Articles + Publications | January 12, 2023

Outgoing DC Attorney General Ushers in Era of Regulated AI

WRITTEN BY

Stephen C. Piepgrass | Ashley L. Taylor, Jr. | Sadia Mirza | Daniel Waltz

In recent months, there has been an explosion of artificial intelligence (AI) tools that have given even technophobes an opportunity to test AI's power from the comfort of their favorite web browser. From DALL-E's ability to generate digital images from natural language prompts to ChatGPT's ability to answer questions, write blog posts, essays, poetry, or even song lyrics, today's AI tools can be used by anyone who can use a web browser.

Behind the scenes of these AI tools and more powerful ones long employed by corporations and government entities, algorithms are hard at work. Although algorithms are a series of objective mathematical instructions, critics have claimed that in some contexts, unless precautions are taken, they can amplify pre-existing subjective biases and worsen socioeconomic disparities based on the data fed to them.

That is why state attorneys general (AGs) are turning their sights to this fast-developing technology. Through lawsuits and — most notably, legislation introduced by Washington, D.C. AG Karl Racine who left office at the end of 2022 — state AGs are making their presence felt as AI technology is increasingly substituting for human decision-making.

As AI becomes increasingly responsible for making decisions on a multitude of aspects of our lives, some observers have asserted that flaws in the system can lead to generational consequences. The move to regulate stems from a widespread belief among industry watchers that discriminatory tendencies must be reined in as soon as possible to prevent those tendencies from proliferating along with AI technologies.

Algorithms and algorithm training data power AI

Algorithms power AI. They are mathematical instructions programmed to solve a problem by instructing a computer to perform a series of predefined "if," "and," "or," or "or not" statements — instructions present in computer programming since at least the 1970s. By layering levels of complex algorithms on top of enormous pools of data, AI can answer complex questions and make recommendations of which only humans were thought capable.

The data used to train an AI model is just as important as the algorithms on which the model is built because the data helps teach the model "right" answers. In addition, many AI models are trained over time with varying levels of human involvement — from supervised learning to entirely unsupervised learning. Because of the complexity of these models, it is frequently the case that after AI models have become fully formed, humans — even those who designed the models — have trouble understanding how variables have been combined and assessed to solve the problem at hand and generate an output. Without adequate oversight, the end result of this complexity is a black box of decision-making.

Biased and discriminatory training data can lead to AI models that create biased and discriminatory outcomes. Imagine a company wants to develop an AI tool to weed through job applicants' resumes to quickly whittle down large numbers of resumes to only a handful and avoid the implicit bias human evaluators might bring. Thus, the company trains its AI model based on resumes of employees it hired over the past two decades.

But because the company rarely hired people with ethnic last names until recently, the AI model could show a strong preference for nonethnic last names, regardless of other factors, because of the data with which it was trained. Each time the model recommends a candidate with a nonethnic last name without it being trained to recommend candidates with ethnic names, the biased and discriminatory nature of the model compounds.

Even though the company had a noble goal of a nonbiased, nondiscriminatory vetting process for resumes, the subjectivity of the underlying data that trained its AI model infiltrated the system and created a discriminatory outcome. The AI ends up reinforcing the very implicit bias it was intended to avoid.

Discriminatory algorithms are not theoretical

Observers note that algorithms trained by flawed data that produce discriminatory outcomes are not theoretical concerns. The use of potentially problematic algorithms in three particular industries that may impact fundamental aspects of human life are driving state AGs to target discriminatory algorithms.

1. **Employment** – where AI may be used to test applicants' abilities or weed out job seekers whose skills and backgrounds as described on their resumes are not matches for the positions for which they have applied.

2. **Health Care** – where hospitals, health care providers, and insurers have relied on algorithms with the goal of making better decisions about how to treat patients.

3. **Tenant Screening** – where S. landlords receive tenant screening reports from companies that employ algorithms to determine whether would-be renters should be offered leases.

