling activities conducted by organizations.

Other Approach: Tiered Approach in Colorado – The Colorado Privacy Rules categorize automated processing into three distinct types: solely automated processing, human reviewed automated processing, and human involved automated processing.[19]

> "(i) Solely Automated Processing means the automated processing of personal data with no human review, oversight, involvement, or intervention.
> (ii) Human Reviewed Automated Processing means the automated processing of Personal Data where a human reviews the automated processing, but the level of human engagement does not rise to the level required for Human Involved Automated Processing. Review of the output of the automated processing with no meaningful consideration [of "available data" used in the processing or any output of the processing] does not rise to the level of Human Involved Automated Processing (available data is not further defined).
> (iii) Human Involved Automated Processing means the automated processing of Personal Data where a human (1) engages in a meaningful consideration of available data used in the Processing or any output of the Processing and (2) has the authority to change or influence the outcome of the Processing."[20]

The Colorado Privacy Rules recognize the right to opt-out of profiling in furtherance of decisions that produce legal or other similarly significant effects based on "solely automated processing" and "human reviewed automated processing."[21] Covered entities are not required to take action on a request to opt-out of profiling if the processing activity is based on "human involved automated processing."

[17] Note that certain states consider implementing regulations concerning the ethical and responsible deployment of generative AI technologies. For instance, in California, the Governor Gavin Newsom has signed an AI Executive Order mandating state agencies to report on the risks and potential harms to communities as well as beneficial uses of generative AI within the state. The Executive Order also tasks agencies with establishing a regulatory sandbox environment to facilitate the testing of generative AI projects. For more information, please see here.
[18] Section 501.1735(1)(i) Florida Digital Bill of Rights, Chapter 2 Section 23 Indiana Consumer Privacy Act, Section 14-4601(AA) in conjunction with Section 14-4605(b)(7)(III) Maryland Online Data Privacy Act, and Section 541.001(24), Section 2(25) Nebraska Data Privacy Act, Texas Data Privacy and Security Act.
[19] Rule 9.04(B) of the CPA Rules.
[20] Rule 2.02 of the CPA Rules
[21] Rule 9.04(B) of the CPA Rules.

Nevertheless, they are still required to provide certain disclosures (at or before processing occurs) to consumers in the privacy notice, including the decision subject to profiling, categories of personal data that were or will be used as part of the profiling, plain language explanation of the logic used and the role of human involvement in the profiling process, the benefits and potential consequences of decisions based on the profiling, and an explanation of how consumers can correct or delete personal data used in the profiling in the decisionmaking process.[22]

Other Approach: California Opt-out Regulation is Not Limited to Profiling – The California privacy laws give the California Privacy Protection Agency (**"CPPA"** or **"Agency"**) rulemaking authority to issue regulations governing access and opt-out rights with respect to businesses' use of automated decisionmaking technology (**"ADMT"**), including profiling.[23]

The draft regulations follow a three-steps test to determine whether a given processing falls within the scope of the opt-out rights:

1. Determining whether a processing activity falls under the definition of "automated decisionmaking technology."

In its draft Risk Assessment and ADMT Regulations, the Agency specifies that consumers have a right to opt-out of the business's use of automated decisionmaking technology for a broad range of activities, including but not limited to profiling activities.[24] The draft regulations define automated decisionmaking technology as "*any technology that processes personal information and uses computation to execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking*." For the purposes of this definition, "technology" includes software or programs, including those derived from machine learning, statistics, other data-processing techniques, or artificial intelligence. The draft regulations also clarify that "substantially facilitate human decisionmaking" means using the output of the technology as a key factor in a human's decisionmaking. The draft regulations also note that automated decisionmaking technology includes profiling. However, the term excludes certain technologies, provided that they do not execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking.[25]

2. If a processing activity qualifies as an ADMT, whether it is used for a covered purpose.

---

[22] Rule 9.04(C) of the CPA Rules.
[23] Civil Code Section 1798.185 (a)(16).
[24] Section 7001 of the California's Draft Risk Assessment and Automated Decisionmaking Regulations (March 2024), available California Privacy Protection Agency March 8, 2024 Board Meeting Records, https://www.cppa.ca.gov/meetings/materials/20240308_item4_draft_risk.pdf. Please note that the CPPA, on March 8, 2024, discussed and voted 3-2 to progress toward formalizing the draft regulations regarding risk assessments and automated decisionmaking technology. However, the Agency did not initiate the formal rulemaking process for these regulations, which is anticipated to begin in July 2024.
[25] These technologies include: web hosting, domain registration, networking, caching, website loading, data storage, firewalls, anti-virus, anti-malware, spam- and robocall-filtering, spellchecking, calculators, databases, spreadsheets, or similar technologies. Section 7001 Draft California Risk Assessment and ADMT Regulations (March 2024).

The CPPA's authority to create regulations regarding access and opt-out rights concerning ADMT includes and extends beyond "significant decisions concerning a consumer," a concept which aligns conceptually with the "legal or similarly significant effects" standard. The regulation gives consumers the right to opt-out of a covered entity's use of ADMT for this and several other specific purposes,[26] which are referred to as covered purposes, namely:

- **For a significant decision concerning a consumer**. For the purposes of this article, "significant decision" means a decision using information that is not subject to the exceptions, that results in access to, or the provision or denial of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services;

- **For extensive profiling of a consumer**. For the purposes of this article, "extensive profiling" means:
    - Profiling a consumer through systematic observation when they are acting in their capacity as an applicant to an educational program, job applicant, student, employee, or independent contractor ("work or educational profiling");
    - Profiling a consumer through systematic observation of a publicly accessible place ("public profiling"); or,
    - Profiling a consumer for behavioral advertising.

- **For training uses of automated decisionmaking technology**, which includes processing consumers' personal information to train automated decisionmaking technology that is capable of being used for any of the following:
    - For a significant decision concerning a consumer;
    - To establish individual identity;
    - For physical or biological identification or profiling;[27] or,
      For the generation of a deepfake. [28]

3. If an ADMT is used for a covered purpose, whether organizations can rely on exceptions that allow them to be exempted from the scope of opt-out rights.

The Draft California Risk Assessment and ADMT Regulations also outline several exceptions to the obligation of providing the right to opt-out to consumers for covered purposes (except profiling for

[26] Section 7221(a) Draft California Risk Assessment and ADMT Regulations (March 2024).
[27] The Draft California Risk Assessment and ADMT Regulations (March 2024) further requires a business that uses physical or biological identification or profiling to (i) conduct an evaluation of the physical or biological identification or profiling to ensure that it works as intended for the business's proposed use and does not discriminate based upon protected classes; and (ii) implement policies, procedures, and training to ensure that the physical or biological identification or profiling works as intended for the business's proposed use and does not discriminate based upon protected classes. *See* Section 7201 Draft California Risk Assessment and ADMT Regulations (March 2024).
[28] Section 7200 of Draft California Risk Assessment and ADMT Regulation.

behavioral advertising or for training uses of automated decisionmaking technology, for which businesses must provide a right to opt out in all circumstances).[29] Specifically, a business would not be required to provide consumers with the ability to opt-out of a business's use of ADMT for a significant decision concerning a consumer, for work or educational profiling or public profiling in the following circumstances:

- The business's use of that ADMT is necessary to achieve, and is used solely for, security, fraud prevention, or safety purposes ("security, fraud prevention, and safety exception");

