

# Preparing Your AI Regulatory Compliance Program For 2023

By **Peter Schildkraut and Jami Vibbert** (October 4, 2022)

Regulatory compliance programs of U.S. companies often overlook artificial intelligence. After all, with limited exceptions, no regulation is directed at AI in the U.S.

That changes next year in Colorado, Connecticut, Virginia and New York City, and theoretically in California, too. Affected companies need to ensure their compliance programs are prepared.

## **New Requirements**

### ***Colorado, Connecticut and Virginia***

Over the past year, Colorado,[1] Connecticut[2] and Virginia[3] have enacted privacy legislation governing automated decision making.

Using virtually identical language, these new statutes contain two mandates particularly relevant to automated decision making. First, they will give consumers the right to opt out of automated decisions resulting in the provision or denial of:

- Financial or lending services;
- Housing;
- Insurance;
- Education enrollment or opportunity (Virginia omits education opportunity);
- Criminal justice;
- Employment opportunities, even though "consumer" excludes individuals acting in an employment context, and, in Colorado, job applicants;
- Health care services; or



Peter Schildkraut



Jami Vibbert

- Access to essential goods or services (in Virginia, basic necessities, such as food and water).

Where a human meaningfully considers the available data and can change or influence the decision, proposed Colorado regulations would permit a business not to honor a consumer's opt-out request if the business explains various aspects of the decision-making process to the consumer. The proposal also would specify how a business may seek a consumer's consent to withdraw an opt-out request.

Second, the new laws will require businesses to conduct and document data protection assessments before using AI or other algorithmic tools to make decisions that pose a reasonably foreseeable risk to consumers of:

- Unfair or deceptive treatment, or unlawful disparate impact;
- Financial, physical or reputational injury (Colorado omits reputational injury);
- Unreasonably offensive intrusion upon solitude, seclusion, or private affairs or concerns; or
- Other substantial injury.

The proposed Colorado regulations would clarify the covered harms and the scope of the required data protection assessments.

Algorithms for sales and marketing communications (including targeted advertising), insurance underwriting, lending and other consumer credit, housing and pricing, among other decisions, all could require document data protection assessments under these statutes.

Document data protection assessment requirements are intended to give companies pause before relying upon automated decision making, to ensure ample attention to the pros and cons from automating the decision.

Nevertheless, automated decision-making algorithms operate on probabilities, not certainties. Sooner or later, an algorithm will make an incorrect prediction. If the consumer harm is big enough, a government investigation or private litigation may result.

Although these privacy laws do not provide for a private right of action, causes of action under other statutes or the common law may exist.

Document data protection assessments must be made available to the state attorney general. While the statutes provide that this disclosure does not waive any privilege, a document data protection assessment may not be privileged in the first instance and could be discoverable in litigation brought by the injured party.

Businesses using automated decision-making technology, thus, should carefully consider the balance between the benefits and risks identified in the document data protection assessment, and they should take all reasonable steps to mitigate the risks. When the benefits do not clearly exceed the risks post-mitigation, companies may find it prudent not to employ automated decision making for the decision in question.

The new privacy laws will take effect in Virginia on Jan. 1, 2023, and in Colorado and Connecticut on July 1, 2023. There are exemptions for businesses below certain thresholds of affected individuals or revenue and for data and processing already regulated under certain federal privacy regimes, among other exceptions.

The Colorado Department of Law seeks comment on its proposals by its Feb. 1, 2023, rulemaking hearing; by Jan. 18, 2023, for consideration in any revisions presented at the hearing; or by Nov. 7, 2022, to inform stakeholder meetings discussing the proposals.

### ***California***

The 2020 California Privacy Rights Act[4] added Civil Code Section 1798.185(a)(16),[5] which requires adoption of regulations

governing access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including ... meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer.

While the California Privacy Protection Agency has proposed[6] most of the rules required by the CPRA, it has yet to unveil draft automated decision-making regulations. Theoretically, the CPPA will adopt final automated decision-making rules ahead of the statute's Jan. 1, 2023, effective date and July 1, 2023, enforceability date, but at least the first seems unlikely.

### ***New York City***

Beginning Jan. 1, 2023, a New York City law[7] will prohibit employers and employment agencies from using automated decision making to screen city residents for employment decisions unless the tool has undergone a bias audit in the previous year.

The bias audit must have been conducted by an independent auditor and, at a minimum, address disparate impacts by race, ethnicity and sex using the categories of the U.S. Equal Employment Opportunity Commission's EEO-1 Component 1 Report.[8]

Covered systems are "any computational process, derived from machine learning, statistical modeling, data analytics, or artificial intelligence, that issues simplified output, including a score, classification, or recommendation, that is used to substantially assist or replace discretionary decision making for making employment decisions that impact natural persons."