In each of these instances, critics have raised concerns about the potential for discriminatory outcomes, resulting in increased regulatory attention. Employers have long used AI.

Regulators take aim at discriminatory algorithms, led by the DC AG

For the last year, D.C. AG Racine led the charge to eliminate discriminatory algorithms with his "Stop Discrimination by Algorithms Act of 2021."

If passed, the act (as originally drafted in December 2021) would, among other things:

- Make it illegal for corporations and organizations to use algorithms that make eligibility determinations based on "an individual's or class of individuals' actual or perceived race, color, religion, national origin, sex, gender identity or expression, sexual orientation, familial status, source of income, or disability in a manner that segregates, discriminates against, or otherwise makes important life opportunities unavailable to an individual or class of individuals."

  These "life opportunities" include "access to, approval for, or offer of" credit, education, employment, housing, a place of public accommodation, or insurance.

- Require companies and organizations to audit their algorithms annually for discriminatory patterns, and document how they built their algorithms, how the algorithms make determinations, and all the determinations made by them.

- Require companies and organizations to disclose to consumers, in plain English, information about their use of algorithms to reach decisions, the personal information they collect, and how their algorithms use that information to reach decisions. In addition, they would be required to provide in-depth explanations about unfavorable decisions and to allow consumers an opportunity to correct inaccurate personal information that could lead to unfavorable decisions.

The act provides the D.C. AG with enforcement authority and the ability to levy up to $10,000 in civil penalties per violation. It also provides a private cause of action for act violations for which courts may award between $100 and $10,000 per violation or actual damages, whichever is greater.

Several states already have enacted legislation aimed at regulating AI applications, while many others have such legislation pending. For example, California's Consumer Protection Act (CCPA), as amended by the California Privacy Rights Act (CPRA), directs the California Privacy Protection Agency (CPPA) to issue regulations concerning an individuals access and opt-out rights with respect to businesses' use of automated decision-making technology. The Virginia Consumer Data Protection Act (VCDPA), Colorado Privacy Act (CPA), and Connecticut Data Privacy Act (CTDPA) also require businesses to provide consumers with the opportunity to opt out of certain automated decision processes that profile consumers in furtherance of decisions impacting financial, lending, housing, and insurance determinations. The CCPA/CPRA and VCDPA are effective January 1, 2023, while the CPA and CTDPA take effect on July 1, 2023. Additional regulations and rulemaking are expected this year, which will clarify the scope of enacted legislation.

In the absence of legislation, however, some state AGs are already taking action to regulate companies' use of algorithms. For example:

- In March 2020, then-Vermont AG Thomas Donovan sued Clearview AI over the company's use of facial recognition technology. AG Donovan alleged Clearview used facial recognition technology to map the faces of individuals, including children, and sold the data to businesses and law enforcement in violation of the Vermont Consumer Protection Act. And, most recently in August 2022, California AG Rob Bonta sent a letter to hospital

CEOs across California, opening an inquiry into their use of potentially biased algorithms.

- In May 2022, the National Association of Attorneys General (NAAG) announced the NAAG Center on Cyber and Technology (CyTech), which will develop resources to support state AGs in understanding emerging technologies, including machine learning, AI, and the potential bias and discrimination that may result.

Welcome to the era of regulated AI

While former D.C. AG Racine might be the first state AG to try to combat discriminatory algorithms through legislation, he is unlikely to be the last. Other state AGs are likely to use current laws, in addition to proposing new ones, to pursue the companies and organizations that create or use algorithms that they view as causing discriminatory outcomes.

We are still in the early days of state AGs regulating AI and algorithms through statehouses and courthouses. Recognizing that state AGs are closely scrutinizing the use of algorithms for discriminatory impact, the companies and organizations creating or using AI should focus their compliance, research, and development efforts accordingly.

RELATED INDUSTRIES + PRACTICES

- Artificial Intelligence
- Regulatory Investigations, Strategy + Enforcement
- State Attorneys General