- For any significant decision concerning a consumer, if the business provides the consumer with a method to appeal the decision to a qualified human reviewer who has the authority to overturn the decision ("human appeal exception");

- For admission, acceptance, or hiring decisions, if the following are true: (i) the ADMT is necessary to achieve, and is used solely for, the business's assessment of the consumer's ability to perform at work or in an educational program to determine whether to admit, accept, or hire them, and (ii) the business has conducted an evaluation of the ADMT to ensure it works as intended for the business's proposed use and does not discriminate based on protected classes, and has implemented policies, procedures and training accordingly;

- For allocation/assignment of work and compensation decisions, if the following are true: (i) the ADMT is necessary to achieve, and is used solely for, the business's allocation/assignment of work or compensation, and (ii) the business has conducted an evaluation of the ADMT and has implemented accuracy and nondiscrimination safeguards; and,

- For work or educational profiling, if the following are true: (i) the ADMT is necessary to achieve, and is used solely for, an assessment of the consumer's ability to perform at work or in an educational program, or their actual performance at work or in an educational program, and (ii) the business has conducted an evaluation of the ADMT and has implemented accuracy and nondiscrimination safeguards.[30]

The Draft California Risk Assessment and ADMT regulations also stipulate that covered entities are required to offer at least two methods for consumers to submit requests to opt-out of the use of the ADMT.[31] In addition, the Draft Regulations mandate that at least one of these methods should be provided in the manner in which the business primarily interacts with the consumer. The Draft Regulations also prescribe illustrative examples of methods that covered entities can integrate, such as via an interactive online form accessible in the privacy notices, a designated email address, and a form submitted in person. However, they explicitly state that a notification or tool regarding cookies, such as cookie banner or cookie

[29] Section 7221(b) of Draft California Risk Assessment ADMT Regulation.
[30] Section 7221(b)(1), (2), (3), (4) and (5) of Draft California Risk Assessment ADMT Regulation.
[31] Section 7221(c) of the Draft California Risk Assessment ADMT Regulation.

controls, is not by itself an acceptable method for submitting opt-out requests. The Draft Regulations also require that covered entities cannot make the exercise of opt-out requests contingent upon the creation of an account or the provision of unnecessary additional information.[32] Furthermore, it prohibits entities from seeking a consumer's consent for at least twelve months from the date of exercising the right to opt-out from the use of ADMT.[33]

Other Approach: Opt-in Requirement in New Jersey for Profiling Concerning Minors – New Jersey's privacy rules prohibit covered entities from processing personal data for the purposes of profiling that produces legal or similarly significant effects without consent if they have actual knowledge or willfully disregard that the consumer is aged between 13 and 17 years old.[34]

Findings & Recommendations:

- Organizations are seeking to establish standardized methods for handling consumer requests, including opt-out of profiling rights, in a manner that is globally applicable. For this purpose, they generally adopt a consistent and uniform definition of profiling, often referencing the GDPR as a benchmark. However, they are also paying particular attention to California's Draft Risk Assessment and ADMT Regulations (and the forthcoming rulemaking process) and certain U.S. state privacy laws such as Connecticut, Delaware, and Virginia, recognizing that these regulations broaden the scope of profiling rules beyond the GDPR, which is limited to "solely automated means." This broader scope suggests that, regardless of any level of human intervention in the process, the processing for the purposes of profiling activities will trigger additional compliance obligations. Lawmakers and regulators should clarify whether and to what extent human intervention in the process will exempt the processing activity from falling within the scope of profiling rules, with the aim of greater consistency between global and domestic requirements. While the differentiation among the three types of automated processing outlined in Colorado state privacy law is a positive step, it is uncertain whether organizations will be able to meaningfully distinguish three distinct types of automated processing for operational and compliance purposes.

- The internal review of a processing activity involves organizations conducting a contextual analysis to determine if the specific processing activity meets the "legal or similarly significant" threshold. Organizations report that when multiple state privacy laws are applicable to the processing activity, they are likely to use the broadest definition of the standard as the baseline. Lawmakers or regulators should provide illustrative examples of profiling producing legal or similarly significant effects and parameters for the threshold to be reached. This will provide clarity and consistency to organizations, although they should also be able to rebut the presumption of those examples producing legal or similarly significant effects in practice. Based

[32] Section 7221(e) of the Draft California Risk Assessment ADMT Regulation.
[33] Section 7221(k) of the Draft California Risk Assessment ADMT Regulation.
[34] Section 9(7) of the New Jersey Privacy Act.

on wide input from organizations in different sectors, CIPL has already prepared a list of examples of decisions which we believe could produce legal effects or similarly significant effects and of decisions we believe do not produce such effects.[35] State law- and policy-makers are encouraged to create a similar list of examples.

- Organizations are concerned about the operational challenges stemming from the ADMT regulations in California, particularly in determining whether their products and data processing activities fall under the covered purposes. This challenge is likely to become more complex due to the fact that California's opt-out rights for profiling activities also apply in the employment context. In addition, if the majority of organizations' ADMT uses are within scope, managing opt-out rights from ADMT could pose technical challenges for organizations because centralizing the collection and execution of opt-outs across multiple systems may require considerable time and resources to develop. Importantly, these challenges may intensify if additional laws with distinct scopes and definitions emerge in the future. Therefore, lawmakers and regulators should avoid forcing organizations to create separate opt-out mechanisms for each state, resulting in inefficient use of resources and time that could be better allocated for implementing meaningful privacy protections.

- Even though Utah and Iowa state privacy laws do not specifically address the concept of profiling or the corresponding opt-out rights related to profiling activities, many organizations still apply the same approach to profiling regulation as outlined in other state laws. This practice illustrates the value and importance of regulatory consistency across jurisdictions from the perspective of businesses.

- Some organizations have suggested that complying with a potential universal opt-out mechanism requirement for profiling activities would pose more implementation challenges compared to existing universal opt-out mechanisms for sales and targeted advertising. This is because the nature of "profiling" activities significantly differs from sales and targeted advertising. Expanding universal opt-out mechanism requirements to include profiling opt-outs could inadvertently lead organizations to adopt more privacy-invasive practices. For example, organizations might be compelled to specifically identify individuals visiting their websites in cases where those individuals may later invoke universal opt-out requests for profiling activities. Therefore, many organizations believe that a more suitable and effective approach in the context of profiling is to continue requiring individuals to receive a notice at or before the point of profiling, informing them about the processing activities and providing them with the option to opt-out.

