Legaltech news

The Liabilities of Artificial Intelligence Are Increasing

The Liabilities of Artificial Intelligence Are Increasing

The longer regulators wait, the more widely used algorithmic decision-making systems become. In the process, the concrete harms these technologies can cause are becoming clear. So what can companies do?

By LegalTech News Staff

Artificial intelligenceImage by Shutterstock

“With the proliferation of machine learning and predictive analytics, the FTC should make use of its unfairness authority to tackle discriminatory algorithms and practices in the economy.”

This statement came from FTC Commissioner Rohit Chopra at the end of May. The fact that these words followed a more formal blogpost from the regulator focused on artificial intelligence—in the midst of a global pandemic, no less—highlights what is becoming the new normal: Liabilities on the use of algorithmic decision-making are increasing. This holds true with or without new federal regulations on AI.

For those paying attention to the rapid adoption of AI, this trend might come as no surprise—especially given that regulators have been discussing new regulations on AI for years (as I've written about here before). But the increasing liability of algorithmic decision-making systems, which often incorporate artificial intelligence and machine learning, also stems from a newer development: the longer regulators wait, the more widely used AI becomes. In the process, the concrete harms these technologies can cause are becoming clear.

Take, for example, automated screening systems for tenants, which the publication *The Markup* recently revealed have been plagued by inaccuracies that have generated millions of dollars in lawsuits and fines. "With about half of the nation's 43 million rentals turning over every year," according to *The Markup*, "even an error rate of 1 percent could upend the lives of hundreds of thousands of people." Among those people are, for example, Hector Hernandez-Garcia who, along with his wife and newborn son, became temporarily homeless after being incorrectly profiled by one such algorithm. (Hernandez-Garcia sued; the company settled.)

Or take the Michigan Integrated Data Automated System, used by the state to monitor filing for unemployment benefits, which was also recently alleged to have falsely accused thousands of citizens of fraud. Class action lawsuits have been filed against the state, alleging a host of problems with the system and demonstrating that automated systems create harms that are as hard-to-detect as they are injurious.

Then there's the recent lawsuit against Clearview AI, filed in Illinois at the end of May by the ACLU and a leading privacy class action law firm, alleging that the company's algorithms violated the state's Biometric Information Privacy Act. That act limits the way that data like fingerprints or facial images can be used, with a fine of up to $5,000 per violation, which other states have sought to imitate in recent years.

In other words, the list of lawsuits, fines and other liabilities created by AI is long and getting longer. The non-profit Partnership on AI even recently released an AI incident database to track how models can be misused or go awry.

All of which means that organizations adopting AI are creating concrete liabilities in the process. Indeed, these harms are becoming more apparent to regulators and consumers alike every day. As the fallout from pandemic creates new pressures for organizations to embrace automation, the adoption of AI is likely to accelerate even more.

So what can companies do?

The first answer is to have plans in place for when AI causes harm. There is a burgeoning field of AI incident response—similar to traditional cybersecurity incident response—focused on crafting clear plans for how to react when algorithms misbehave. This type of algorithmic misbehavior might have internal causes, like when the data the AI was trained on differs too widely from data in the real world. Or it can have external causes, like an attacker attempting to manipulate the algorithm.

Whatever the cause, there's a range of materials that lawyers can use to help their organizations prepare, like this series of articles focused on legal planning for the adoption of AI. (I've contributed directly to that literature as well.)

Second is asking the right questions to mitigate major risks before they emerge. To help lawyers in this role, my boutique law firm, bnh.ai, teamed up with the non-profit Future of Privacy Forum to release a set of 10 questions called "10 Questions on AI Risk" earlier this month. These basic questions can help guide lawyers as they seek to understand key areas of liability created by AI.

Last, and perhaps most importantly, is the importance of not waiting until an incident occurs to address AI risks. When incidents do occur, for example, it's not simply the incidents that regulators or plaintiffs scrutinize, it's the entire system in which the incident took place. That means that reasonable practices for security, privacy, auditing, documentation, testing and more all have key roles to play in mitigating the dangers of AI. Once the incident occurs, it's frequently too late to avoid the most serious harms.

An ounce of prevention, to quote the old proverb, is worth a pound of cure. And that's true now more than ever for organizations adopting AI.