Before using such a system, employers and employment agencies must summarize on their

websites the results of the most recent bias audit and the distribution date of the tool.

At least 10 business days before using the screening system, the employer or employment agency must notify a candidate or employee of its plan to use an automated tool, the job qualifications and characteristics the tool will use in the assessment, and the candidate's right to request an alternative selection process or accommodation.

### **State AI Laws Already in Force**

These California, Colorado, Connecticut, Virginia and New York City automated decision-making laws are not the first laws governing AI in the U.S.

For several years, California[9] has prohibited certain chatbots, e.g., automated social media accounts or agents that pop up to offer help on certain websites. Specifically, the law proscribes intentionally deceitful use of chatbots masquerading as real people to influence purchases of goods or services or voting.

Since Jan. 1, the Illinois Artificial Intelligence Video Interview Act[10] has required employers to notify applicants when they use AI to vet video job interviews, explain how the system evaluates applicants and obtain applicants' consent to AI screening. The statute also imposes certain disclosure and data-retention limitations and requires the collection and reporting of demographic data for applicants rejected or hired solely by the AI system.

In addition, a number of federal, state and local agencies have enforced existing statutes that do not expressly contemplate AI — for instance, anti-discrimination or consumer protection laws — when the technology causes violations.

### **Compliance Considerations**

The first step for incorporating these new laws into a compliance program is identifying the AI and other automated decision-making systems used to make decisions about consumers, employees and job candidates. Obvious as that sounds, it may not be an easy task. Companies may not have needed such an inventory before, so they may have to build one from scratch.

For each automated decision-making system, the next step is to assess its risks. To spot them, adapt a checklist such as The Assessment List for Trustworthy AI[11] to the business and automated decision-making system.

Even with a checklist, it can be hard to achieve a full understanding of a system's risks.

The system's operators may not have trained or developed the underlying model. The system may rely on a mix of open-source and proprietary components and code. The proprietary elements may blend customized and commercial off-the-shelf modules. The customized portions may have been produced in-house or by vendors.

In short, nobody may have the full picture, so the risk assessment may require peeling the onion layer by layer.

Once the risks are understood, a company should take reasonable steps to mitigate them. Mitigating automated decision-making risk involves many dimensions.

Explainability is a good place to start. Explaining an adverse decision enables an effective

appeal if a system's prediction doesn't make sense, or acceptance of the outcome if it does.

In addition, having a broad array of explanations for each system will facilitate oversight and give leadership greater confidence the system is accurate and comports with legal requirements and business objectives. "Explaining Decisions Made with AI" by the Information Commissioner Office and The Alan Turing Institute is a practical guide to providing meaningful explanations.[12]

Bias should be another focus for risk mitigation. Companies conducting their own bias audits — recall the New York City law requires independent bias audits — may wish to consult the Algorithmic Bias Playbook.[13]

At the end of the day, however, as the Brookings Institution explains, "there is no simple metric to measure fairness that a software engineer can apply. ... Fairness is a human, not a mathematical, determination."[14]

Bias audits may turn up disparate impacts against protected classes, but the differences may be legally justified by bona fide business reasons. In those circumstances, a company will have to consider whether the justification is consistent with its values.

The new laws also mandate retention of document data protection assessments and bias audits, and businesses may have other reasons to record how their AI and other automated decision-making systems were developed, trained and used.

When mistaken decisions happen — and, as discussed above, they will — evidence of due care to mitigate risks can help defend against government investigations or private litigation. Of course, increased retention has its own difficulties. The imperative is reconsidering whether existing policies strike the right balance.

### **Global Automated Decision-Making Regulation**

The state and local laws taking effect next year are part of a global march toward regulating AI and other automated decision making. Federally, the leading congressional privacy bills would regulate algorithms. Meanwhile, the Federal Trade Commission has published an advance notice of proposed rulemaking addressing automated decision making as well as privacy and data security.[15]

Additionally, the White House Office of Science and Technology Policy has released its "Blueprint for an AI Bill of Rights" to inform policy decisions.[16]

The California, Colorado, Connecticut and Virginia automated decision-making provisions echo Article 22[17] of the European Union General Data Protection Regulation. Building on the GDPR, the EU is expected to adopt the extremely prescriptive Artificial Intelligence Act[18] next year, once the co-legislators complete their deliberations.

The Chinese Cyberspace Administration has adopted Internet Information Service Algorithmic Recommendation Management Provisions[19] and is finalizing its regulation[20] of algorithmically created content, including virtual reality, text generation, text to speech and deepfakes.