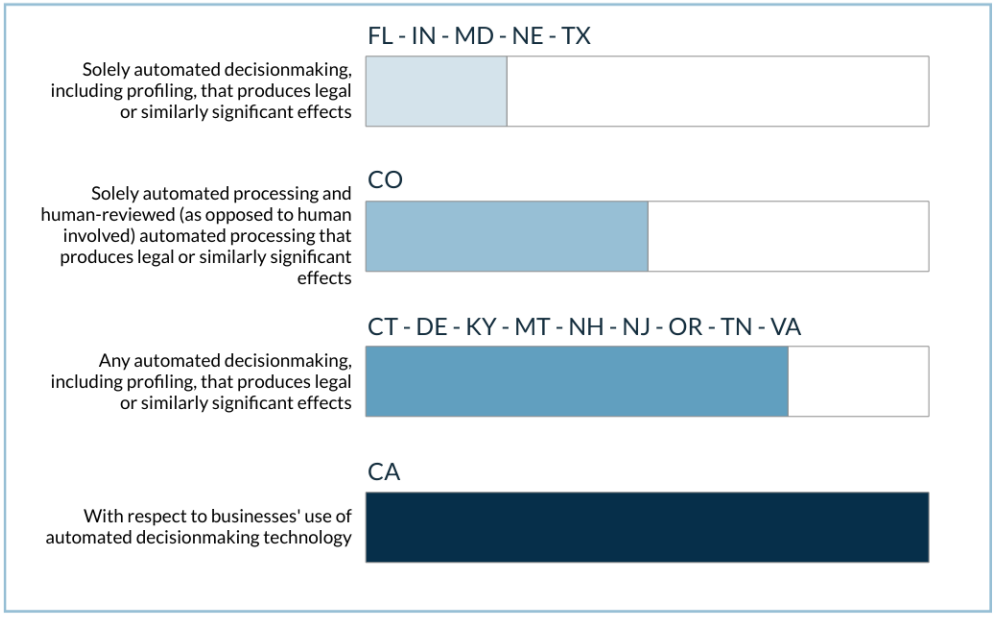
[35] Centre for Information Policy Leadership, "*Response by CIPL to the CPPA's Invitation for Preliminary Comments on Proposed Rulemaking on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking*", March 27, 2023, pages 14-15, available here.

- Organizations evaluate whether and how to use publicly available information on a case-by-case basis. For contexts such as development of generative AI, publicly available data is important for ensuring model quality and functionality. States should ensure that the training of such models can take place using publicly available information, provided that those using the data put in place demonstrable policies and procedures to ensure that the data are used responsibly.[36] Furthermore, states should clarify that the training of models does not automatically constitute automated decision-making or profiling, which would trigger the right to opt out of profiling.

[36] Centre for Information Policy Leadership, "*Response to ICO Consultation on the Lawful Basis for Web Scraping to Train Generative AI Models*," March 1, 2024, available here.

Scope of Opt-out Rights in the Context of Automated Decisionmaking and Profiling

Opt-out Rights for ADM & Profiling Activities



No Opt-out Rights for Profiling

IA UT

For Comparison: Opt-in Consent for ADM & Profiling Activities

For solely ADM, including profiling, that produces legal or similarly significant effects on individuals

EU UK

For profiling involving special categories of personal data

EU UK

For profiling Concerning Minors

NJ

Findings and Recommendations

Organizations globally adopt standardized methods, often referencing GDPR, for handling consumer requests including opting out of profiling.

Lawmakers and regulators must clarify the impact of human intervention on exempting processing from profiling rules.

The legal or similarly significant effects standard should be clarified with illustrative examples.

Compliance challenges may arise if additional law with distinct and prescriptive requirements emerge in the future.

Source: Centre for Information Policy Leadership

2. Notice Requirement

Most Common Approach: General Notice Requirement – All US state privacy laws require covered entities to provide consumers with a reasonably accessible, clear and meaningful privacy notice while some states (see below) also have specific additional ADM-related requirements.[37] This general notice should include various elements, including instructions on how consumers can exercise their rights, such as the right to opt out of profiling activities that produce legal or similarly significant effects. Covered entities must also describe how a consumer may appeal decisions made by the entity in response to the consumer's request.

Other Approach: Specific Pre-Notice Requirement in Colorado – The Colorado Privacy Act Rules prescribe a specific privacy notice requirement for profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer.[38] In particular, such a privacy notice must, at a minimum, include: (i) what decision is subject to profiling; (ii) the categories of personal data that were or will be processed as part of the profiling; (iii) a non-technical, plain language explanation of the logic used in the profiling process; (iv) a non-technical, plain language explanation of how profiling is used in the decisionmaking process, including the role of human involvement, if any; (v) if the system has been evaluated for accuracy, fairness, or bias, and the outcome of any such evaluation; (vi) the benefits and potential consequences of the decision based on the profiling; and (vii) information about how a consumer may exercise the right to opt-out of the processing of personal data for profiling in furtherance of decisions that produce legal or other similarly significant effects. In addition, as addressed in Section 1 above, covered entities are also required to provide certain disclosures at or before the processing occurs, if they decide not to take action on a request to opt out of profiling if it is based on human involved automated processing.[39]

Other Approach: Pre- and Post-Notice Requirements in California – The Draft California Risk Assessment and ADMT Regulation specifically imposes a pre-use notice requirement on businesses using ADMT for covered purposes before engaging in such processing activities.[40] Similar to Colorado's notice

[37] Section 7220 California Draft Risk Assessment and ADMT Regulation, Section 6-1-1308(1)(A) Colorado Privacy Act, Section 6(c) Connecticut Data Privacy Act, Section 12D-106 (c) Delaware Personal Data Privacy Act, Section 501.711(1) Florida Digital Bill of Rights, Chapter 4 Section 3 Indiana Consumer Privacy Act, Section 4(3) Kentucky Consumer Data Protection Act, Section 14-4607(D) Maryland Online Data Privacy Act, Section 7(5) Montana Consumer Data Privacy Act, Section 13 Nebraska Data Privacy Act, Section 507-H:6(3) New Hampshire Data Privacy Act, Section 3(a) New Jersey Data Privacy Act, Section 5(4) Oregon Consumer Privacy Act, Section 47-18-3204(c) Tennessee Information Protection Act, Section 541.102 Texas Data Privacy and Security Act, Section 59.1-574(c) Virginia Consumer Data Protection Act. While Iowa and Utah also require a notice, they do not offer the right to opt-out of profiling activities. This means that informing consumers of how to exercise this right would not be one of the subjects of the notice requirement in these states.

[38] Rule 9.03(A) of the CPA Rules. Rule 9.03(B) also acknowledges that the notice requirement will not be interpreted as obliging covered entities to disclose their trade secrets.

[39] Rule 9.04 of the CPA Rules.

[40] Section 7220 of the Draft California Risk Assessment ADMT Regulation. The pre-use notice must be presented prominently and conspicuously to the consumer before the business process the consumer's personal information using ADMT and also be presented in the manner in which the business primarily interacts with the consumer.

requirement, the Draft California ADMT Regulation requires businesses to include the following elements in their pre-use notices:

> (i) A plain language explanation of the specific purpose for which the business proposes to use the ADMT;
> (ii) A description of the consumer's right to opt-out and access information about the business's use of the ADMT, along with instructions on how a consumer can exercise these rights;
> (iii) That the business is prohibited from retaliating against consumers for exercising their CCPA rights; and,
> (iv) A simple and easy-to-use method, such as a layered notice or hyperlink, for consumers to obtain additional information about the use of ADMT. This additional information should include details about the logic used, key parameters affecting the output, intended output, how the business plans to use the output for decisionmaking, and the role of any human involvement.[41]

Importantly, covered entities are prohibited from describing the purpose of their use of ADMT in generic terms, such as "to improve services," because generic terms are found insufficient for consumers to understand the intended purpose for using the ADMT.[42]

