Webinar Recap: Designing Effective AI Compliance Programs

By Emilie Feyler, Pedro Chirinos Terrones, David Toniatti, and Georgina Scoville

ABA Antitrust Law Section (May 1, 2024)

Artificial Intelligence (AI) tools' increasingly "black box" nature has significant implications for potential enforcement actions. How can firms implement effective compliance audit programs as AI rapidly transitions from a predictive tool to a generative technology capable of creating information on the fly?

On February 28th, 2024, the Media and Technology Committee of the ABA Antitrust Law Section hosted a webinar titled "Designing Effective AI Compliance Programs."[1] The webinar was moderated by Rishi Satia (Morgan Lewis), with panelists Amir Ghavi (Fried Frank), Ben Rossen (OpenAI), and John Horton (MIT Sloan School of Management).

This panel discussed the evolving landscape of AI, mainly focusing on recent advancements, legal challenges, regulatory responses, and standard-setting efforts. The panel also addressed the potential risks of AI, such as algorithmic collusion in pricing strategies and the need to distinguish between legitimate uses of predictive algorithms and potential misinformation.

Introduction: definition of AI technologies

Dr. Horton, Associate Professor of Information Technologies at the MIT Sloan School of Management, discussed the recent developments in AI technologies. According to Dr. Horton, the distinguishing factor of recent AI technologies is its generative nature. In prior years, AI models were primarily capable of predictions or recommendations; more recent technology is capable of creating information goods on the fly and has several uses, including summarizing documents or assisting in decision-making. AI raises questions around accountability and responsibility, specifically when an agent takes an action or decision based on recommendations from an AI tool.

Current legal challenges: recent claims against AI tools

Legal challenges, primarily copyright-related, have emerged, with debates around fair use and labor issues gaining traction. Mr. Ghavi provided his perspective on recent AI-related claims as a lawyer specializing in Intellectual Property and Technology. He mentioned that, as of the day of the webinar, a number of copyright claims had been filed.

From Mr. Ghavi's perspective, plaintiffs in these cases argue that AI tools are trained without the consent of content owners, while defendants argue fair use as a statutory defense. According to Mr. Ghavi, from the time copyrights have been legally recognized, courts have understood that, in order for copyrights to work, some exceptions are needed; otherwise, development stagnates. Hence, the main question around copyright cases is whether training AI tools with publicly available data is "fair use" under the copyright statute or not. In Mr. Ghavi's opinion, copyright is often not the right tool to fight back against AI; instead labor law may be more promising. As an example, Mr. Ghavi cited SAG-AFTRA and the Writers Guild of America, who were able to navigate AI law successfully, while copyright claims have mostly been dismissed.

Mr. Horton explained that, from a policy perspective, pretending to cover everything under copyright law is unworkable given the different use cases and implications for market definition. In his view, it is unlikely that large language models (LLMs) are competitors to content-creating platforms. For example, it is unlikely that consumers will consider ChatGPT and New York Times true competitors, so they are unlikely to be included in the same product market. Mr. Ghavi pointed out that the market displacement argument is the dispositive factor in determining fair use under copyright law.

Current legal challenges: AI regulation

Mr. Satia turned the focus of the discussion to regulatory issues, including the Executive Order on Safe, Secure, and Trustworthy AI issued by the Biden administration. Mr. Rossen, Associate General Counsel at OpenAI, provided a brief description of this Executive Order, which contains:

- Regulation for the use of AI within different agencies and best practices on a whole range of issues.
- The urging of independent agencies (such as the FTC) to use their power to protect consumers and investigate probable anticompetitive issues related to AI.

From Mr. Rossen's perspective, the Order's invocation of the Defense Production Act has an important impact, since it allows the administration to take steps that directly affect the industry. In addition, the Order has new requirements for companies that develop "dual-use foundation models" (referring to the most powerful kind of general-purpose AI models), such as reporting new training runs and the amounts of compute

power to conduct them. This will allow the federal government to have visibility on the emerging capabilities of the most powerful models. This reporting requirement has a threshold based on the amount of compute power used, but several models are rapidly reaching this threshold.