The U.K. government is seeking[21] comment on its proposed AI regulatory framework and plans to introduce its AI-governance strategy late this year. The Canadian government has introduced the Artificial Intelligence and Data Act within broader legislation.[22] Brazil, too,

is crafting a law<sup>[23]</sup> regulating AI. And countries like Brazil, China and South Africa also address automated decision making in their privacy laws.

In sum, legislators and regulators worldwide are focusing on the risks of AI and other automated decision-making systems. Whether solely domestic or truly global, U.S. companies developing, selling, procuring or using those systems should too. They can begin by readying their compliance programs for the new laws taking effect next year.

---

*Peter J. Schildkraut is a partner and co-leader of the technology, media and telecommunications group at Arnold & Porter.*

*Jami Vibbert is a partner and chair of the privacy, cybersecurity and data strategy group at the firm.*

*Arnold & Porter associates Darrel Pae and Leah A. Schultz contributed to this article.*

*The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.*

[1] C.R.S. § 6-1-1301, <https://advance.lexis.com/documentpage/?pdmfid=1000516&crd=9c47ee38-8a37-440a-b865-a2d6c9b615c0&nodeid=AAGAABAABAAOAC&nodepath=%2FROOT%2FAAG%2FAAGAAB%2FAAGAABAAB%2FAAGAABAABAAO%2FAAGAABAABAAOAC&level=5&haschildren=&populated=false&title=6-1-1301.+Short+title.&config=014FJAAyNGJkY2Y4Zi1mNjgyLTRkN2YtYmE4OS03NTYzNzYzOTg0OGEKAFBvZENhdGFsb2d592qv2Kywlf8caKqYROP5&pddocfullpath=%2Fshared%2Fdocument%2Fstatutes-legislation%2Furn%3AcontentItem%3A63JP-6XP3-GXJ9-330N-00008-00&ecomp=vgf59kk&prid=f9c3a23a-7ec8-4470-91b2-8cb6140b427e>.

[2] <https://www.cga.ct.gov/2022/act/Pa/pdf/2022PA-00015-R00SB-00006-PA.PDF>.

[3] <https://law.lis.virginia.gov/vacode/title59.1/chapter53/>.

[4] <https://www.arnoldporter.com/en/perspectives/advisories/2020/11/voters-overhaul-cpa-via-ballot-initiative>.

[5] [https://leginfo.legislature.ca.gov/faces/codes\\_displaySection.xhtml?sectionNum=1798.185&lawCode=CIV#:~:text=\(I\)%20Global%20opt%20out%20from,of%20My%20Sensitive%20Personal%20Information.%E2%80%9D](https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.185&lawCode=CIV#:~:text=(I)%20Global%20opt%20out%20from,of%20My%20Sensitive%20Personal%20Information.%E2%80%9D).

[6] <https://www.arnoldporter.com/en/perspectives/advisories/2022/07/ca-privacy-protection-agency-invites-comments>.

[7] <https://codelibrary.amlegal.com/codes/newyorkcity/latest/NYCAadmin/0-0-0-135839>.

[8] [https://eeocdata.org/pdfs/EEO-1\\_Fact\\_Sheet.pdf](https://eeocdata.org/pdfs/EEO-1_Fact_Sheet.pdf).

[9] [https://leginfo.legislature.ca.gov/faces/codes\\_displayText.xhtml?lawCode=BPC&division](https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=BPC&division)

=7.&title=&part=3.&chapter=6.&article=.

[10] <https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=4015&ChapterID=68>.

[11] <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>.

[12] <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-artificial-intelligence/>.

[13] <https://www.chicagobooth.edu/research/center-for-applied-artificial-intelligence/research/algorithmic-bias>.

[14] <https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/>.

[15] <https://www.arnoldporter.com/en/perspectives/advisories/2022/08/major-changes-ahead-for-the-digital-economy>.

[16] <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf>.

[17] <https://gdpr-info.eu/art-22-gdpr/>.

[18] <https://www.arnoldporter.com/en/perspectives/advisories/2021/04/ec-proposes-legislation-regulating-ai>.

[19] <https://www.arnoldporter.com/en/perspectives/publications/2022/03/have-your-websites-online-services-unlawful>.

[20] <https://digichina.stanford.edu/work/translation-internet-information-service-deep-synthesis-management-provisions-draft-for-comment-jan-2022/>.

[21] <https://www.arnoldporter.com/en/perspectives/blogs/enforcement-edge/2022/07/uk-proposes-framework-for-regulating-ai>.

[22] <https://www.parl.ca/legisinfo/en/bill/44-1/c-27>.

[23] <https://www12.senado.leg.br/noticias/materias/2022/05/11/comissao-do-marco-regulatorio-da-inteligencia-artificial-estende-prazo-para-sugestoes>.