The Draft California Risk Assessment and ADMT Regulation also includes a requirement for covered entities to provide consumers with a post-notice when a business used ADMT for certain significant decisions that are adverse to the consumer ("adverse significant decision") as soon as possible, but no later than 15 business days from the date of the adverse significant decision.[43] The Draft Regulation defines "adverse significant decision" as (i) resulted in a consumer who was acting in their capacity as a student, employee, or independent contractor being denied an educational credential; having their compensation decreased; or being suspended, demoted, terminated, or expelled, or (ii) resulted in a consumer being denied financial or lending services, housing, insurance, criminal justice, healthcare services, or essential goods or services. The notice must include:

> (i) that the business used ADMT to make the significant decision with respect to the consumer,
> (ii) that the business is prohibited from retaliating against consumers for exercising their CCPA rights,
> (iii) that the consumer has a right to access information about the business's use of the ADMT and how the consumer can exercise their access rights, and

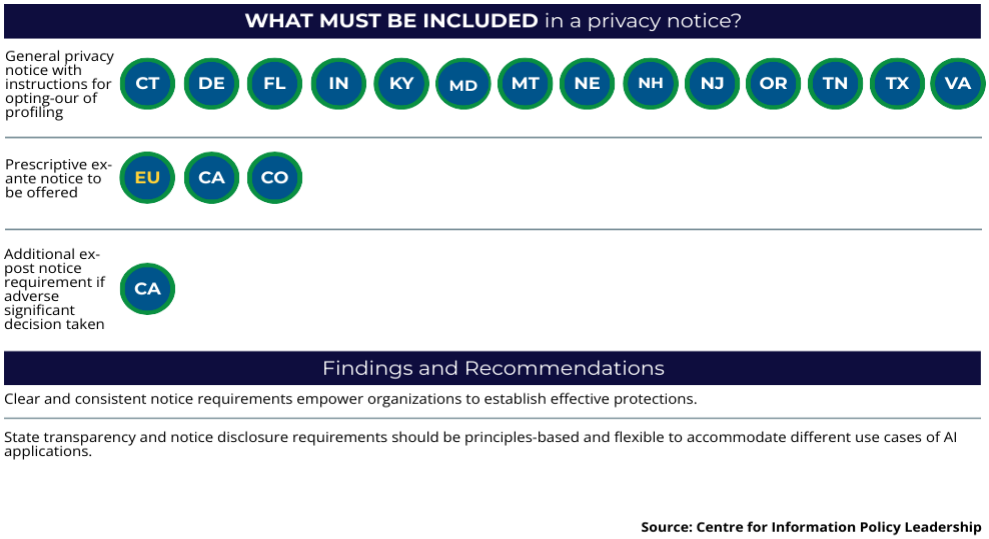
[41] Section 7220(b)(4) of the Draft California Risk Assessment ADMT Regulation. Note that if a business relying upon security, fraud prevention, and safety exception to providing a consumer with the ability to opt-out, it is not required to provide information that would compromise its use of ADMT for these security, fraud prevention, or safety purposes. Also, if the business proposes to use ADMT solely for training uses of ADMT, the business is not required to include the prescribed additional information (subheading iv).
[42] *Ibid.*
[43] Section 7222(k)(1) Draft California Risk Assessment ADMT Regulation.

(iv) if the business is relying upon the human appeal exceptions, that the consumer can appeal the decision and how the consumer can submit the appeal and any supporting documentation.[44]

Findings & Recommendations:

- Organizations typically evaluate whether state-specific notices are necessary, such as in cases where their existing notices do not align with state formatting or content requirements. Where there are substantive differences, they typically adjust their notices, for example, by implementing a state-specific notice mechanism for California, especially for broader applications like employee data. However, this process of creating and maintaining jurisdiction-specific notices places a significant time and resource burden on organizations. Indeed, the sustainability of this approach is called into question by the continual enactment of new state laws and varying regulatory interpretations of notice requirements. More consistency in state notice requirements would enable organizations to focus resources on ensuring that notices provide meaningful transparency rather than ensuring "box-checking"-style compliance with heterogeneous requirements.

- Transparency and notice disclosure are fundamental features of nearly all privacy laws worldwide. One major objective of these principles is empowerment of individuals. They provide visibility into an organization's commitment to use data for specified purposes and not for other unspecified or unexpected purposes. States' transparency and notice disclosure requirements should be principles-based, given that there are countless AI contexts and appropriate transparency may look very different for different AI applications. Providing appropriate AI transparency is contextual and rules on transparency should be flexible enough to accommodate different use cases.



[44] Section 7222(k)(2) Draft California Risk Assessment ADMT Regulation.

3. Access Right

Most Common Approach: General Access Right – Most US state privacy laws provide consumers the right to confirm whether a controller is processing the consumer's personal data and to access such personal data, unless such confirmation or access would require the controller to reveal a trade secret.[45] This obligation extends to profiling activities conducted by covered entities subject to access rights.

Other Approach: Specific Access Right in California – The Draft California Risk Assessment and ADMT Regulation specifies the consumer's right to access information about the business's use of ADMT for a covered purpose concerning the consumer (except if a business uses ADMT solely for training uses of ADMT).[46] In particular, when responding to a consumer's request to exercise the access right, a business must provide plain language explanations of certain information, including (i) the specific purpose for which the business used ADMT; (ii) the output of the ADMT concerning the consumer; (iii) how the business used the output to make a decision regarding the consumer; (iv) how the automated decisionmaking technology worked regarding the consumer (including information about the logic, key parameters affecting the output, aggregate output statistics); (v) that the business is prohibited from retaliating against consumers for exercising their CCPA rights; and, (vi) instructions for how the consumer can exercise other CCPA rights.[47]

Findings & Recommendations:

- Organizations usually have a centralized team for responding to data subject access requests, and those requests are reviewed on a case-by-case basis. The emergence of different and more expansive requirements for access rights in some states poses challenges for organizations seeking to maintain uniform procedures for responding to requests. To the extent that novel different requirements are prescriptive without creating substantive new protections for individuals, they may make compliance more difficult without corresponding, material benefits.

- Privacy rules should not be interpreted by state lawmakers and regulators in a way that requires organizations to provide "full transparency" of algorithms (i.e. disclosure of source code or extensive descriptions of the inner workings of algorithms, including scoring models) when responding to a consumer's access request. In many instances, such an approach would not