Mr. Rossen further explained that another disposition of the Executive Order is the creation of a new AI Safety Institute, similar to entities in the European Union or the United Kingdom. The AI Safety Institute has a consortium (which includes OpenAI), where the industry shares insights with the government to help develop practices for evaluating models and new capabilities, assesses risks, and conducts red teaming. Even though this institute does not have the authority to regulate under the Executive Order, they can help to create best practices and new guidance around AI compliance. Overall, Mr. Rossen said that the Executive Order is a very ambitious order. He considers it encouraging that the federal government is taking steps towards studying AI's impact on labor markets, civil rights, and national security applications.

The panelists then discussed recent developments in standard-setting guidelines. Mr. Rossen discussed the C2PA and its impact on the industry. The C2PA is a metadata-based standard for watermarking and provenance that identifies the source of the information used by an AI model. Mr. Rossen believes that the C2PA will not prevent advanced threats from engaging in sophisticated disinformation, but he notes that it could establish trust on social media platforms: the absence of C2PA metadata itself could signal that a source is not authentic. Mr. Rossen said he does not believe C2PA came from the Executive Order, but it is one of the different solutions people are using to address the issue of provenance.

AI governance and effective compliance programs

The panelists then discussed the issues involved in designing effective AI compliance programs. Mr. Ghavi provided some key aspects businesses should focus on:

- When AI governance is mentioned, businesses should begin by considering the "who." For instance, does it make sense to develop guidelines for businesses, such as OpenAI, for developers adjusting models to fit company needs, or for employees using the technology? Second, businesses could consider use cases; for instance, whether AI is being used to create a new product, as an internal business process, or as a cost-saving device.
- Using AI tools does not mean that existing laws no longer apply. According to Mr. Ghavi, the use of AI tools have resulted in legal claims related to violations of labor laws, among others. Business should focus on conducting appropriate red testing or anti-bias testing.

The panelists then discussed who should implement AI governance and compliance programs, and how much they should rely on the end user as opposed to the upstream developer. Mr. Ghavi explained that it is important to determine who is responsible for

compliance. For instance, the Executive Order places a large number of obligations on the developers. In addition, he stated that companies that use AI tools usually do fine-tuning, which is adapting those tools to their businesses by retraining those models to their specific datasets. The question is who should be responsible for the differential between the programmer's original product and the users' fine-tuned product.

Mr. Rossen followed up by recognizing that a virtue of the Executive Order is the distinction between developers and deployers, each with different responsibilities and abilities to evaluate compliance. There are things that developers are better suited to evaluate downstream. The responsibility of compliance will likely depend on who has the information once the model is out and fine-tuned.

Dr. Horton raised awareness of the fact that these new regulations can create fixed costs for existing AI developers and would limit the new entrants to this market, which could lead to more oligopolistic markets.

AI and collusion

The panelists discussed how much human oversight is needed, and whether AI models can govern themselves. Dr. Horton opined that having humans involved in the process is reasonable and sensible, especially because this technology can have capabilities and applications their creators may not have initially anticipated. Regarding anticompetitive conduct, Dr. Horton explained that some academic papers show how sophisticated algorithms can learn to collude. However, algorithmic collusion has only been observed in laboratory models, not in real-world cases yet.

Mr. Satia then asked Mr. Ghavi about the antitrust implications of having the models trained under the same dataset and if there is a potential risk for collusive or coordinated conduct. Mr. Ghavi explained that, indeed, these models have the same DNA because they use the same dataset. However, the difference depends on how they have been trained. Models trained differently will have different outcomes even if they rely on the same dataset.

Finally, Mr. Satia and Mr. Rossen discussed the guardrails that developers (or even end users) should implement to limit the dissemination of sensitive data that is fed into a model. They concluded that company policies are crucial to limit the risk of employees leaking information to AI models, and that there will be a bigger push in the next year to provide AI literacy work to the public.

Endnotes

1 The webinar was co-sponsored by the Joint Conduct Committee and Compliance and Ethics Committee.