PUBLICATIONS | 02.08.2024

2024 Boston Bar Association Privacy, Cybersecurity and Digital Law Conference on AI Takeaways

We have compiled key takeaways from the recent Boston Bar Association Privacy, Cybersecurity and Digital Law Conference, which focused on five insightful panel discussions related to issues arising from AI.

What Tech Experts Wish Lawyers Knew About Generative AI

As generative AI has evolved, the associated legal risks related to safety, cybersecurity, intellectual property, and data privacy have also changed. The vast quantity of data used to train AI models is increasingly rendering human-performed quality checks impossible, and higher quality training data is leading to the unlicensed use of protected information and the inability to copyright AI-generated content.

AI-related safety risks include potential mental health risks for people employed to review and remove violent, indecent, and traumatizing content, and an end user's intentional circumvention of a model's safety parameters causing the model to return answers that developers intended to prevent (i.e., bomb-making instructions).

There are many inherent cybersecurity and data privacy vulnerabilities to consider, including the potential for training data to become compromised or to include malicious code, and the accidental exposure of confidential training data to an end user. Additionally, there are reliability concerns related to models' tendency to fabricate answers (called "hallucinations") when those AI models are posed questions on which they have inadequate training.

Bias and Ethics Issues for Tech Companies

Companies using AI should consider how their activities will appear to consumers or to a jury. For, as long as there is little legislation or regulation directed specifically at AI, plaintiffs will bring legal claims based on generally applicable statutes, such as consumer protection statutes or anti-discrimination laws in personnel, credit, housing, or other kinds of decisions.

State of Regulation of AI

Experts believe that existing state laws, such as Massachusetts' Chapter 93A (prohibiting unfair or deceptive business practices), can put some meaningful checks on the use of AI. Furthermore, companies have a responsibility to ensure that their AI practices, whether those be data collection, targeted advertising, media manipulation, and the like – do not run afoul of existing state data privacy and consumer protection laws.

That said, experts predict an increasing amount of targeted legislation and regulation at the state and federal level, as highlighted by the Biden Administration's recent Executive Order seeking to manage the risks of AI and calling on Congress to enact legislation to address privacy concerns and protect consumers. The Executive Order does not provide much substantive framework, but it is an example of increased governmental attention to this issue.

In light of this increased governmental attention, companies should enact compliance measures to monitor and prevent any bias

and discrimination stemming from AI technology and should also provide employees and customers complete transparency, including around which decisions are being made with the help of AI tools.

How Private is AI? How Private can it be?

Some companies are inadvertently collecting more personal and biometric data than is necessary, without obtaining proper consent from customers or employees. These companies may be violating data privacy laws that require clear notice of both the collection and use of personal data.

To help companies manage data privacy risk and ensure that their AI is compliant with existing statutes and regulations, companies should audit their AI systems and regularly monitor them, so the companies can be prepared in the event of a government investigation or other legal claims.

Does My Chatbot Have Rights? Privacy, the First Amendment, and Rights Surrounding AI Input

While it may be a long time before courts recognize rights in something other than people, it is possible courts could eventually consider ChatGPT or other AI tools "a person" for convenient legal reasons. For example, if ChatGPT libels or defames someone, what is that person's recourse? The individual might not have a viable claim against OpenAI, the company that owns ChatGPT, because the company can respond that it did not knowingly engage in libel. Therefore, a court could conceivably impose legal duties on ChatGPT to provide recourse to libel victims, although how that would work is not at all clear.

Experts also observe an increased tension between efforts to regulate AI and First Amendment issues. While there are valid regulatory reasons to restrict the use of AI through age verification, content regulation, etc., efforts to implement these restrictions without infringing on First Amendment rights will bring significant judicial scrutiny, as we have already seen with overly broad social media content regulations being struck down.

Printable version.

Adam J. Bookbinder
Co-Chair, Government Enforcement & Compliance

Elizabeth Powers
Of Counsel

Rebecca Brownell
Associate

Sarah Gonsenhauser
Associate