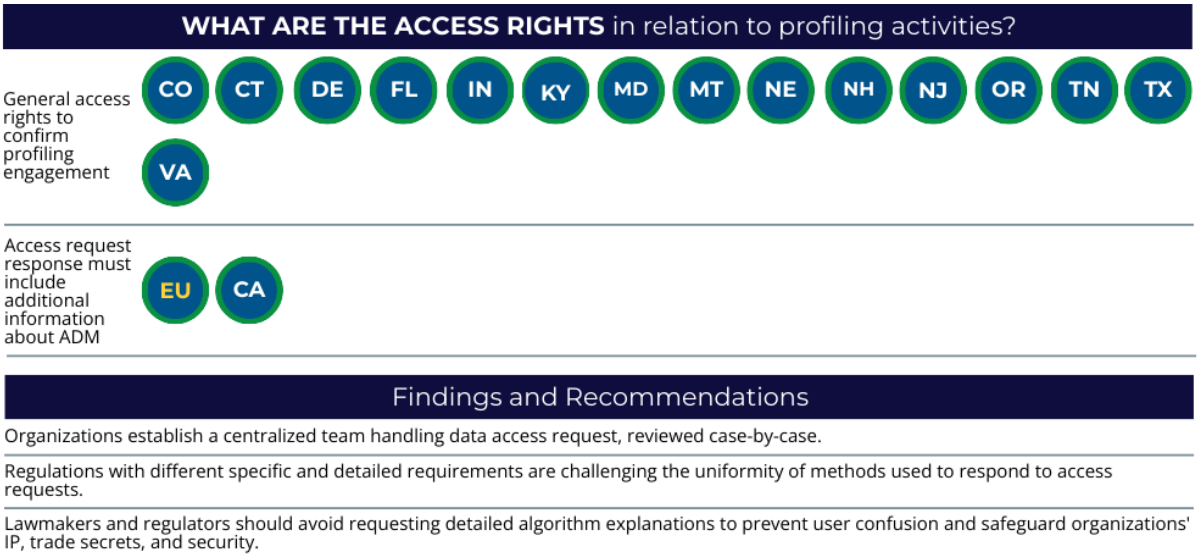
[45] Section 7222(a) California Draft Risk Assessment and ADMT Regulation, Section 6-1-1306(1)(B) Colorado Privacy Act, Section 4(a)(1) Connecticut Data Privacy Act, Section 12D-104(a)(1) Delaware Personal Data Privacy Act, Section 501.705(2)(a) Florida Digital Bill of Rights, Chapter 3 Section 1(b)(1) Indiana Consumer Privacy Act, Section 3(2)(a) Kentucky Consumer Data Protection Act, Section 14-4605(B)(2) Maryland Online Data Privacy Act, Section 5(1)(a) Montana Consumer Data Privacy Act, Section 7(2)(a) Nebraska Data Privacy Act, Section 507-H:4(1)(a) New Hampshire Data Privacy Act, Section 7(a)(1) New Jersey Data Privacy Act, Section 3(1)(a)(a) Oregon Consumer Privacy Act, Section 47-18-3203(a)(2)(A) Tennessee Information Protection Act, Section 541.051(b)(1) Texas Data Privacy and Security Act, Section 59.1-573(a)(1) Virginia Consumer Data Protection Act. While Iowa and Utah also provide consumers with access rights, they do not offer the right to opt-out of profiling activities.

[46] Section 7222(a) Draft California Risk Assessment ADMT Regulation. The business must respond to a request to access as soon as feasibly possible, but no later than 45 calendar days from the date of the business receives the request.

[47] Section 7222(b) Draft California Risk Assessment ADMT Regulation.

meaningfully advance people's understanding of how their data is being handled in automated decisionmaking processes.

- In addition, when considering the extent of any transparency to be provided, it must be kept in mind that full transparency of algorithms raises intellectual property and trade secret issues for organizations, just like the disclosure of other types of proprietary information, such as software and patents. Protecting algorithms from full disclosure is vital for technological innovation. Finally, maintaining a minimum level of opaqueness surrounding how algorithms operate is necessary to prevent individuals from manipulating the algorithm unethically or illegally for personal gain (e.g. an individual who is able to obtain full disclosure of the algorithmic process and criteria for deciding who to audit for tax purposes). This is comparable to situations where the security of processing would be put at risk if full transparency of security measures and protections are made available to bad actors.



Source: Centre for Information Policy Leadership

4. Data Protection Assessment

Most Common Approach: Heightened Risk of Harm – As highlighted in the CIPL Discussion Paper on Data Protection Assessments, the privacy laws in many US states explicitly require a data protection assessment for processing activities that present a heightened risk of harm to consumers.[48] This includes profiling that presents a reasonably foreseeable risk of substantial injury to consumers, such as unfair or deceptive treatment, financial, physical, or reputational injury. Furthermore, these states require similar content elements to be covered in data protection assessments, including asking covered entities to demonstrate how their risk assessments weigh the benefits of the processing against the risks that it may cause to individuals, and which safeguards are in place.[49] In doing so, they also prescribe similar factors to be considered, including (i) the use of deidentified data, (ii) reasonable expectations of consumers, (iii) the context of the processing and (iv) the relationship between the covered entities and consumer whose personal data will be processed.[50]

Other Approach: Additional Requirements for a Business Using ADMT in California and Processing for Profiling Purposes in Colorado – The Draft California Risk Assessment and ADMT Regulations set forth additional risk assessment content requirements for businesses using automated decisionmaking technology.[51] Accordingly, businesses must provide a plain language explanation of the following:

- Whether the business evaluated the ADMT to ensure it works as intended for the business's proposed use and does not discriminate based upon protected classes;

- The policies, procedures, and training the business has implemented or plans to implement to ensure that the ADMT works as intended for the business's proposed use and does not discriminate based upon protected classes;

- The output(s) secured from the ADMT and how the business will use the output(s);

- The actions the business has taken or any actions it plans to take to maintain the quality of personal information processed by the ADMT, including the source of personal information and whether that source is reliable; and,

[48] Section 7152 California Draft Risk Assessment and ADMT Regulation, Section 6-1-1309 Colorado Privacy Act and Rule 9.06 Colorado Privacy Act Rules, Section 8 Connecticut Data Privacy Act, Section 12D-108 Delaware Personal Data Privacy Act, Section 501.713 Florida Digital Bill of Rights, Chapter 6 Section 1 Indiana Consumer Privacy Act, Section 6(1) Kentucky Consumer Data Protection Act, Section 14-4610 Maryland Online Data Privacy Act, Section 9(1) Montana Consumer Data Privacy Act, Section 16 Nebraska Data Privacy Act, Section 507-H:8(I) New Hampshire Data Privacy Act, Section 9(a)(9) and Section 9(b) & (c) New Jersey Data Privacy Act, Section 8 Oregon Consumer Privacy Act, Section 47-18-3206 Tennessee Information Protection Act, Section 541.105 Texas Data Privacy and Security Act, Section 59.1-576 Virginia Consumer Data Protection Act.
[49] *Ibid.*
[50] *Ibid.*
[51] Section 7152 of California's Draft Risk Assessment Regulations.

- The logic of ADMT including any assumptions of the logic.[52]

The Colorado Privacy Act Rules outline a list of additional content requirements for businesses processing personal data for profiling purposes, which are conceptually similar to those listed above.[53] It is important to emphasize once more that the scope of profiling regulation in Colorado is narrower compared to the ADMT regulation in California, which addresses processing activities beyond profiling.[54]

Other Approach: Additional Requirements for a Business Training AI or ADMT in California – In cases where an organization processes personal information to train AI or ADMT and makes the technology available to others for use, California's draft regulations would also require the organization to provide users with a plain language explanation of any requirements for or limitations on the use of ADMT or AI.[55] Additionally, if an organization processes personal information to train AI or ADMT and makes the technology available to other organizations (referred to as "recipient-businesses"), the organization must provide all facts necessary for those recipient-businesses to conduct the recipient-businesses' risk assessments.[56] The California Draft Regulations highlight that the above requirements are only applicable to ADMT and AI trained using personal information.

