THE NATIONAL LAW JOURNAL

Governing AI: Addressing Opportunities and Challenges Through State and Local Law

By Karen Sebaski | May 8, 2023

As artificial intelligence technology becomes increasingly sophisticated and more widely utilized, providers of AI solutions, and the entities that implement such technology in commercial settings, face a myriad of legal and ethical issues, including bias and diversity, privacy, and confidentiality concerns, just to name a few. Although the federal government has not yet passed comprehensive legislation specifically governing AI technology, a patchwork of state and local laws to address such challenges have started to develop. This article discusses these key issues, with examples of legislation, and a potential avenue for federal oversight.

Bias and Diversity

In commercial settings, hiring decisions and performance evaluations are a notable use case for AI technology. Amazon's high-profile attempt several years ago to develop an automated recruiting tool to review and rank job candidates illustrates how the use of such decision tools can impact outcomes. Specifically, the company scrapped the project after realizing "its new system was not rating candidates for software developer jobs and other technical posts in a gender-neutral way. That is because Amazon's computer models were trained to vet applicants by observing patterns in resumes submitted to the company over a 10-year period. Most came from men, a reflection of male dominance across the tech industry," according to Jeffrey Dastin of Reuters.

New York City's new Local Law No. 144 of 2021, the first of its kind in the United States, is aimed at remedying such scenarios. Local Law 144 requires employers and employment agencies that use automated employment decision tools in connection with employment decisions to take various steps to notify candidates and ensure nondiscriminatory decision-making. An automated employment decision tool is defined as "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," and employment decisions means screening candidates for employment or employees for promotion within NYC. Just weeks ago, the New York City Department of Consumer and Worker Protection adopted the final rules implementing the law, which will be enforced beginning in July. Requirements include annual bias audits conducted by an independent auditor, the results of which are summarized in a "clear and conspicuous manner" in the employment section of the employer or employment agency's website; 10 business days' notice to candidates of the qualifications or characteristics that the firm's AI tool will be looking for, with an opportunity to request an alternative selection process; and to make available the type of data collected for the AI tool, the source of such data, and the data retention policy.

Privacy and Confidentiality

Many AI use cases implicate privacy and confidentiality issues. Generative AI tools such as ChatGPT, for example, are trained to extract patterns from and understand natural language, and predict the best answers to user inputs. As one might expect, training requires large quantities of data. Notably, developers may retain the right to utilize user prompts to retrain or improve the algorithm. OpenAI's terms of use, for example, state that "[w]e may use Content from Services other than our API ('Non-API Content') to help develop and improve our services." OpenAI's website confirms that ChatGPT and DALL-E, which generates images and art from natural language descriptions, are non-API consumer services, although consumers can request to opt out of such usage via an online form. As a result, the best practice is to assume that generative AI inputs will be used by the developer and not to input prompts that may reveal confidential information—whether standing alone or in association with the identity of the prompter. Likewise, enterprise versions of such platforms may provide organizations with an opportunity to negotiate such terms of service.

AI tools that use biometric data, such as facial and voice recognition and fingerprints, to authenticate individuals, raise privacy concerns. In 2008, Illinois enacted the Illinois Biometric Information Privacy Act, which explains that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, Social Security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, [and] is at heightened risk for identity theft." The BIPA requires companies to obtain written informed consent before collecting biometric data and to implement and maintain data security measures. BIPA also creates a private right of action for statutory damages to remedy any violations. Likewise, a Washington state law requires notice and either consent or a mechanism to prevent subsequent use before a biometric identifier may be used for a commercial purpose. In Texas, the attorney general has relied on the Texas Capture or Use of Biometric Identifier Act, which also addresses commercial use of biometrics, to bring lawsuits for alleged improper use of data to train AI models.

Karen Sebaski, *counsel at Holwell Shuster & Goldberg, has a broad-based practice, with particular emphasis on patent litigation, internal investigations and complex commercial litigation.*

Opportunities for Federal Oversight

At the national level, the Federal Trade Commission is increasingly focused on AI and its impacts for consumers. In 2021, Congress directed the FTC to examine how AI "may be used to identify, remove, or take any other appropriate action necessary to address" particular "online harms," including fake reviews, child sexual exploitation and deepfakes. Although "Congress instructed the commission to recommend laws that could advance the use of AI to address online harms," a report released by the FTC in June 2022 concluded that "given that major tech platforms and others are already using AI tools to address online harms, lawmakers should consider focusing on developing legal frameworks that would ensure that AI tools do not cause additional harm." Whether, and how quickly, federal lawmakers do so remains to be seen.