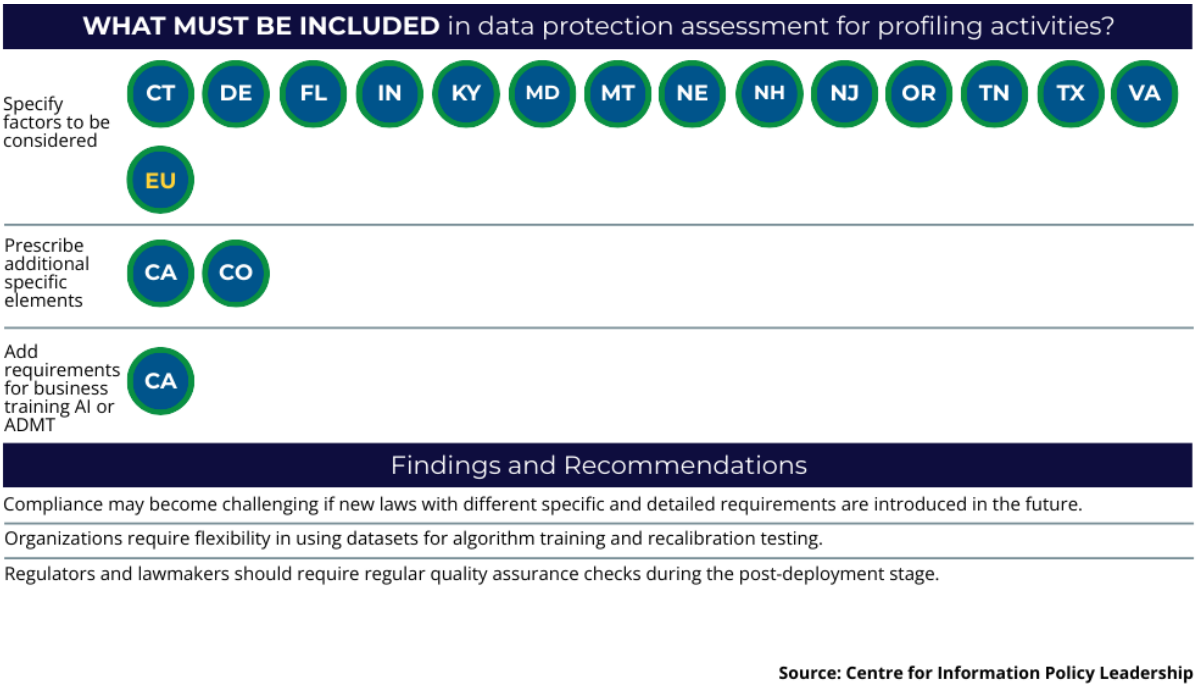
Findings & Recommendations:

- Organizations often establish comprehensive privacy programs of which data protection assessments are crucial components. These programs are designed to fulfill vital compliance requirements across various US and global jurisdictions while maintaining consistent safeguards for their customers. However, as new laws with specific and prescriptive requirements continue to emerge, e.g., in California and Colorado, this approach may become increasingly complex. As a result, organizations may find themselves needing to create separate assessments for each state, deviating from their unified global strategy. This leads to redundant processes and inefficient allocation of resources and time, which could otherwise be used to implement more impactful privacy measures.

- Before deploying a new profiling or ADMT process, organizations must identify potential risks and harms associated with the process and take appropriate steps to mitigate such harms. For example, if a risk assessment shows that an ADMT tool yields biased results, the organization, having conducted a risk assessment to determine this can recalibrate the specific ADMT model to ensure fair outcomes. States should permit organizations to use datasets for training the algorithm and testing the recalibration, rather than imposing processing restrictions when the risks to consumers outweigh the benefits, as this could also amount to prior restraint on speech. Having this ability to recalibrate is crucial for organizations deploying new profiling and ADM

[52] Sections 7152(a)(2)(B), 7152(a)(3)(G), and 7152(a)(6)(B) of California's Draft Risk Assessment and ADMT Regulations (March 2024).
[53] Rule 9.06(f) of the CPA Rules.
[54] See Section 2 above.
[55] Section 7153(b) of California's Draft Risk Assessment and ADMT Regulations.
[56] Section 7153(a) of California's Draft Risk Assessment and ADMT Regulations.

processes. Furthermore, lawmakers and regulators should require that organizations engage in regular quality assurance checks and algorithmic auditing after a profiling or ADMT process has been deployed. These practices constitute important best practices to ensure fairness and mitigate risks associated with ADMT systems.



Source: Centre for Information Policy Leadership

5. Specific State-level AI Regulations

In October 2023, U.S. President Biden issued an Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, directing actions across certain areas, including advancing equity and civil rights, and standards for AI safety and security.[57] While implementation of the Executive Order continues, several states have passed laws related to AI and automated decision-making, with many more proposed as of the time of writing of this paper.[58] This is particularly notable in the context of employment and algorithmic discrimination.

Employment-specific AI regulations in Maryland, Illinois, and New York: In the absence of a federal-level regulation,[59] a few states, including Maryland, Illinois, and New York have passed legislation to regulate the use of artificial intelligence in employment settings.[60] Maryland's HB1202 prohibits employers from using certain facial recognition services (e.g., to create a facial template) during a job applicant's interview unless the applicant provides written consent.[61] Similarly, the Illinois AI Video Interview Act restricts employers' ability to analyze recorded video interviews of job applicants using AI, permitting such use only if candidates are informed in advance about the process and how AI analysis works, and consent to this practice.[62] Employers that solely rely on this technology for interview analysis must collect the demographic data (e.g., race, ethnicity) of those selected, rejected, and ultimately hired, and must submit this data annually to the IL Department of Commerce and Economic Opportunity for review. The scope of New York City Local Law 144 is broader than that of Maryland and Illinois, regulating the use of automated employment decision tools for both job applicants and employees.[63] It prohibits the use of such tools to screen applicants for hiring decisions or employees for promotion decisions without proper notice and unless an independent auditor conducts an annual bias audit before their use, and the audit results are

[57] See Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, available here. The Executive Order directs a number of agencies to take actions related to ensuring the fairness of automated systems. However, these requirements are expected to be articulated within 180 days of the release, which is around April 2024. Notably, the Executive Order requires private companies to share with the federal government the result of red-team safety tests for foundation models that pose a serious risk to national security, public health and safety. The Administration will also issue guidance to landlords, federal benefits programs, and federal contractors to prevent AI algorithms from contributing to discrimination and will use training and technical assistance to advance best practices for investigation and prosecuting AI-related civil rights violations. Another provision of the Executive Order empower the Department of Health and Human Services to establish a safety program to address risks associated with the use of AI in healthcare.

[58] Ryan Heath, "*Exclusive: States are introducing 50 AI-related bills per week*," *Axios,* February 14, 2024, available here.

[59] Please note that the Algorithmic Accountability Act was introduced in both 2022 and 2023 to tackle the use of AI in employment decisionmaking. However, as of May 10, 2024, the Act had not been passed.

[60] Additional pending laws include: Massachusetts H.1873 "An Act Preventing a Dystopian Work Environment;" Illinois HB3773 which would amend state's Human Rights Act to include in scope an employer's use of predictive data analytics; New Jersey S1588 which would regulate the use of AI tools in hiring decisions to minimize discrimination; and Vermont H.114 which would regulate employee data and ADM tools used for employment related decisions, judgements, or conclusions.

[61] Maryland House Bill 1202, Available here.

[62] Illinois Artificial Video Interview Act, available here.

[63] New York City Local Law 144, Available here.

published on the employer's website. Additionally, New York's pending Bill S56641A requires that both the deployer and developer of an automated employment decision tool must conduct an impact assessment for any automated employment decision tools that are used, and must establish a governance program referencing reasonable safeguards that are put in place.[64]

Algorithmic Discrimination: Several states, including California,[65] Colorado,[66] Connecticut,[67] District of Columbia,[68] Hawaii,[69] Illinois,[70] Oklahoma,[71] Rhode Island,[72] Vermont,[73] Virginia,[74] and Washington[75] have taken steps to address algorithmic discrimination resulting from the use of artificial intelligence. These states have introduced specific legislation that would generally require deployers and developers of automated decision tools to (i) conduct an impact assessment for any automated decision tool they utilize, (ii) notify individuals who are subject to consequential decisions made by automated decision tools before or at the time such tools are being used,[76] and (iii) establish reasonable administrative and technical safeguards to map, measure, manage and govern the reasonably foreseeable risks of algorithmic discrimination associated with the use or intended use of an automated decision tool. Among these states, California, Illinois, Oklahoma, Rhode Island and Vermont (Bill H711) would also provide individuals with the private right of action against covered entities in the event of a violation.

---

[64] New York Bill S5641A, available here.
[65] California Bill AB 2930, available here. CA Bill AB 2930 also requires annual impact assessments to be submitted to the state's Civil Rights Department.
[66] Colorado SB24-205 ("Consumer Protections for Artificial Intelligence," introduced on April 10, 2024, available here. On May 8th, 2024, the legislature passed this legislation. As of May 14, 2024, it awaits Governor Jared Polis's signature.
[67] Connecticut SB 2, available here. The Bill includes various sections aimed at mitigating potential AI-related risks, such as safeguarding consumers against algorithmic bias and ensuring transparency regarding the use of AI tools. On April 24, 2024, the Bill passed through the Connecticut Senate. It has now progressed to the Connecticut House for the next stage of the legislative process.
[68] District of Columbia Stop Discrimination by Algorithm Act of 2023, available here. The Act would, in principle, prohibit covered entities (any individual or legal entity) from making an algorithmic eligibility determination based on an individual's actual or perceived race, color, religion, national origin, sex, gender identity or expression, sexual orientation, familial status, source of income, or disability.
[69] Hawaii Bills HB1607 and SB 2524, available here and here.
[70] Illinois HB 5116, available here. This Bill is limited to deployers of an automated decision tools, and does not address deployers,
[71] Oklahoma Bill HB 3835, available here.
[72] Rhode Island Bill HB 7521, available here.
[73] Vermont H710, available here. Vermont's pending Bill H711 would apply to developers and deployers of inherently dangerous AI systems, like generative AI, and would regulate their use or sale. *See* Vermont H711, available here.
[74] Virginia Bill HB 747, available here. Virginia HB HB747 requires similar impact assessment, notice and risk management governance requirements for developers of high risk artificial intelligence systems. However, it excludes certain systems such as those designated for narrow procedural tasks or enhancing the outcome of a previously completed human activity.
[75] Washington Bill HB 1951, available here.
[76] Consequential decision is, in general, defined as any decision that has a material legal, or similarly significant, effect on consumer's access to credit, criminal justices, education, employment, health care, housing or insurance.

Moreover, the New York legislature has been actively involved in regulating algorithmic discrimination and artificial intelligence in general. The proposed Bill A8129, often referred to as the "New York AI Bill of Rights," would provide residents with rights and protections to ensure than any system making decisions without human intervention impacting their lives do so lawfully, properly, and with meaningful oversight.[77] These rights and protections would include: (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 an individual, (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.[78] The New York legislature could further regulate high-risk, advanced AI systems through proposed Bill A8195.[79] The Bill would also require any person developing a high-risk advanced AI system, whether in whole or in part, to disclose the system's existence and functions by applying for a license and registering the disclosed AI system.[80]

In Colorado, algorithmic discrimination is addressed specifically within the insurance sector through SB21-169, which prohibits insurers from unfairly discriminating based on an individual's personal traits in any insurance practice. Additionally, it forbids the use of any external consumer data and information source ("ECDIS"), algorithm, or predictive model in any insurance practice that could unfairly discriminate against an individual based on personal traits.[81] Notably, on May 8th, 2024, the legislature passed comprehensive AI legislation also addressing algorithmic discrimination, i.e., SB24-205. This bill specifically targets consumer protections in engagements with high-risk artificial intelligence systems.[82]

Finally, it is important to also consider Utah, as it has recently enacted the Utah Artificial Intelligence Policy Act (UAIP), which regulates the use of generative AI in private-sector.[83] The UAIP imposes certain disclosure requirements on entities using generative AI tools in their customer interactions. Accordingly, if a business or individual employs generative AI to engage with an individual for commercial purposes, they are obligated to clearly and conspicuously disclose to the individual that they are interacting with AI

[77] New York Assembly Bill A8129, available here.
[78] *Ibid.*
[79] New York Bill A8195, available here. The Bill defines "high-risk advanced AI system" as an AI system that possesses capabilities that can cause significant harm to the liberty, emotional, psychological, financial, physical, or privacy interest of an individual or groups of individuals, or which have significant implications on governance, infrastructure or the environment,
[80] *Ibid,* Section 410.
[81] Colorado SC21-169, available here. Please also note that in September 2023, the Colorado Division of Insurance released its Final Governance and Risk Management Framework Requirements for Life Insurers' Use of ECDIS, Algorithms, and Predictive Models (available here). According to the Final Regulation, the concept of ECDIS includes credit scores, social media habits, locations, purchasing habits, home ownership, educational attainment, licensures, civil judgments, court records, occupation that does not have a direct relationship to mortality, morbidity or longevity risk, consumer-generated Internet of Things data, biometric data, and any insurance risk scores derived by the insurer or third party from the above listed or similar data and/or information sources (Section 4(c)).
[82] Colorado SB24-205 ("Consumer Protections for Artificial Intelligence"), available here.
[83] Utah SB 149 ("Artificial Intelligence Policy Act"), enacted on March 23, 2024, available here.

and not a human.[84] Additionally, if the service involves regulated professions like clinical mental health, dentistry, or medicine, restrictive disclosure requirements, including verbal disclosure at the start of an oral exchange and through electronic messaging before a written exchange, are prescribed by the UAIP.[85] The UAIP also prohibits businesses from blaming generative AI to avoid responsibility for consumer protection violations or liability.[86] Lastly, the UAIP establishes the Office of Artificial Intelligence Policy, which is responsible for developing and managing an AI Learning Laboratory Program and tasked with engaging with stakeholders regarding AI regulatory proposals.[87]

Findings & Recommendations:

- As additional states begin to pass AI regulations, organizations are proactively working to develop and implement a global AI policy baseline that considers emerging requirements, as well as leading regulations and standards such as the EU AI Act and the NIST Risk Management Framework. However, there is growing concern about the feasibility of managing such a strategy in the near future, particularly with signals of a forthcoming wave of state-level AI regulation, each with unique definitions, requirements, and standards. This will ultimately compel organizations to establish separate governance structures for each state or regional approach, resulting in the inefficient use of AI systems and resources, and potentially less robust privacy protections.

- Many laws already address potential harms to consumers in a technology-agnostic way, e.g., data protection, fair lending, civil rights, and consumer protection laws. The fact that these laws are technology-agnostic allows these critical protections to remain applicable no matter how technology evolves in the future. While new AI-specific policies may be appropriate in some cases, there is a wide range of legal instruments which are already in place and should be leveraged by states. AI–specific laws should avoid overlap and inconsistencies with existing applicable laws.

- Organizations closely monitor the dynamic relationship between state-level AI regulations and comprehensive state privacy laws. Typically, they begin their analysis with the assumption that their globally harmonized approach to privacy law applies to the jurisdiction, then evaluate the impact of AI regulation against that backdrop. However, they are concerned about the divergence between comprehensive privacy laws and AI-specific laws, which could complicate organizations' ability to manage their overall compliance. In addressing the tensions between the needs of AI technology and data protection principles, state lawmakers and regulators should take into account:

[84] *Ibid,* Section 13-2-12(3).
[85] *Ibid,* Section 13-2-12(5).
[86] *Ibid,* Section 13-2-12(2).
[87] *Ibid,* Section 13-70-201 and Section 13-70-301.

- The outcomes intended by some data protection principles, especially data minimization, retention limitations, and purpose specification, could be achieved more effectively and pragmatically through mandating strong accountability-based safeguards, including risk assessments, transparency, internal oversight, monitoring, training and awareness, and effective enforcement of organizational policies;

- The data protection rules should recognize the need to process more data in some AI contexts (e.g. processing of sensitive data to prevent, detect and mitigate bias);

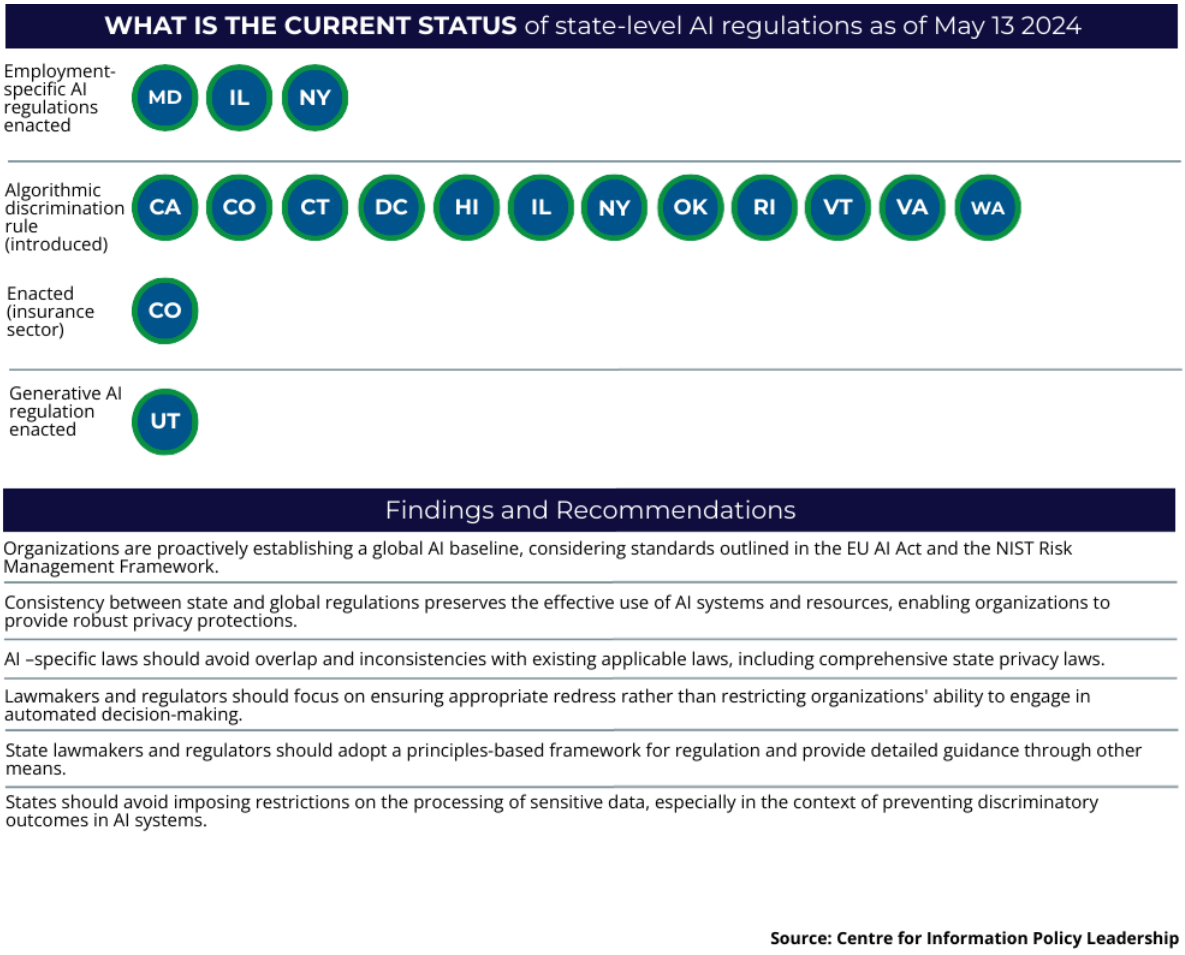
- Any transparency requirements should be high-level and principles-based to enable the delivery of appropriate and different forms of transparency for a variety of AI contexts; and,

- Any rules on automated decision-making should not restrict wholesale the ability to engage in ADM, but rather take a risk-based approach with a focus on ensuring appropriate oversight and avenues for redress, including through rights to review and appeal automated decisions.

- State lawmakers and regulators should articulate core objectives in laws (i.e., principles-based frameworks) and provide more detailed guidance subsequently. If the law itself includes requirements that are too specifically pegged to the technologies and business practices in use at the time of drafting, the law will soon become outdated. Indeed, unlike an overly prescriptive policy regime, a principles-based framework allows for swift adjustment to technological and societal changes and enables participants deploying a range of technologies to compete and innovate.

- It is often necessary to process sensitive forms of personal information (such as data on race, ethnicity, gender, etc.) to prevent and detect bias in algorithms. Denying access to or preventing the retention of such data can make it harder to detect and remedy bias, while also depriving all segments of society of the full benefits of AI. States should remain mindful of these complexities when designing rules for the processing of sensitive data, especially in the context of preventing discriminatory outcomes in AI systems. In fact, there is a global trend demonstrating that regulators are increasingly cognizant of this issue and understand that organizations need the ability to test for and mitigate bias in AI systems.[88]

[88] For example, Section 13 of the American Privacy Rights Act ("APRA") specifies that covered entities' self-testing efforts to prevent or mitigate unlawful discrimination serve as an exception to the general prohibition against processing data in a discriminatory manner. Additionally, the Office of the Privacy Commissioner for Personal Data, Hong Kong (HK PCPD) has noted in recent guidance that the quality of the data used to train AI systems should be managed, especially when the decisions made by the AI systems may have significant impacts on individuals, and



Source: Centre for Information Policy Leadership

recommends that organizations test data for bias before using it to train AI systems. If bias exists in the training dataset, the HK PCPD recommends that sampling techniques may be used to rebalance the class distribution. Moreover, the Singapore Personal Data Protection Commission (PDPC) has stated in its AI Model Governance Framework that while addressing bias in datasets may not be easy, organizations can mitigate the risk of inherent bias by having a heterogeneous dataset (i.e. collecting data from a variety of reliable sources). Hong Kong PCPD, "Guidance on the Ethical Development and Use of Artificial Intelligence," available here. Singapore PDPC, "Model Artificial Intelligence Governance Framework," available here.